NOTICE OF FILING

Details of Filing

Document Lodged:	Statement of Claim - Form 17 - Rule 8.06(1)(a)
Court of Filing	FEDERAL COURT OF AUSTRALIA (FCA)
Date of Lodgment:	7/12/2022 7:52:14 AM AEDT
Date Accepted for Filing:	7/12/2022 8:54:31 AM AEDT
File Number:	NSD1046/2022
File Title:	CHIEF EXECUTIVE OFFICER OF THE AUSTRALIAN TRANSACTION REPORTS AND ANALYSIS CENTRE v SKYCITY ADELAIDE PTY LTD ABN 72 082 362 061
Registry:	NEW SOUTH WALES REGISTRY - FEDERAL COURT OF AUSTRALIA

Registrar

Important Information

This Notice has been inserted as the first page of the document which has been accepted for electronic filing. It is now taken to be part of that document for the purposes of the proceeding in the Court and contains important information for all parties to that proceeding. It must be included in the document served on each of those parties.

The date of the filing of the document is determined pursuant to the Court's Rules.

Form 17
Rule 8.05(1)(a)

STATEMENT OF CLAIM

FEDERAL COURT OF AUSTRALIA
DISTRICT REGISTRY: NEW SOUTH WALES
DIVISION: COMMERCIAL AND CORPORATIONS **NO NSD OF 2022**

CHIEF EXECUTIVE OFFICER OF THE AUSTRALIAN TRANSACTION REPORTS AND ANALYSIS CENTRE
Applicant

SKYCITY ADELAIDE PTY LTD
ABN: 72 082 362 061
Respondent

INDEX

Filed on behalf of the Applicant, the Chief Executive Officer of the Australian Transaction Reports and Analysis Centre

Prepared by: Sonja Marsic
AGS lawyer within the meaning of s 55I of the *Judiciary Act 1903*

Address for Service:
The Australian Government Solicitor,
Level 10, 60 Martin Place, Sydney, NSW 2000
Sonja.Marsic@ags.gov.au

File ref: 22008262

Telephone: 02 958 17505
Lawyer's Email:
Sonja.Marsic@ags.gov.au
Facsimile: 02 9581 7650

PARTIES

The Chief Executive Officer of AUSTRAC

1. The Applicant is the Chief Executive Officer (**CEO**) of the Australian Transaction Reports and Analysis Centre (**AUSTRAC**) an office established under s 211 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (the **Act**).

2. The AUSTRAC CEO may apply for a civil penalty order by reason of s 176 of the Act.

3. The objects of the Act, among others, include to provide for measures to detect, deter and disrupt money laundering, the financing of terrorism and other serious financial crimes.

Particulars

Section 3(1)(aa) of the Act.

4. The objects of the Act, among others, also include to promote confidence in the Australian financial system through the enactment and implementation of controls and powers to detect, deter and disrupt money laundering, terrorism financing and other serious crimes.

Particulars

Section 3(1)(ad) of the Act.

5. The AUSTRAC CEO may, by writing, make rules prescribing matters required or permitted by any provision of the Act to be prescribed by the Rules.

Particulars

Section 229 of the Act.

Anti-Money Laundering and Counter-Terrorism Financing Rules 2007 (the **Rules**).

SkyCity Adelaide Pty Ltd

6. The Respondent, SkyCity Adelaide Pty Ltd (**SCA**):

   a. is and was at all material times a company incorporated in Australia;

   b. is and was at all material times a person within the meaning of s 5 of the Act;

   c. at all material times has carried on activities or business through a permanent establishment in Australia for the purposes of the Act;

   d. is and was at all material times a reporting entity within the meaning of s 5 of the Act; and

   e. provides designated services to customers within the meaning of s 6 of the Act, including:

      i. **Item 6, table 1** – making a loan, where the loan is made in the course of carrying on a loans business.

      ii. **Item 7, table 1** – in the capacity of a lender for a loan, allowing the borrower to conduct a transaction in relation to the loan, where the loan was made in the course of carrying on a loans business.

iii. **Item 31, table 1** – in the capacity of a non-financier carrying on a business of giving effect to remittance arrangements, accepting an instruction from a transferor entity for the transfer of money or property under a designated remittance arrangement.

iv. **Item 32, table 1** – in the capacity of a non-financier carrying on a business of giving effect to remittance arrangements, making money or property available, or arranging for it to be made available, to an ultimate transferee entity as a result of a transfer under a designated remittance arrangement.

v. **Item 1, table 3** – receiving or accepting a bet placed or made by a person, where the service is provided in the course of carrying on a gambling business.

vi. **Item 4, table 3** – paying out winnings in respect of a bet, where the service is provided in the course of carrying on a gambling services.

vii. **Item 6, table 3** – accepting the entry of a person into a game, where: (a) the game is played for money or anything else of value; (b) the game is a game of chance or of mixed chance and skill; (c) the service is provided in the course of carrying on a gambling business; and (d) the game is not played on a gaming machine located at an eligible gaming machine venue.

viii. **Item 7, table 3** – exchanging money or digital currency for gaming chips or tokens or betting instruments, where the service is provided in the course of carrying on a business.

ix. **Item 8, table 3** – exchanging gaming chips or tokens or betting instruments, for money or digital currency, where the service is provided in the course of carrying on a business.

x. **Item 9, table 3** – paying out winnings, or awarding a prize, in respect of a game, where: (a) the game is played for money or anything else of value; (b) the game is a game of chance or of mixed chance and skill; (c) the service is provided in the course of carrying on a gambling business; and (d) the game is not played on a gaming machine located at an eligible gaming machine venue.

xi. **Items 11 to 13, table 3** – in the capacity of account provider:

A. opening an account; or

B. allowing a person to be a signatory to an account; or

C. allowing a transaction to be conducted in relation to an account,

where the account provider is a person who provides a service covered by items 1, 2, 3, 4, 6, 7, 8 or 9 of table 3, and the purpose, or one of the purposes, of the account is to facilitate the provision of a service covered by items 1, 2, 3, 4, 6, 7, 8 or 9 of table 3, and the service is provided in the course of carrying on a gambling business.

xii. **Item 14, table 3** – exchanging one currency (whether Australian or not) for another (whether Australian or not), where the exchange is provided by a person who provides a service covered by items 1, 2, 3, 4, 6, 7, 8 or 9 of item 3, and the service is provided in the course of carrying on a business.

SkyCity Entertainment Group Limited

7. At all relevant times SkyCity Entertainment Group Limited (**SCEG**) was the parent company of SCA.

Particulars

See paragraphs 158 and 159.

THE ML/TF RISKS FACED BY SCA

8. Money laundering:

   a. is the process of turning the proceeds of crime into money that appears to be legitimate;

   b. aims to conceal the identity, source, and destination of illicitly-obtained money; and

   c. aims to move illicitly-obtained money through a legitimate business or transfer system.

9. The Act requires reporting entities to identify, mitigate and manage the money laundering and terrorism financing (**ML/TF**) risks reasonably faced with respect to the provision of designated services to customers.

Particulars

See paragraphs 29 to 41.

10. The ML/TF risks faced by SCA arise from both:

   a. the provision of gambling services (table 3, s 6 designated services); and

   b. the movement of money facilitated by the provision of financial services (table 1, s 6 designated services).

The risk-based approach and ML/TF risk

11. The Act and Rules permit a risk-based approach to the identification, mitigation and management of ML/TF risks by reporting entities.

12. When determining and putting in place appropriate risk-based systems and controls, a reporting entity must have regard to the nature, size and complexity of its business and the type of ML/TF risk it might reasonably face.

Particulars

Rule 8.1.3 of the Rules.

13. In identifying, mitigating and managing ML/TF risks, a reporting entity must consider the risk posed by:

   a. its customer types, including any politically exposed persons (**PEPs**);

   b. the types of designated services it provides;

   c. the methods by which it delivers designated services (which is known as channel risk); and

   d. the foreign jurisdictions with which it deals.

Particulars

Sections 84(2)(a) and (c) of the Act and r 8.1.4 of the Rules.

The nature, size and complexity of SCA's business and ML/TF risks reasonably faced

14. SCA facilitate high volume, high frequency and high value designated services, almost 24 hours a day, and 7 days a week, including across international borders.

15. From 7 December 2016 to about 17 November 2022, each version of SCA's AML/CTF Programs recorded that the SCA casino attracts an average of 5,500 visitors per day and provides gambling services from up to 200 tables and up to 1,500 gaming machines in multiple locations within the venue, and that the casino generates international, interstate and local business.

16. The proceeds of crime are often in cash.

17. The casino operated by SCA is vulnerable to laundering of proceeds from a range of serious and organised crime activities including drug and tobacco offences, tax evasion, tax and welfare fraud and illegal gambling because:

    a. they are cash intensive businesses; and

    b. the source and ownership of cash is harder to trace compared to other forms of money.

18. A customer of SCA can move money through different designated services, including by:

    a. transferring money through cash, casino value instruments (**CVIs**), such as chips and tickets, and gaming accounts (table 3, s 6 services);

    b. transferring money to or from their own gaming account (items 32 and 31, table 1, s 6 services, respectively, or **remittance services**); and

    c. drawing on or redeeming credit provided by SCA (item 7, table 1, s 6 services – **loans or credit**), which could be used for table 3, s 6 gambling service and could involve remittance services.

19. The movement of money through different designated services by SCA customers can involve:

    a. long and complex transaction chains; and

    b. multiple channels, including non-face-to-face channels

    which make it difficult to understand the purpose of transactions, the beneficial owner of funds or the ultimate beneficiary of value moved.

20. SCA provided both gambling and financial services to higher risk customers, including:

    a. through junket channels and individual commission programs as pleaded at paragraphs 382 to 430;

    b. to customers from foreign jurisdictions, including international VIPs; and

    c. to PEPs, including foreign PEPs.

21. SCA dealt with customers, including higher risk customers, through agents and third parties.

Money laundering vulnerabilities and typologies

22. The Financial Action Task Force (**FATF**), the Asia/Pacific Group on Money Laundering (**APG**) and AUSTRAC have identified significant money laundering vulnerabilities, related case studies and 'ML/TF typologies' specific to casinos.

23. **ML/TF typologies** are the various methods that criminals use to conceal, launder or move illicit funds.

24. The FATF, APG and AUSTRAC publications describe the following vulnerabilities and ML/TF typologies:

    a. As casinos are cash intensive businesses, they are vulnerable to **structuring**. This is the deliberate diversion of a large amount of cash into smaller deposits to avoid the reporting threshold in s 43 of the Act.

    b. **Cuckoo smurfing** is a method of money laundering used by criminals to move funds across borders and money generated by their illegal activities appear to have come from a legitimate source.

    c. Cuckoo smurfing is facilitated by professional money laundering syndicates who work with a corrupt remitter based overseas:

        i. The corrupt remitter accepts an instruction from a customer to make a payment to an Australian-based beneficiary customer.

        ii. The corrupt remitter hijacks the money transfer coming into Australia in order to place funds in the Australian-beneficiary account which are sourced from criminal activity.

        iii. A **smurf or third party agent**, deposits cash into Australian bank accounts on behalf of a money laundering syndicate controller.

        iv. The international transfer is offset without the physical movement of funds.

    d. Casinos accepting cash or third party deposits for customers are vulnerable to cuckoo smurfing.

    e. Designated services facilitated through junkets are vulnerable to cuckoo smurfing and structuring. Junket operators may act as remitters and may facilitate cuckoo smurfing.

    f. **Offsetting** enables the international transfer of value without actually transferring money. This is possible because the arrangement involves a financial credit and debit (offsetting) relationship between two or more persons in different countries. Criminals can exploit offsetting to conceal the amount of illicit funds transferred, obscure the identity of those involved and avoid reporting to AUSTRAC.

    g. Gaming accounts are vulnerable to offsetting.

    h. **Loans or credit** can also be used to launder funds. Loans can be taken out as a cover for laundering criminal proceeds under the guise of repayments, including by lump sum cash payments, smaller structured cash amounts or offsetting.

    i. Customers of casinos may seek to use third parties to obtain designated services on their behalf. Third parties may also seek to deposit money into a customer's gaming account. A customer may seek to transfer money from their gaming account to a third party. The involvement of third parties in transactions such as these can distance

customers from illicit funds, disguise ownership of funds and complicate asset confiscation efforts by authorities. Third parties can also be used as smurfs.

j. Money deposited with a casino or exchanged for CVIs (including chips and tickets) and then withdrawn with **minimal or no gaming activity** may appear to have a legitimate origin, even though very little money was actually risked.

k. Gambling losses sustained by a customer, even if minimal, can give the incorrect appearance that the customer is engaging in genuine gambling activity.

l. Gambling involving **high turnover or high losses** may indicate unusual or suspicious activity and may raise questions about the customer's source of wealth or funds.

m. Gambling involving **escalating rates of high turnover or high losses** may indicate unusual or suspicious activity and may raise questions about the customer's source of wealth or funds.

Particulars

Turnover is the total amount wagered by customers at a table or gaming machine.

Paragraphs 386 and 423 particularises how commissions were calculated on turnover.

n. **High turnover** offers further opportunities for the **placement and layering of illicit funds**. This is a particular problem with junkets, where funds are pooled and the payment of winnings facilitated by the junket operator. The problem is exacerbated where cash can be brought into private gaming rooms by unknown persons who are not junket players.

o. Games that have a **low house edge** can be attractive to money launderers, as they offer the opportunity to launder large amounts with minimised losses. The house edge is a term used to describe the mathematical advantage that a game, and therefore the casino, has over the customer with play over time.

p. Where games permit **even-money wagering** (such as roulette and baccarat), two customers can cover both sides of an event bet to give the appearance of legitimate gambling activity while minimising losses.

q. Games that permit **rapid turnover of cash or CVIs** are vulnerable to money laundering. This vulnerability is exacerbated where the game is automated and not face-to-face.

r. **Chips and other CVIs are highly transferable** and may be handed over to third parties or removed from casinos and used as currency by criminal groups, or taken out of the jurisdiction as a means of transferring value. The chips may be returned to the casino by third parties and cashed out, including in amounts below a reporting threshold.

s. **Purchase of CVIs** such as tickets means a money laundering typology whereby individuals purchase CVIs from other customers using illegitimate funds and claim winnings from the Cage.

t. The acceptance of **bank cheques** made out to casinos may facilitate money laundering. Bank cheques are essentially anonymised, as the casino cannot identify

the source of the funds. A customer may use the bank cheque to purchase CVIs, which may then be converted to cash.

u. **Bill stuffing** involves a customer putting cash into an electronic gaming machine (**EGM**), collecting tickets with nominal gambling activity, then cashing out or asking for a cheque.

v. Casinos are also vulnerable to **refining**, which involves changing of an amount of money from smaller denomination bills into larger ones.

w. **Loan sharking** is when a person lends money in exchange for its repayment at an excessive interest rate, and may involve intimidating or illegal methods to obtain repayment. Although there is no specific offence for loan sharking, the conduct of a loan shark may breach other laws.

x. Money may be **parked** in gaming accounts. Parking of illicit money puts distance between the act or acts that generated the illicit funds and the ultimate recipients of those funds, making it harder to understand or trace the flow of money. Gaming accounts can be used to park or hide funds from law enforcement and relevant authorities.

Particulars

Vulnerabilities of Casinos and Gaming Sector, FATF/APG Report, (March 2009), (**FATF/APG Casino Typologies Report**).

Detect and Report Cuckoo Smurfing: Financial Crime Guide, (June 2021), AUSTRAC and Fintel.

Junket Tour Operations in Australia: Money Laundering and Terrorism Financing Risk Assessment, (2020), AUSTRAC (**AUSTRAC Junket Assessment**).

FATF - Risk Based Approach Guidance for Casinos, (October 2008) (**FATF RBA Guidance**).

25. At all times, SCA was exposed to the vulnerabilities and ML/TF typologies pleaded at paragraph 24 with respect to the provision of designated services.

26. By reason of the matters pleaded at paragraphs 14 to 25, the provision of designated services by SCA involves higher ML/TF risks.

THE AML/CTF PROGRAM

27. A reporting entity must not commence to provide a designated service to a customer unless the reporting entity has adopted and maintains an anti-money laundering and counter-terrorism financing program (**AML/CTF program**), within the meaning of s 83 of the Act, that applied to the reporting entity.

Particulars

Sections 81(1) and 83 of the Act and rule 1.2.1 of the Rules.

28. An AML/CTF program is relevantly defined to include a standard AML/CTF Program.

Particulars

Section 83(1)(a) of the Act.

STANDARD AML/CTF PROGRAM

29. A standard AML/CTF Program is:

    a. a written program that applies to a particular reporting entity; and

    b. divided into Part A (general) and Part B (customer identification).

Particulars

Section 84(1) of the Act.

30. Part A of a standard AML/CTF program is a part the primary purpose of which is to:

    a. identify; and

    b. mitigate; and

    c. manage;

    the risk the reporting entity may reasonably face that the provision by the reporting entity of designated services at or through a permanent establishment of the relevant reporting entity in Australia might (whether inadvertently or otherwise) involve or facilitate money laundering or financing of terrorism (**ML/TF risk**).

Particulars

Section 84(2)(a) of the Act.

31. Part A of a standard AML/CTF program must comply with the Rules.

Particulars

Section 84(2)(c) of the Act.

32. Part B of a standard AML/CTF program has the sole or primary purpose of setting out the applicable customer identification procedures (**ACIPs**) for the purposes of the application of the Act to customers of the reporting entity.

Particulars

Section 84(3)(a) of the Act.

33. Part B of a standard AML/CTF program must comply with the Rules.

Particulars

Section 84(3)(b) of the Act.

The Rules – The Part A Program

34. Section 84(2)(c) of the Act requires a Part A program to comply with requirements specified in the Rules including:

    a. rule 8.1.3 which requires a reporting entity, when putting in place appropriate risk-based systems or controls, to have regard to the nature, size and complexity of the reporting entity's business and the type of ML/TF risk that the reporting entity might reasonably face;

    b. rule 8.1.4 which requires a reporting entity in identifying its ML/TF risk to consider the following factors:

i. its customer types, including any PEPs;

ii. the types of designated services it provides;

iii. the methods by which it delivers designated services; and

iv. the foreign jurisdictions with which it deals;

c. rule 8.1.5 which requires the Part A program to be designed in a way so as to enable the reporting entity to:

i. understand the nature and purpose of the business relationship with its customer types;

ii. understand the control structure of non-individual customers;

iii. identify significant changes in ML/TF risk for the purposes of its Part A and Part B programs, including (a) risks identified by consideration of the factors in rule 8.1.4 and (b) risks arising from the changes in the nature of the business relationship, control structure, or beneficial ownership of its customers;

iv. recognise such changes in ML/TF risk for the purposes of the requirements of its Part A and Part B programs; and

v. identify, mitigate and manage any ML/TF risk arising from: (a) all new designated services prior to introducing them to the market; (b) all new methods of designated service delivery prior to adopting them; (c) all new or developing technologies used for the provision of a designated service prior to adopting them; and (d) changes arising in the nature of the business relationship, control structure or beneficial ownership of its customers;

d. rule 8.4.1 which requires a reporting entity's Part A program to be approved by its governing board and senior management. The Part A program must also be subject to the ongoing oversight of the reporting entity's board and senior management; and

e. rule 8.5.1 which requires the Part A program to provide for the reporting entity to designate a person as the AML/CTF Compliance Officer (**AMLCO**) at the management level.

The Rules – Carrying out the applicable customer identification procedures and the Part B Program

35. Reporting entities are required to carry out ACIPs to identify customers, generally before commencing to provide a designated service.

Particulars

Section 32 of the Act.

36. Exceptions to this general rule apply in relation to some designated services provided by SCA.

Particulars

Chapter 10 of the Rules made under s 39 of the Act.

37. Chapter 10 of the Rules relevantly provides:

a. The obligation in s 32 of the Act does not apply in respect of a designated service under items 1, 2, 4, 6, 7, 8 or 9 of table 3, s 6 that involves an amount less than $10,000.

Particulars

Rule 10.1.4 of the Rules (from 7 December 2016 to 16 June 2021).

Rule 10.1.3 of the Rules (from 17 June 2021).

b. The obligation in s 32 of the Act does not apply in respect of a designated service under items 1, 2, 4, 6 or 9 of table 3, s 6 that involves:

i. an amount of $10,000 or more; and

ii. the customer giving or receiving only gaming chips or tokens.

Particulars

Rule 10.1.5 of the Rules (from 7 December 2016 to 16 June 2021).

Rule 10.1.4 of the Rules (from 17 June 2021).

38. The exemptions in rules 10.1.4 and 10.1.5 (from 7 December 2016 to 16 June 2021) and rules 10.1.3 and 10.1.4 (from 17 June 2021) do not apply in circumstances where a reporting entity determines in accordance with its enhanced customer due diligence (**ECDD**) program that it should obtain and verify any know your customer (**KYC**) information in respect of a customer in accordance with its customer identification program.

Particulars

Rule 10.1.6 of the Rules (from 7 December 2016 to 16 June 2021).

Rule 10.1.5 of the Rules (from 17 June 2021).

39. Rule 14.4 of the Rules relevantly provides that the obligation in s 32 of the Act does not apply to a designated service under item 14, table 3, s 6 (foreign exchange):

a. where the value of currency is less than $1,000 (in Australian dollars or foreign equivalent); and

b. the proceeds and/or funding source of the designated service is in the form of physical currency.

40. The exemption in rule 14.4 does not apply where a reporting entity determines in accordance with its ECDD program that it should obtain and verify any KYC information about a customer in accordance with its customer identification program.

Particulars

Rule 14.5 of the Rules.

41. Section 84(3)(b) of the Act requires a Part B program to comply with the requirements specified in Chapter 4 of the Rules, which includes the following:

a. Rule 4.1.3 provides that for the purposes of meeting the requirements of Chapter 4 of the Rules, a reporting entity must consider the risk posed by the following facts when identifying its ML/TF risk:

i. its customer types, including any PEPs;

ii. its customers' source of funds and wealth;

iii. the nature and purpose of the business relationship with its customers;

iv. the types of designated services it provides;

v. the methods by which it delivers designated services (or channel); and

vi. the foreign jurisdictions with which it deals.

b. Rule 4.2.2 requires a Part B program to include appropriate risk-based systems and controls that are designed to enable the reporting entity to be reasonably satisfied that a customer who is an individual is the individual that he or she claims to be.

c. Rule 4.2.3 requires a Part B program to include a procedure for the reporting entity to collect, at a minimum, the following KYC information about an individual: full name, date of birth, and residential address.

d. Rule 4.2.5 requires a Part B program to include appropriate risk-based systems and controls for the reporting entity to determine whether any other additional KYC information will be collected in addition to this information.

e. Rule 4.2.6 requires a Part B program to include a procedure for the reporting entity to verify, at a minimum, the customer's full name and either the customer's date of birth or their residential address.

f. Rule 4.2.8 requires a Part B program to include appropriate risk-based systems and controls for the reporting entity to determine whether any additional KYC information should be verified.

g. Rules 4.2.10 to 4.2.14 set out 'safe harbour' ACIPs for individual customers whose risk is medium or lower.

h. Part 4.11 makes provision for ACIPs for agents of customers.

i. Rule 4.11.2 requires a Part B program to include a procedure for the reporting entity to collect, at a minimum:

   i. the full name of each individual who purports to act for or on behalf of the customer with respect to the provision of a designated service by the reporting entity; and

   ii. evidence (if any) of the customer's authorisation of any such individual.

j. Rule 4.11.3 requires a Part B program to include appropriate risk-based systems and controls for the reporting entity to determine whether and to what extent it should verify the identity of individuals (either the customer or their purported agents).

k. Part 4.13 of the Rules provides for the collection and verification of PEP information.

l. Rule 4.13.1 requires a Part B program to include appropriate risk-management systems to determine whether a customer or beneficial owner is a PEP; either before the provision of a designated service to the customer or as soon as practicable after the designated service has been provided.

m. For domestic PEPs and international organisation PEPs, r 4.13.2 requires a Part B program to determine whether the person is of high ML/TF risk.

n. If the person is a domestic PEP or international organisation PEP who has been assessed as posing a high ML/TF risk, or if the person is a foreign PEP, then rr 4.13.2(3) and 4.13.3 respectively require a Part B program to include appropriate risk-management systems for the reporting entity to undertake each of the following steps:

i. comply with identification requirements in rules 4.2.3 to 4.2.9 of the Rules in the case of a beneficial owner;

ii. obtain senior management approval before establishing or continuing the business relationship;

iii. take reasonable measures to establish the PEP's source of wealth and source of funds; and

iv. comply with Chapter 15 of the Rules.

THE SCA AML/CTF PROGRAM

42. At all times on and from 7 December 2016, SCA could not commence to provide a designated service to a customer unless it adopted and maintained a standard AML/CTF program.

Particulars

Sections 81(1), 83 and 84 of the Act.

Section 81(1) is a civil penalty provision: s 81(2) of the Act.

SCA's Standard AML/CTF Program

43. For the period from 7 December 2016 to on or about 17 November 2022, SCA purported to adopt and maintain a standard AML/CTF program that included a Part A (the **Standard Part A Programs**).

Particulars

The SCA Standard Part A Programs comprised:

The program effective from 9 February 2015 to 6 February 2017, sections 1 to 19 (the **2015 Standard Part A Program**);

The program effective from 7 February 2017 to 6 February 2018, sections 1 to 15 (the **2017 Standard Part A Program**);

The program effective from 7 February 2018 to 16 April 2019, sections 1 to 15 (the **2018 Standard Part A Program**);

The program effective from 17 April 2019 to 15 February 2021, sections 1 to 15 (the **2019 Standard Part A Program**);

The program effective from 16 February 2021 to 8 June 2021, sections 1 to 15 (the **February 2021 Standard Part A Program**);

The program effective from 9 June 2021, sections 1 to 15 (the **June 2021 Standard Part A Program**);

The program effective from 28 October 2021, sections 1 to 15 (the **October 2021 Standard Part A Program**).

44. On or about 17 November 2022, the SCA Board and SCA senior management approved a standard Part A Program (the **November 2022 Standard Part A Program**).

45. For the period from 7 December 2016, SCA purported to adopt and maintain a standard AML/CTF program that included a Part B (the **Standard Part B Programs**).

Particulars

The SCA Standard Part B Programs comprised:

The program effective from 9 February 2015 to 6 February 2017, sections 20 to 25 (the **2015 Standard Part B Program**);

The program effective from 7 February 2017 to 18 June 2017, sections 16 to 20 (the **2017 Standard Part B Program**);

The program effective from 19 June 2017 to 6 February 2018, sections 16 to 20 (the **Amended 2017 Standard Part B Program**);

The program effective from 7 February 2018 to 16 April 2019, sections 16 to 20 (the **2018 Standard Part B Program**);

The program effective from 17 April 2019 to 15 February 2021, sections 16 to 20 (the **2019 Standard Part B Program**);

The program effective from 16 February 2021 to 8 June 2021, sections 16 to 20 (the **February 2021 Standard Part B Program**);

The program effective from 9 June 2021, sections 16 to 20 (the **June 2021 Standard Part B Program**);

The program effective from 28 October 2021, sections 16 to 20 (the **October 2021 Standard Part B Program**);

The program approved by the SCA Board and SCA senior management on or about 17 November 2022 (the **November 2022 Standard Part B Program**)

The November 2022 Standard Part B Program is identical to the October 2021 Standard Part B Program.

SCA'S INFORMATION MANAGEMENT SYSTEMS

46. SCA had multiple information management systems to record information relevant to its customers and the provision of designated services.

47. From 8 July 2012, SCA used a suite of programs under the Bally Gaming System (**Bally**).

48. **Bally CMP** was used to:

a. record:

i. rated gambling activity on EGMs and table games;

ii. transaction history, including transactions conducted at a gambling table such as 'Cash Buy In' and 'Chip Buy In' against a customer's profile when using their loyalty card;

iii. transactions relating to a customer's Front money account (**FMA**);

iv. information relating to a customer's risk rating (against a player's profile);

v. loyalty program status and history;

vi. customer identification and KYC information records (against a customer's player profile), including a copy of the photo identification provided by the customer and any discrepancy that arose during the course of verifying KYC information;

Particulars

Section 15, paragraph 3 and section 16, paragraph 14 of the 2017-2021 Standard Part A Programs.

vii. the customer's occupation details (if provided);

Particulars

Section 16, paragraphs 15-16 of the 2017-2021 Standard Part A Programs.

viii. notes entered by frontline staff;

ix. VIP sponsorship history;

x. information relating to ongoing customer due diligence or ECDD carried out with respect to a customer (against a customer's player profile); and

xi. from February 2017, whether an agent was acting on behalf of a customer in relation to a designated service, which could be used as authorisation with respect to the provision of further designated services;

Particulars

Section 17, paragraph 6 of the 2017-2021 Standard Part A Programs.

b. create new loyalty accounts; and

c. create tags to record if the customer was a match for a PEP, relative or close associate (**RCA**), or a special interest person (**SIP**).

49. **Bally Cage** was used to:

a. record transactions performed at the Cage when linked to a customer's account, including:

i. FMA deposits and withdrawals, including electronic bank transfers and inter-company (between SCEG and SCA) transfers;

ii. chip purchases and redemptions;

iii. ticket-in ticket-out (**TITO**) ticket issues and redemptions;

iv. hand-pay slip redemptions; and

v. chip purchase voucher (**CPV**) purchases and redemptions;

b. record transactions that could be identified as threshold transactions; and

Particulars

Section 11, paragraphs 9-10 of the 2017-2021 Standard Part A Programs.

c. manage inventory, including cash, chips and cheques.

50. Slot Data System **(SDS)**, which had the primary function of slot accounting and player tracking, including recording the following gambling activity on EGMs or electronic table games (**ETGs**):

    a. machine turnover;

    b. credits won;

    c. games played;

    d. cash inserted or collected;

    e. funds transferred via cashless;

    f. funds removed; and

    g. jackpots won.

51. When a customer was playing on an EGM or an ETG and was using their membership card, SDS transferred the data collected in relation to the customer's gambling activity to the customer's profile in Bally.

52. Bally Cage interfaced with Bally CMP such that any transactions of $10,000 or more recorded in Bally Cage would be recorded against the customer's profile.

53. Data from Bally was also used to manually generate transaction monitoring reports for SCA's transaction monitoring program.

54. From March 2015, SCA used the **Jade** system (previously named Wynyard) to:

    a. record:

        i. information relating to a customer's risk rating;

        ii. customer identification and KYC information;

        iii. PEP screening records*;*

Particulars

Section 15, paragraph 5 of the 2017-2021 Standard Part A Programs.

        iv. transaction history;

Particulars

Section 11, paragraph 5 of the 2017-2021 Standard Part A Programs.

        v. TTR submission history against a customer's profile;

        vi. IFTI history against a customer's profile (after January 2021);

        vii. certain customer due diligence (**CDD**) information;

        viii. loyalty program and status history; and

        ix. rule alert history, including the results of reviews of transaction alerts;

    b. generate the following reports and alerts through a combination of automated and manual processes:

        i. possible PEP matches and adverse media in relation to SCA customers;

Particulars

Section 19, paragraph 6 of the 2017-2021 Standard Part A Programs

ii. transaction alerts triggered by transaction rules; and

Particulars

Section 13, paragraphs 5-8 of the 2017-2021 Standard Part A Programs.

iii. template reports in relation to TTRs and IFTIs for uploading to AUSTRAC. From November 2020, SCA moved to an automated IFTI reporting process.

55. From 11 November 2015, SCA used **iTrak** to:

a. record, relevantly:

i. incident files and records relating to potentially suspicious matters*;*

Particulars

Section 11, paragraph 5 of the 2017-2021 Standard Part A Programs.

ii. customer identification and KYC information records (for subject profiles);

iii. information relating to customer PEP screening;

iv. incidents recorded by the surveillance department and security department in the form of incident files, audits and daily logs;

v. source of funds and source of wealth information (where provided);

vi. information relating to ongoing customer due diligence or ECDD carried out with respect to a customer (for subject profiles); and

Particulars

Section 14, paragraph 9 of the 2017-2021 Standard Part A Programs.

vii. transactions monitored or logged by the surveillance department;

b. store records of SMRs provided to AUSTRAC.

Particulars

Section 13, paragraph 9 of the 2017-2021 Standard Part A Programs.

56. At all times, an iTrak profile would be created for a customer only if they were the subject of a surveillance, security, host responsibility or compliance related incident (where the latter included being the subject of an observation report, an AML investigation, a positive PEP screening match, an SMR report or an AML-related barring).

57. iTrak was not synchronised with or linked to Bally or Jade.

58. From 4 June 2014, SCA also used its **network drives** to, relevantly:

a. record:

i. information relating to a customer's risk rating, including records relating to ongoing customer due diligence or ECDD carried out with respect to a customer;

ii. customer identification and KYC information records;

iii. information relating to customer PEP screening, including the results of a manual check of the Dow Jones database for Junket operators, representatives and players;

iv. source of funds and source of wealth information (when provided); and

v. results of system-generated reviews of transactions (other than reviews generated by Jade);

b. store records of SMRs provided to AUSTRAC.

59. Prior to November 2015 and the introduction of iTrak, SCA used **iBase** as its incident management system, which included recording SMRs submitted with respect to certain customers.

60. Until January 2021, SCA manually entered records from IFTI reports into iBase. From January 2021, IFTI records were recorded and managed in Jade.

61. From June 2016, frontline employees used **Sharepoint** to submit observation forms to the AML team, which would generate an email to the AML team.

Particulars

From 7 December 2016 until about November 2021, **the AML team** included the:

i. AMLCO;

ii. AML Analyst;

iii. Compliance Manager up until 1 July 2017l and

iv. AML Compliance Manager from 5 April 2021.

See also particulars to paragraph 453.

62. Deficiencies with SCA's information management systems and record-keeping procedures limited the ability of SCA's transaction monitoring and enhanced customer due diligence to operate as intended.

Particulars

See paragraphs 456 to 474 and 524 to 528.

The procedures, systems and controls in the transaction monitoring program and the ECDD Program were not capable, by design, of operating in the manner described in SCA's AML/CTF Programs due to the deficiencies in information management systems and record keeping.

THE STANDARD AML/CTF PROGRAM CONTRAVENTIONS – SECTION 81

63. A reporting entity cannot adopt and maintain a standard AML/CTF program for the purposes of s 81 of the Act unless it has adopted and maintained both a:

a. standard Part A program; and

b. standard Part B program.

Particulars

Section 84(1) of the Act.

The Standard Part A Program

64. A reporting entity cannot adopt and maintain a standard Part A program for the purposes of s 81 of the Act unless the Part A program complies with the requirements of:

a. section 84(2)(a) of the Act;

b. section 84(2)(c) of the Act; and

c. rules made under s 84(2)(c) of the Act, including Chapters 8 and 15 of the Rules.

65. From 7 December 2016, the SCA Standard Part A Programs and the November 2022 Standard Part A Program did not meet the requirements of s 84(2) of the Act and Chapters 8 and 15 of the Rules because the Standard Part A Programs did not:

a. have the primary purpose of identifying, mitigating and managing the ML/TF risks that SCA reasonably faced and did not comply with the requirements of the Rules.

Particulars

Sections 84(2)(a) and (c) of the Act and rr 8.1.3, 8.1.4, 8.1.5, 8.4 and 8.7 of the Rules.

See paragraphs 74 to 79 and 559 to 562.

b. include a transaction monitoring program that complied with the requirements of the Rules.

Particulars

Section 84(2)(c) of the Act and rr 8.1.3, 8.1.4, and 15.4 to 15.7 of the Rules.

See paragraphs 431 to 495 and 549 to 562.

c. include an enhanced customer due diligence program that complied with the requirements of the Rules.

Particulars

Section 84(2)(c) of the Act and rr 1.2.1 (definition of KYC information), 8.1.3, 8.1.4 and 15.8 to 15.11 of the Rules.

See paragraphs 496 to 528 and 559 to 562.

d. include systems and controls designed to ensure SCA complied with the reporting requirements under Part 3 of the Act.

Particulars

Rule 8.9.1(2) of the Rules, made for the purposes of s 84(2)(c) of the Act.

See paragraphs 529 to 542 and 559 to 562.

66. By reason of the matters pleaded in paragraphs 64 to 65, SCA did not adopt and maintain a Standard Part A program for the purposes of s 81 of the Act from 7 December 2016.

67. By reason of the matters pleaded in paragraphs 6, 63 and 66, SCA commenced to provide designated services from 7 December 2016 in contravention of s 81(1) of the Act.

68. By reason of the matters pleaded in paragraph 67, SCA contravened s 81(1) of the Act on each occasion that it provided a designated service from 7 December 2016.

Particulars

Section 81(1) of the Act is a civil penalty provision: s 81(2) of the Act.

The Standard Part B Programs

69. A reporting entity cannot adopt and maintain a standard Part B program for the purposes of s 81 of the Act unless the Part B program complies with the requirements of:

a. section 84(3)(a) of the Act;

b. section 84(3)(b) of the Act; and

c. rules made under s 84(3)(b) of the Act, including Chapter 4 of the Rules.

70. From 7 December 2016, the SCA Standard Part B Programs did not comply with the requirements of s 84(3) of the Act because it did not:

a. set out the ACIPs for the purposes of the application of the Act to all customers of SCA: s 84(3)(a); and

b. comply with the requirements of Chapter 4 of the Rules made under s 84(3)(b) of the Act.

Particulars

Chapter 10 and rule 14.4

See paragraphs 543 to 557 and 563.

71. By reason of the matters pleaded in paragraph 70, SCA did not adopt and maintain a Standard Part B program for the purposes s 81 of the Act from 7 December 2016.

72. By reason of the matters pleaded in paragraphs 6 and 71, SCA commenced to provide designated services from 7 December 2016 in contravention of s 81(1) of the Act.

73. By reason of the matters pleaded in paragraph 72, SCA contravened s 81(1) of the Act on each occasion that it provided a designated service from 7 December 2016.

Particulars

Section 81(1) of the Act is a civil penalty provision: s 81(2) of the Act.

THE STANDARD AML/CTF PROGRAM CONTRAVENTIONS – S 81

The primary purpose of identifying, mitigating and managing the ML/TF risks reasonably faced

74. From 7 December 2016 to about 17 November 2022, the Standard Part A Programs did not:

a. have the primary purpose of identifying, mitigating and managing the ML/TF risks that SCA reasonably faced with respect to designated services for the purposes of s 84(2)(a); and

b. comply with the requirements specified in the Rules for the purposes of s 84(2)(c)

for the reasons pleaded at paragraphs 75 to 78 below.

75. The Standard Part A Programs did not include an appropriate **risk methodology** that was capable of appropriately identifying and assessing the ML/TF risks of its designated services for the reasons pleaded at paragraphs 80 to 90.

76. The Standard Part A Programs were not **aligned to the ML/TF risks reasonably faced** by SCA with respect to the provision of designated services for the reasons pleaded at paragraphs 91 to 155.

77. The Standard Part A Programs did not include or establish an **appropriate approval and oversight framework** that was capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by SCA and of meeting the requirements of the Rules for the reasons pleaded at paragraphs 156 to 199.

78. The Standard Part A Programs did not include **appropriate risk-based systems and controls** that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by SCA with respect to:

    a. **Front money accounts (FMAs),** for the reasons pleaded at paragraphs 207 to 219;

    b. **Designated services involving third party transactions,** for the reasons pleaded at paragraphs 220 to 231.

    c. **Remittance services,** including with respect to:

        i. transfers through the SCEG Customer account channel for the reasons pleaded at paragraphs 239 to 268; and

        ii. transfers through the SCA Customer account channel for the reasons pleaded at paragraphs 269 to 291;

        iii. transfers through the SkyCity New Zealand channel for the reasons pleaded at 292 to 306

        iv. transfers between FMAs for the reasons pleaded at 307 to 312.

    d. **Loans and transactions relating to loans**, including cheque cashing facilities (CCFs) for the reasons pleaded at paragraphs 313 to 343.

    e. **The exchange of money for casino value instruments such as chips and tickets (and vice-versa),** for the reasons pleaded at paragraphs 344 to 348.

    f. **Table games and electronic gaming machines,** for the reasons pleaded at paragraphs 349 to 355.

    g. **EZYPlay Guest Cards,** for the reasons pleaded at paragraphs 356 to 367.

    h. **Foreign currency exchange**, for the reasons pleaded at paragraphs 368 to 375.

    i. **Designated services provided in cash**, for the reasons pleaded at paragraphs 376 to 381.

    j. **Designated services provided through junket channels,** for the reasons pleaded at paragraphs 382 to 418.

    k. **Designated services provided through individual commission programs**, for the reasons pleaded at paragraphs 419 to 430.

79. From about 17 November 2022, the November 2022 Standard Part A Program did not:

a. have the primary purpose of identifying, mitigating and managing the ML/TF risks that SCA reasonably faced with respect to designated services for the purposes of s 84(2)(a); and

b. comply with the requirements specified in the Rules for the purposes of s 84(2)(c)

for the reasons pleaded at paragraphs 558 to 562 below.

Risk methodologies

80. A standard Part A program will not be capable, by design, of identifying, mitigating and managing ML/TF risks if it does not include an appropriate risk methodology to identify and assess the ML/TF risks of the designated services provided by the reporting entity.

Particulars

Sections 84(2)(a) and (c) of the Act and rr 8.1.3, 8.1.4 and 8.1.5 of the Rules.

81. At all times from 7 December 2016, the Standard Part A Programs did not include or incorporate an appropriate risk methodology that was capable of appropriately identifying and assessing the ML/TF risks of its designated services for the reasons pleaded at paragraphs 82 to 90 below.

Particulars

Sections 84(2)(a) and (c) of the Act and rr 8.1.3, 8.1.4 and 8.1.5 of the Rules.

82. The Standard Part A Programs did not include or incorporate a methodology to appropriately assess the inherent ML/TF risks with respect to designated services.

Particulars

The Standard Part A Programs did not include or incorporate any documented methodology for the assessment, weighting or rating of the inherent risk attributes reasonably faced by SCA with respect to the designated services they provided.

Nor did the Standard Part A Programs include a methodology that covered all relevant inherent risks and associated risk attributes reasonably faced by SCA with respect to each designated service.

The Standard Part A Programs did not include a methodology that had regard to the nature, size and complexity of SCA's business.

In 2018, an external review observed there was no documented methodology or procedure that described how the SCA ML/TF risk assessment was conducted, how those risks were monitored and reassessed and how SCA identified and recognised significant changes in ML/TF risk (the **2018 external review**). It recommended that SCA consider adopting a quantitative risk assessment methodology. While in response to this recommendation SCA amended section 3 of the 2019 Standard Part A Program to provide for a periodic review process, in August 2021, an external review recommended that SCA consider adopting a more comprehensive risk assessment methodology to defend the overall inherent risk

rating and use it as a basis for the controls required and for updating the SCA risk assessment (the **August 2021 external review**). It observed that there may be insufficient controls due to a lack of risk identification.

Rules 8.1.3 and 8.1.4 of the Rules.

See paragraphs 11 to 26.

83. The Standard Part A Programs did not include or incorporate a methodology to appropriately consider the ML/TF risks posed by the types of designated services provided by SCA.

Particulars

There was no methodology that appropriately applied to all designated service types provided by SCA, including both table 1, s 6 financial services and table 3, s 6 gambling services.

Rule 8.1.4(2) of the Rules.

84. The Standard Part A Programs did not include or incorporate a methodology to appropriately consider the risk factor of channel in assessing the ML/TF risks posed by designated services.

Particulars

Rule 8.1.4(3) of the Rules.

85. The Standard Part A Programs did not include or incorporate a methodology to appropriately consider the risk factor of foreign jurisdictions in assessing the ML/TF risks posed by designated services.

Particulars

Rule 8.1.4(4) of the Rules.

From 7 December 2016, SCA did not factor jurisdictional risk into risk assessments for products.

From 7 December 2016, SCA's only method of identifying changes in jurisdictional risk was monitoring changes to Australia's autonomous sanctions via the Department of Foreign Affairs and Trade (**DFAT**) website or FATF lists of non-cooperative countries and territories or high-risk countries.

From 17 September 2019, SCA introduced a one-page 'high-risk jurisdictions' standard operating procedure (**SOP**) to give effect to its procedure of identifying changes in jurisdictional risk.

The SOP did not set out an appropriate methodology to identify, mitigate or manage the risks of a customer being from a high-risk jurisdiction.

The SOP did not address how jurisdictional risk affects the risk assessments for designated services.

86. The Standard Part A Programs did not include or incorporate a methodology to appropriately consider the ML/TF risks posed by customer types receiving designated services:

Particulars

Rule 8.1.4(1) of the Rules.

a. The Standard Part A Programs did not appropriately identify and define the categories of customers that were not low risk.

Particulars

Section 13 of the 2015 Standard Part A Program.

Section 3 and Schedule 1 of the 2017-2021 Standard Part A Programs.

b. The Standard Part A Programs did not include appropriate criteria or risk parameters for categorising customer types who were not low risk.

Particulars

Section 13 of the 2015 Standard Part A Program.

Section 3 and Schedule 1 of the 2017-2021 Standard Part A Programs.

While the Standard Part A Programs did include some criteria to trigger an assessment of a customer's risk rating, many of the criteria were vague and not supported by any guidance regarding their application.

In 2021, an external review observed that some of the risks in the 'customer types' risk assessment in Schedule 1 of the 2017-2021 Standard Part A Programs were more appropriate to the assessment of 'designated services' risks (the **September 2021 external review**).

See *The ML/TF risk factors – customers* below.

c. The Standard Part A Programs did not set appropriate criteria for identifying significant changes to the level of risk posed by different customer types.

87. The Standard Part A Programs did not include or incorporate a methodology to appropriately assess the ML/TF risks reasonably faced by SCA with respect to complex designated service chains, having regard to the nature, size and complexity of its business, including that:

a. during the course of a visit to the casino, customer funds could be moved through cash, gaming chips and gaming accounts (table 3, s 6 services), and transferred to or from third parties in certain circumstances, another casino, or a domestic or foreign bank (items 31 and 32, table 1, s 6 and item 13, table 3 s 6 services);

Particulars

See *Third party deposits* and *Third party transfers* below.

b. the designated services provided to customers could involve long and complex transactional value chains ranging from inwards remittance of money, account management, gambling activities and outward remittance of money; and

c. these transactional chains involved different channels and jurisdictions.

Particulars

Rules 8.1.3 and 8.1.4 of the Rules.

See, for example, *The SCEG Customer account channel* below.

88. The Standard Part A Programs did not include a methodology to assess the residual ML/TF risks of designated services, once risk-based controls had been applied.

Particulars

Rules 8.1.3 and 8.1.4 of the Rules.

89. On 10 June 2022, SCA completed a documented Business Unit and Enterprise ML/TF Risk Assessment Methodology (the **June 2022 ML/TF Risk Methodology**).

90. The June 2022 ML/TF Risk Methodology is yet to be fully articulated and reflected in Standards included or incorporated into SCA's Standard Part A Program.

Particulars

See paragraphs 559 to 561.

Alignment of SCA's Standard Part A Program to ML/TF risk

91. Once a reporting entity identifies the ML/TF risks it reasonably faces, and carries out an assessment of those risks in accordance with an appropriate ML/TF risk methodology, the reporting entity must align its Part A Program to those risks as assessed.

Particulars

Sections 84(2)(a) and (c) and rr 8.1.3 and 8.1.4 of the Rules.

92. In aligning a Part A Program to the ML/TF risks reasonably faced, a reporting entity must have regard to:

a. the nature, size and complexity of its business; and

b. the type of ML/TF risks it reasonably faces.

Particulars

Rule 8.1.3 of the Rules.

93. When having regard to the ML/TF risk it reasonably faces, a reporting entity must have regard to the risk factors of:

a. designated services;

b. customers;

c. channel; and

d. foreign jurisdictions.

Particulars

Rule 8.1.4 of the Rules.

94. The ML/TF risks reasonably faced by SCA with respect to designated services are also dynamic.

95. A reporting entity must review and update ML/TF risk assessments, at intervals that are appropriate having regard to the nature, size and complexity of its business.

Particulars

Rules 8.1.3 and 8.1.5 of the Rules.

96. For the reasons pleaded in paragraphs 97 to 146, at no time were SCA's Standard Part A Programs aligned to the ML/TF risks reasonably faced by SCA having regard to the requirements pleaded at paragraphs 91 to 95.

The risk assessments

97. From 7 December 2016, risk assessments were included or incorporated into the Standard Part A Programs.

98. SCA's risk assessments were contained in:

    a. Appendix B of the 2015 Standard Part A Program;

    b. Section 3, Schedule 1 and Schedule 1A of the 2017-2021 Standard Part A Programs; and

    c. a separate risk assessment was conducted In October 2020, with respect to the use of TITOs through electronic gaming machines, but not included in the Standard Part A Programs.

    (the **Risk Assessments**).

99. The Risk Assessments purported to set out SCA's risk assessment, including an assessment of the following factors:

    a. the nature, size and complexity of SCA's business;

    b. SCA's customer types;

    c. the sources of funds and source of wealth of customers;

    d. the nature and purpose of the business relationship with customers;

    e. the types of designated services provided by SCA;

    f. the delivery of the designated services;

    g. SCA's dealings with foreign jurisdictions; and

    h. new methods of delivering designated services and/or technologies used for the provision of a designated service, prior to adoption.

100. The Risk Assessments did not clearly articulate or assess a number of the ML/TF risks that SCA might reasonably have faced with respect to the provision of designated services, including for the reasons pleaded at paragraphs 101 to 113.

101. The Risk Assessments did not appropriately assess or describe a number of ML/TF risks that SCA might reasonably have faced with respect to the types of designated services it provided, including risks with respect to different product or designated services types.

Particulars

The Risk Assessments did not assess individual games provided by SCA.

The Risk Assessments did not assess the provision of loans (items 6 and 7, table 1, s 6) or remittance services (items 31 and 32, table 1, s 6) by SCA.

Appendix B of the 2015 Standard Part A Program set out some ML/TF risks of groups of designated services and Attachment 1 set out some ML/TF typologies and methods with respect to some designated services. However, the 2015 Standard Part A Program did not identify all the ML/TF typologies pleaded at paragraph 24 and did not assess the ML/TF risks identified in accordance with an appropriate methodology or clearly articulate those ML/TF risks with respect to different product types.

Schedule 1 of the 2017-2021 Standard Part A Programs allocated risk ratings to some red flag indicators relating to FMAs, currency exchange, receiving or accepting a bet and exchanging chips. However, the assessment of ML/TF risks was limited, and did not include an assessment of appropriate risk-based controls to mitigate those ML/TF risks and an assessment of the level of residual ML/TF risks.

102. The Risk Assessments did not appropriately assess or describe the ML/TF risks that SCA might reasonably face with respect to customer types.

Particulars

Paragraphs 44 to 54 of Appendix B of the 2015 Standard Part A Program sets out some customer-related ML/TF risks. However, it did not appropriately assess the ML/TF risk of customer types or provide a framework that enabled SCA to appropriately categorise and rate the risks posed by different types of customers.

Section 3 and Schedule 1 of the 2017-2021 Standard Part A Programs also set out risk ratings for some customer types. However, SCA did not identify all customer types.

103. The Risk Assessments did not appropriately assess or describe all delivery methods or channels through which SCA provided designated services, including:

a. the junket channel;

b. the SCEG Customer account channel;

c. the SCA Customer account channel;

d. the SkyCity New Zealand channel; and

e. private gaming rooms.

Particulars

Appendix B of the 2015 Standard Part A Program and Section 3 of the 2017-2021 Standard Part A Programs, including Schedules 1 and

1A, did not consider junkets, the SCEG Customer account channel or SkyCity New Zealand channel as channels through which SCA provided designated services.

Paragraph 25, Appendix B of the 2015 Standard Part A Program identified that designated services could be provided through the SCA Customer account channel. However, SCA did not appropriately define the ML/TF risk attributes associated with this channel.

Paragraph 25 of Appendix B of the 2015 Standard Part A Program stated that the SCA Customer account channel was the one exception to providing its designated services face-to-face.

Section 3 of the 2017-2021 Standard Part A Programs stated that SCA delivered its designated services face-to-face. It did not acknowledge or identify which designated services it provided via non-face-to-face channels.

At no time did the Risk Assessments or the Standard Part A Programs consider the ML/TF risks associated with the provision of designated services in private gaming rooms.

104. The Risk Assessments did not clearly articulate or assess ML/TF risks SCA might reasonably have faced with respect to the provision of designated services and the risk factor of jurisdiction.

Particulars

See *The ML/TF risk factors – jurisdiction* below.

105. The Risk Assessments did not appropriately assess or describe the ML/TF risks that SCA might reasonably face with respect to new methods of delivering designated services and/or technologies used for the provision of designated services.

Particulars

See *Changing or emerging ML/TF risks – reviewing and updating ML/TF risk assessments and controls* below.

106. The Risk Assessments did not clearly articulate or assess all ML/TF typologies and vulnerabilities (as defined at paragraph 24) that SCA might reasonably have faced with respect to the provision of designated services, including but not limited to:

a. structuring;

b. cuckoo smurfing;

c. money parked in FMAs;

d. loan sharking;

e. customers attempting to deposit front money or make payments using complex means;

f. the involvement of third parties in relation to customer transactions;

Particulars

Appendix E of the 2015 Standard Part A Program identified the involvement of third parties in relation to customer transactions as a

suspicious indicator for reporting SMRs. However, SCA did not appropriately assess the risk of third parties with respect to customer transactions in relation to all designated services. For example, the Risk Assessments did not address the use of third parties to repay CCFs.

g. offsetting;

h. customer requests for transfers to and from other casinos; and

i. misuse of CVIs.

Particulars

Appendix B, paragraph 55 of the 2015 Standard Part A Program and section 3, paragraph 20 of the 2017-2021 Standard Part A Programs identified some factors relevant to the ML/TF risk posed by SCA's designated services, including the use of CVIs. However, SCA did not appropriately assess the ML/TF risk of CVIs and did not include or incorporate appropriate risk-based controls in relation to the misuse of CVIs.

107. The Risk Assessments were not carried out in accordance with an appropriate risk methodology.

Particulars

See *Risk methodologies* above.

108. The Risk Assessments did not provide a basis for a determination that SCA's overall inherent ML risk was medium.

Particulars

Appendix B, paragraph 11 of the 2015 Standard Part A Program and Section 3, paragraph 6 of the 2017-2021 Standard Part A Programs assessed SCA's inherent ML risk as medium.

109. The Risk Assessments did not assess the effectiveness of any risk-based controls that were intended to identify, mitigate and manage the ML/TF risks reasonably faced by SCA.

110. The Risk Assessments did not include any assessment or determination of SCA's residual risk.

111. In or around May 2022, as part of its AML Enhancement Programme, SCA introduced the following ML/TF risk assessments:

a. Table games ML/TF risk assessment,

b. Player Programs ML/TF risk assessment,

c. Loyalty Rewards ML/TF risk assessment,

d. EGM ML/TF risk assessment,

e. Cage ML/TF risk assessment,

f. Enterprise wide AML/CTF risk assessment

(the **2022 Risk Assessments**).

112. At no time were the controls under the:

a. October 2021 Standard Part A Program aligned to the 2022 Risk Assessments; or

b. November 2022 Standard Part A Program aligned to the 2022 Risk Assessments.

Particulars

See *The November 2022 Standard Part A Program* below.

113. The 2022 Risk Assessments did not include any determination of SCA's residual risk.

Particulars

The operational control effectiveness of the Standard Part A Program was not assessed. Overall control effectiveness was rated as not mitigating.

The ML/TF risk factors

The ML/TF risk factors - designated services

114. The risk-based systems and controls in the Standard Part A Programs were not aligned to the ML/TF risks reasonably faced by SCA with respect to each of the designated services it provided under tables 1 and 3, s 6 of the Act.

115. From 7 December 2016 to about 17 November 2022, SCA did not appropriately identify and assess the ML/TF risks of designated services according to an appropriate methodology.

Particulars

See *Risk methodologies* above.

116. From 7 December 2016 to about 17 November 2022, the Standard Part A Programs did not identify all designated services provided by SCA.

Particulars

The Standard Part A Programs did not identify or address credit or loans (items 6 and 7, table 1, s 6) or remittances (items 31 and 32, table 1, s 6) as designated services provided by SCA.

See *Remittance services – items 31 and 32, table 1, s 6 designated services* and *Loans – items 6 and 7, table 1, s 6 designated services* below.

117. In the absence of appropriate risk assessments, SCA's Standard Part A Programs did not include appropriate risk-based controls to identify, mitigate and manage the ML/TF risks of designated services, as pleaded at paragraphs 200 to 430 below.

Particulars

Rule 8.1.4(2) of the Rules.

See paragraphs 97 to 113.

The ML/TF risk factors - customers

118. The risk-based procedures, systems and controls in the Standard Part A Programs were not aligned to the ML/TF risks reasonably faced by SCA with respect to customers, for the reasons pleaded at paragraphs 119 to 144 below.

Particulars

Rules 8.1.4(1), 8.1.5(1), 15.2 and 15.3 of the Rules.

119. For the reasons pleaded at paragraph 81, the Standard Part A Programs did not establish a framework that enabled SCA to appropriately categorise and rate the risks posed by different types of customers.

Customer type risk classification categories and low default ratings

120. At all times, the Standard Part A Programs provided that all SCA customers were to be considered low risk by default (the **default rating**), unless the customer was required by the Program to be risk rated.

Particulars

The circumstances in which the SCA Standard Part A Programs required a customer to be risk rated and potentially assessed above low are set out at paragraphs 122 to 132.

On 12 April 2021, the SCEG Board decided permanently to cease dealing with junket operators. SCEG and SCA ceased doing business with all junkets at that time. The June 2021 Standard Part A Program removed references to junkets.

121. The SCA Standard Part A Programs did not:

a. set out an appropriate basis for customers to be rated low risk by default, if they did not meet the criteria pleaded at paragraphs 122 to 132;

b. set out appropriate criteria for customer risk ratings above low; or

c. include appropriate systems and controls to identify customers who met the criteria for risk ratings above low.

Particulars

The criteria for customer risk did not appropriately cover the full range of circumstances in which customer risks were not low.

Many criteria for customer risk ratings from 2017 were discretionary, not the subject of articulation by reference to ML/TF risks, and not capable of consistent application.

Criteria based on transactional parameters were not capable of being consistently identified due to limitations with transaction monitoring.

122. The 2015 Standard Part A Program stated that all SCA customers were automatically rated low risk by default, unless the Program or a decision made under it required otherwise.

Particulars

Section 13 of the 2015 Standard Part A Program.

123. The 2015 Standard Part A Program stated that the AML Committee/AML Compliance Officer (**AMLCO**) shall assign customers an elevated risk rating of moderate, high or significant where they met certain criteria.

Particulars

Section 13 of the 2015 Standard Part A Program.

The 2015 Standard Part A Program stated that a customer shall have their risk rating elevated to moderate when, for example, SCA receives enquiries from government agencies seeking information in relation to the customer; SCA receives advice from a reliable source stating that the customer is engaged in criminal activity of a kind that suggests a ML/TF risk; or the customer conducts transactions exceeding $100,000 over the course of a month.

The 2015 Standard Part A Program stated that a customer shall have their risk rating elevated to high when, for example, the customer's primary residence is in a high risk jurisdiction; the customer is the subject of a SMR; or where the customer's gambling patterns are not supported by their occupation and there is no other reasonable explanation to support their level of turnover.

The 2015 Standard Part A Program stated that a customer shall have their risk rating elevated to significant when, for example, the customer is identified as a foreign PEP; the customer is from a high risk jurisdiction and presents front money in excess of $100,000; or the customer is known to have a criminal record of a kind that might point to involvement in ML/TF activities or is known to have engaged in such activities in the past.

The Standard Part A Programs did not include appropriate risk-based systems and controls to consistently identify and escalate customers who met the criteria in section 13 of the 2015 Standard Part A Program.

The criteria for customer risk did not appropriately cover the full range of circumstances in which customer risks were not low.

124. The 2017-2021 Standard Part A Programs stated that all customers received a default rating of low risk, and having regard to customer types, the manner in which designated services were used and any unusual changes in behavioural traits would determine whether the default rating should be elevated in particular cases.

Particulars

Section 3, paragraph 31 of the 2017 to February 2021 Standard Part A Programs.

Section 3, paragraph 30 of the June 2021 and October 2021 Standard Part A Programs.

The process for determining whether the default rating should be elevated were predominantly discretionary (subject to paragraph 125), not the subject of articulation by reference to ML/TF risks, and not capable of consistent application.

125. The 2017-2021 Standard Part A Programs:

a. identified some categories of customer that were to rated higher than low risk, as pleaded at paragraphs 126 to 132 below; but

b. did not include appropriate risk-based systems and controls to consistently identify customers who met these criteria and to refer them for a risk assessment.

126. The 2017-2021 Standard Part A Programs stated that foreign PEPs or international organisation PEPs should automatically be accorded a significant risk rating.

Particulars

Section 3, paragraph 9 of the 2017-2021 Standard Part A Programs.

127. The 2017-2021 Standard Part A Programs also required customers identified as residing in high risk jurisdictions to automatically be accorded a high risk rating.

Particulars

Section 3, paragraph 10 of the 2017-2021 Standard Part A Programs.

128. The 2017-2021 Standard Part A Program also required the following types of customers to be accorded a moderate risk rating by default:

a. domestic PEPs; and

b. all participants in a junket group.

Particulars

Section 3, paragraph 9 of the 2017-2021 Standard Part A Programs required domestic PEPs to have a moderate risk rating of default.

Section 3, paragraph 12 of the 2017-February 2021 Standard Part A required all participants in a junket group to have a moderate risk rating of default.

SCA ceased operating junket programs on 12 April 2021.

The Standard Part A Programs did not include appropriate risk-based procedures to consistently escalate junket participants for a risk assessment where their ML/TF risk profile indicated risks above moderate.

129. The February 2021 Standard Part A Program required junket operators to automatically be accorded a high risk rating and junket representatives and players to automatically be accorded a moderate risk rating.

Particulars

Section 3, paragraph 12 of the February Standard Part A Program.

SCA ceased operating junket programs on 12 April 2021.

130. The 2017-2021 Standard Part A Programs also stated that where there was reliable information to indicate a customer had a criminal record of a kind which might point to involvement in ML/TF activities, that person should generally be accorded a high risk rating depending on the specific circumstances.

Particulars

Section 3, paragraph 11 of the 2017-2021 Standard Part A Program.

The Standard Part A Programs did not include appropriate risk-based systems and controls to consistently identify customers who met these criteria and to refer them for a risk assessment. Nor were these criteria clearly defined.

131. The 2017-2021 Standard Part A Programs provided that customers transacting at the levels specified below should be accorded a moderate risk:

a. transactions exceeding $100,000 over the course of any month;

b. five or more threshold transactions over the course of any month; and

c. five or more foreign currency transactions in excess of $1,000 over the course of any month;

but the transaction monitoring program was not capable of consistently identifying and escalating customers who met these criteria.

Particulars

Section 3, paragraph 13 of the 2017 to February 2021 Standard Part A Programs.

Section 3, paragraph 12 of the June 2021 and October 2021 Standard Part A Programs.

See *The Standard Part A Programs - Transaction monitoring program* below.

132. The 2017-2021 Standard Part A Programs provided for a number of circumstances that were a general guide to the assignment of ML/TF risk having regard to the issues identified in section 3, paragraphs 8-29 of the Standard Part A Programs.

Particulars

Section 3, paragraph 32 of the 2017- February 2021 Standard Part A Programs.

Section 3, paragraph 31 of the June 2021 and October 2021 Standard Part A Programs.

In some circumstances, a risk rating trigger would result in an automatic elevated risk rating. For example, where the risk rating trigger was the result of a transaction monitoring rule alert or a system-generated report.

The Standard Part A Programs did not include risk-based systems and controls to consistently identify and escalate customers who met these criteria. Nor were these criteria clearly defined.

Identification, escalation and assessment of customers who were not low risk

133. From 7 December 2016 to about 17 November 2022, the Standard Part A Programs did not include appropriate procedures to:

a. trigger an assessment of a customer's risk rating to determine if they were not low risk by default; or

b. determine if they should have had their risk rating elevated

for the reasons pleaded at paragraphs 134 to 137 below.

134. The AML Analyst and from April 2021 the AML/CTF Compliance Manager were primarily responsible for customer risk rating assessments, but the Standard Part A Programs did not include:

a. appropriate procedures to consistently escalate potentially higher risk customers to the AMLCO or other senior management for assessment.

b. appropriate documented guidance, for assessing a customer's risk rating.

Particulars

For example, there was no documented guidance on the searches or checks to be performed by the AMLCO, in considering a customer's risk rating.

The Standard Part A Programs did not include any appropriate guidance or criteria on assessing the ML/TF risks of customers with respect to table 1, s 6 financial services, including with respect to loans and remittance services.

The International Business Patron Account Team carried out assessments of the credit risks posed by customers applying for CCFs. These credit risk assessments were not subject to any appropriate guidance or criteria relevant to ML/TF risks and customer risk ratings.

135. The Standard Part A and B Programs included screening procedures that were intended to identify domestic, foreign and international organisation PEPs and to identify whether a customer was on a terrorism or sanctions list or was otherwise subject to adverse media.

Particulars

<u>From December 2016 until February 2017</u>

Section 20 of the 2015 Standard Part B Program required all customers undertaking the following designated services to be screened:

(a) opening an account;

(b) making deposits to, or withdrawals from, an account;

(c) exchanging foreign currency at or over the value of $1,000;

(d) purchasing chips at the Cage or over the value of $10,000;

(e) redeeming chips at the Cage or over the value of $10,000;

(f) purchasing chips at the gaming table or over the value of $10,000;

(g) receiving pay out of winnings and accumulated credits on a gaming machine at or over the value of $10,000;

international funds transfer instructions.

Appendix B, paragraph 90 required all junket operators, representatives and players to be screened prior to arrival or on arrival at the SCA casino.

Section 15 of the 2015 Standard Part A Program required customers who returned a negative screening result, who were still active customers and were rated moderate risk, to be re-screened at least once every two years.

Section 15 of the 2015 Standard Part A Program required customers who were rated high risk or above to be re-screened annually.

From February 2017 to November 2022

Section 19 of the 2017-2021 Standard Part B Programs required the following customers to be screened: (a) those undertaking the following designated services in amounts of at least $10,000:

(i) purchase of gaming chips; (ii) redemption of gaming chips; (iii) redemption of jackpot/cancelled credits;

(b) those exchanging foreign currency in an amount of at least $1,000;

(c) those establishing an FMA; and

(d) those having been rated high or significant risk junket operators, representatives and players.

From February 2017 until June 2017 all customers who were screened under section 19 of the Standard Part B Programs were required to be re-screened annually.

From June 2017 until on or around November 2022, customers rated moderate risk or higher were required to be re-screened annually.

136. The provisions in the SCA Standard Part A and Part B Programs relating to screening pleaded at paragraph 135 were not capable of consistently identifying customers, on a risk basis, who should have been escalated to the AML team for an assessment or reassessment of their risk rating.

Particulars

From 2017, screening was not triggered (i) by the reporting of a SMR or TTR; (ii) as part of the enhanced customer due diligence (**ECDD**) process; (iii) with respect to non-cash transactions including through the SCA Customer account channel and SCEG Customer account channel.

Customers who were playing uncarded could not be consistently screened.

At all times, re-screening did not occur with sufficient regularity.

137. The Standard Part A and Part B Programs did not include or incorporate appropriate risk-based procedures, in addition to screening, to identify, escalate and risk rate customers who were not low risk:

a. The Standard Part A Programs did not include or incorporate a process to consistently identify customers from high risk jurisdictions and apply an automatic high risk rating.

Particulars

Section 13 of the 2015 Standard Part A Program.

Section 3 of the 2017-2021 Standard Part A Programs.

While the 2017-2021 Standard Part A Programs required a customer residing in a high-risk jurisdiction to be assigned an automatic 'high' risk rating, the Standard Part A Programs did not include or incorporate a system to identify and adjust a customer's risk rating based on these criteria.

b. Prior to 12 May 2020, there was no written procedure in place for SCA to appropriately consider whether information received from law enforcement in relation to a customer required a customer's risk rating to be higher than moderate.

c. The Standard Part A Programs also provided for daily and monthly system-generated transaction monitoring reports. For the reasons pleaded at paragraphs 435 to 474, these processes were not capable of consistently identifying customers who were not low risk.

d. Many of the triggers in the Standard Part A Programs for rating a customer moderate risk or above were based on identifying transactional activity within certain parameters. However:

i. there were no clear procedures to ensure that customers that fell within some of those parameters would be consistently identified;

ii. there were no procedures to ensure that the results of the transaction monitoring program were used to review the level of risk accorded to customers;

iii. to the extent those parameters relied on frontline staff submitting observation reports, SCA's AML/CTF training was inadequate; and

iv. the transaction monitoring program was not capable, by design, of identifying unusual transactional activity relevant to customer risk ratings.

Particulars

See *The Standard Part A Programs - Transaction monitoring program* below.

Procedures to collect, update and review KYC information

138. The Standard Part A Programs did not include or incorporate appropriate risk-based procedures to collect, verify and analyse appropriate KYC information for the purposes of assessing a customer's risk, including with respect to source of wealth or source of funds.

a. Prior to 23 December 2019, SCA collected source of funds information from customers on an ad hoc basis.

Particulars

While at the time of collecting KYC information SCA requested occupation information from customers in accordance with the Standard Part A Programs, it was optional for the customer to provide this.

b. It was not until 23 December 2019 that SCA introduced a requirement for a Source of Funds Declaration Form to be completed by International Business customers, including customers who received designated services through junket channels, who presented $100,000 or more in cash.

Particulars

No supporting documentation was required to be submitted with the forms.

There was no requirement for domestic customers to complete a Source of Funds Declaration Form for cash deposits of any amount.

c. On 17 December 2020, SCA introduced updated requirements for a Source of Funds Declaration Form, with supporting documentation, to be completed by interstate and local customers as well as International Business customers.

Particulars

Source of Funds Declaration Forms, with supporting information, were required to be completed by:

a) domestic customers for cash transactions of $150,000 and above, and

b) International Business customers for cash transaction of $250,000 and above.

d. It was not until 19 July 2021 that SCA introduced a requirement for collecting source of funds information in relation to customers presenting cash amounts under $100,000.

Particulars

Source of Funds Declaration Forms, with supporting documentation, were required to be completed by any customer presenting more than $100,000 in cash.

Source of Funds Declaration Forms were required to be completed by any customer presenting cash between $50,000 to $100,000 in cash. No supporting documentation was required.

There remained no requirements in relation to cash amounts under $50,000.

e. In relation to 138.b to 138.d there were no appropriate written review criteria to assess the information provided on the Source of Funds Declaration Form.

f. Prior to 19 July 2021, SCA did not require customers transferring funds to SCA by electronic transfer to provide source of wealth information with supporting documentation.

Particulars

On and from 19 July 2021, SCA required a Source of Wealth Declaration Form, with supporting information, to be completed by domestic customers who made an inward EFT transfer of $300,000 or more, and international customers who made an inward EFT transfer of $1,000,000 or more.

In July 2021, SCA initiated a process of collecting source of wealth information from all of its current top tier (Black) loyalty program members.

See paragraph 516 below.

g. As part of its ECDD, the Standard Part A Programs required the AMLCO to take 'reasonable measures' to identify the source of wealth and source of funds for PEPs who were rated at least high risk.

Particulars

Section 15 and 17 of the 2015 Program; Section 14, paragraph 11 of the 2017- 2021 Standard Part A Programs.

The 'reasonable measures' were at the discretion of the AMLCO, and there was no guidance or procedures relating to their application, such that the measures were not appropriately risk-based.

The Standard Part A Programs did not include or incorporate any guidance or criteria for the analysis of source of wealth information, having regard to ML/TF risks or any ML/TF risk appetite to be accepted with respect to customers.

h. In the absence of a risk-based requirement in the Standard Part A Programs to consistently obtain and assess information about source of wealth or source of funds (such as occupation), SCA was unable to understand the risk posed by certain customers.

Particulars

See the definition of 'KYC Information' in r 1.2.1 of the Rules in relation to customers who are individuals.

Source of wealth and source of funds information was not required from all customers. However, there were higher ML/TF risks related to source of wealth and source of funds for international premium customers, among others.

139. The Standard Part A Programs did not include appropriate risk-based processes to collect or verify further KYC information relating to the beneficial ownership of funds or the beneficiaries of transactions being facilitated, including the destination of funds.

Assurance

140. The Standard Part A Programs did not include or incorporate any assurance processes relating to the methodology to assign risk ratings to customers.

141. The Standard Part A Programs did not establish appropriate systems and procedures with respect to the audit trails of customer risk assessments.

Particulars

Customer risk ratings were entered into Bally CMP but, from 2017, were not linked to the record in Bally CMP of the reason for elevating a customer's risk rating.

The 2018 external review identified that the process to record and elevate a customer's risk rating was manual, prone to manual error and that is was difficult to establish a reliable audit trail in the risk rating recording process.

The limitations with the system were identified by SCA as a lack of auditability of who and when a customer risk rating was changed and an ability to record a risk rating comment.

142. It was not until August 2021 that SCA commenced a feasibility study into Bally's suitability to maintain a full audit history on customer risk rating data. SCA has not yet implemented any system or system update that allows for a full audit history of customer risk rating data.

Risk based controls

143. The Standard Part A Programs did not include appropriate risk-based systems and controls to mitigate and manage the ML/TF risks of customers who had been assessed as high risk or above.

Particulars

The Standard Part A Programs did not require customers rated high risk or above to be subject to any additional ongoing transaction monitoring.

144. The Standard Part A Programs did not include appropriate risk-based systems and controls to identify customers who presented ML/TF risks outside of SCA's risk appetite.

Particulars

Sections 84(2)(a) and 84(2)(c) of the Act and Parts 8 and 15 of the Rules.

See paragraphs 519 to 520 below.

The ML/TF risk factors - channel

145. The risk-based procedures, systems and controls in the Standard Part A Programs were not aligned to the ML/TF risks reasonably faced by SCA having regard to the channels through which designated services were delivered, including for the following reasons:

a. The Standard Part A Programs did not appropriately address channel risk.

Particulars

SCA's determination and assignment of ML/TF risk ratings for its delivery channels were not based on any written guidance or procedure.

SCA did not perform any regular or periodic reviews of its purported delivery channel risk assessments.

SCA did not have any written policies or procedures relating to delivery channel risk assessments.

b. The SCA Customer accounts, identified at paragraph 269 below, were not appropriately recognised by the 2017-2021 Standard Part A Programs as a channel through which designated services were provided and the ML/TF risks of this channel were therefore not appropriately assessed.

Particulars

See particulars at paragraph 103.

c. The SCEG Customer accounts, identified at paragraph 239 below, were not appropriately recognised by the 2017-2021 Standard Part A Programs as a channel through which designated services were provided and the ML/TF risks of this channel were therefore not appropriately assessed.

d. The SkyCity New Zealand channel was not recognised in the 2017-2021 Standard Part A Programs as a channel though which designated services were provided and the ML/TF risks of this channel were therefore not appropriately assessed.

e. The Standard Part A Programs did not appropriately recognise or assess the higher ML/TF risks posed by the provision of designated services in private gaming rooms.

Particulars

SCA did not have any policies, procedures or controls that were specific to private gaming rooms, notwithstanding the higher ML/TF risks associated with the provision of designated services in private gaming rooms. Additionally:

i. there were higher transactional limits in the private gaming rooms than on the main gaming floor; and

ii. private gaming rooms were used to facilitate junket programs, which presented higher ML/TF risks for the reasons identified at paragraph 392.

SCA did not conduct or document any ML/TF risk assessments relating to the provision of designated services in private gaming rooms.

See paragraph 380.

f. The Standard Part A Programs did not appropriately recognise that not all designated services provided by SCA were provided face-to face, including the following:

i. some items 31 and 32, table 1, s 6 designated services (remittance services) provided by SCA were not provided face-to-face, including those provided through the SCA Customer account channel and SCEG Customer account channel.

Particulars

Paragraph 25, Appendix B of the 2015 Standard Part A Program identified that designated services through the SCA Customer account channel could be conducted when a customer was not physically present at SCA. However, SCA did not appropriately

assess the associated ML/TF risks or include appropriate risk-based controls.

Section 3 of the 2017-2021 Standard Part A Programs stated that SCA delivered its designated services face-to-face. It did not acknowledge or identify which designated services it provided via a non-face-to-face channel.

ii. some item 13, table 3, s 6 designated services (FMA transactions) were not provided face-to-face, including through the SCEG Customer account channel and the SCA Customer account channel.

Particulars

Winnings could be transferred from a customer's FMA, while the customer was not on site, to their personal bank account, the bank account of another casino or to a third party.

Money could be deposited into a customer's FMA, through the non-face-to-face SCA Customer account and SCEG Customer account channels, including from overseas.

For example, between September 2016 and November 2016, just under $3.5 million was transferred from Customer 3's FMA to other SCA customers' FMA, including Customer 12. Customer 3 never physically visited the SCA premises: see *Customer 3's risk profile*, below.

iii. some item 7 table 1, s 6 designated services (CCFs) were not provided face-to-face; and

Particulars

CCFs could be redeemed or repaid by customers by non-face-to-face transfers.

iv. some items 6, 7, 8 and 9, table 3, s 6 designated services were not provided face-to-face where provided through an EGM, automated table game (**ATG**) or cash redemption terminal (**CRT**) (accepting entry of a person into a game, exchanging money for gaming chips or tokens and vice versa, paying out winnings or awarding a prize in respect of a game).

Particulars

Some item 6, table 3, s 6 designated services were provided through an EGM or ATG.

Some items 7 and 9, table 3, s 6 designated services were provided through an EGM, ATG or CRT.

Some item 8, table 3, s 6 designated services were provided through a CRT.

The Standard Part A Programs did not recognise that designated services provided through EGMs, ATGs and CRTs were being provided through a non-face-to-face channel.

g. The Standard Part A Programs did not include appropriate risk-based systems and controls that were aligned to the ML/TF risks of providing designated services through junket channels, for the reasons pleaded at 382 to 418.

h. As a result of the matters pleaded at sub-paragraphs a. to g., the Standard Part A Programs did not include risk-based systems and controls that applied to and were aligned to each of these channel risks.

Particulars

Rule 8.1.4(3) of the Rules.

The ML/TF risk factors - jurisdiction

146. The risk-based procedures, systems and controls in the Standard Part A Programs were not aligned to the ML/TF risks reasonably faced by SCA with respect to designated services having regard to foreign jurisdictions for the following reasons:

a. At no point did SCA conduct an overall assessment of SCA's jurisdictional risk.

Particulars

Given the number of international customers and the volume of funds received from overseas, an overall jurisdictional ML/TF risk assessment was necessary to understand ML/TF risks and to implement appropriate controls within the Standard Part A Programs.

b. The Standard Part A Programs did not identify the foreign jurisdictions that SCA dealt with.

Particulars

Appendix B of the 2015 Standard Part A Program identified some of the jurisdictions where the SCEG Customer accounts operated.

However, SCA did not identify all the foreign jurisdictions that SCA dealt with. For example, SCA did not identify all the foreign jurisdictions to which it could transfer funds or receive funds from.

The 2017-2021 Standard Part A Programs did not identify any of the jurisdictions where the SCEG Customer accounts operated, or the foreign jurisdictions that SCA dealt with, with the exception of references to SkyCity New Zealand.

c. It was not until September 2019, that SCA introduced an SOP providing for jurisdiction to be considered (once known) by utilising recognised lists published by relevant government authorities.

d. The Standard Part A Programs did not include or incorporate any processes to red-flag customers from high risk jurisdictions.

Particulars

See paragraph 137.a.

Rule 8.1.4(4) of the Rules.

e. The Standard Part A Programs did not identify how jurisdictional risks were factored into the assessment of the ML/TF risks of designated services or channels.

Particulars

For example, the jurisdictional risks of international payment channels were not appropriately considered.

Changing or emerging ML/TF risks – reviewing and updating ML/TF risk assessments and controls

147. At no time did the Standard Part A Programs include appropriate risk-based systems and controls to identify significant changes in ML/TF risks and to recognise such changes for the purpose of the Standard Part A and Standard Part B Programs for the reasons pleaded at paragraphs 100 to 113 below.

Particulars

Rule 8.1.5(3) and (4) of the Rules.

148. The Standard Part A Programs did not include appropriate procedures requiring regular review of the Risk Assessments.

Particulars

Paragraphs 106-109 of Appendix B of the 2015 Standard Part A Program provided for SCEG in conjunction with SCA to review the ML/TF risk assessment from time to time.

Section 3, paragraph 37 of the 2019 and February 2021 Standard Part A Programs and section 3, paragraph 36 of the June 2021 and October 2021 Standard Part A Programs provided that SCA would review any typology reports released by AUSTRAC, and more generally, feedback provided by AUSTRAC and SCEG's own intelligence gathering and audit process to determine whether changes to the ML/TF risk assessment in section 3 and schedule 1 may be necessary from time to time.

Section 3, paragraph 38 of the 2019 and February 2021 Standard Part A Programs and section 3, paragraph 37 of the June 2021 and October 2021 Standard Part A Programs provided that the risk assessment would be subject to a formal review process every two years to ensure these disciplines had been implemented.

At no time did the Standard Part A Programs include appropriate procedures identifying when (aside from the formal review process) reviews would be conducted; or how new risk information and intelligence would trigger a review of the ML/TF risk assessment.

149. By reason of the matters pleaded at paragraphs 100 to 108 above, at all times the Risk Assessments did not include key ML/TF risks reasonably faced.

150. By reason of the matters pleaded at paragraph 149, the reviews of the Risk Assessments on their own were not capable of identifying significant changes in ML/TF risks and recognising such changes for the purposes of the Standard Part A and Standard Part B Programs.

Particulars

Each of the reviews conducted between 7 December 2016 and on or around 17 November 2022, failed to recognise and address the matters pleaded at paragraphs 100 to 108.

151. As the Standard Part A Programs did not include an appropriate risk-based risk methodology, ML/TF risks were not capable of being consistently assessed and re-assessed over time.

Particulars

See *Risk methodologies* above.

The 2018 and August 2021 external reviews advised SCA that there was a lack of methodology or procedure to identify and recognise significant changes in risk.

152. The Standard Part A Programs did not include risk-based procedures for SCA to identify and assess trends arising from or disclosed by:

a. usage of designated services or channels;

b. transaction monitoring;

c. suspicious matter reporting;

d. information from AUSTRAC and law enforcement;

e. internal financial crime reporting; and

f. the external risk environment.

Particulars

See paragraphs 191 to 192.

The Standard Part A Programs did not include any procedures for escalating any typology reports or feedback from AUSTRAC for the purposes of reviewing risk assessments. Nor were there any procedures to identify what SCEG intelligence or audit outcomes would be escalated and to whom for the purposes of reviewing SCA's risk assessment. See paragraph 148 above.

153. The Standard Part A Programs did not include appropriate risk-based procedures to escalate emerging trends to senior management.

Particulars

See paragraphs 176, 191 and 192.

154. The Standard Part A Programs did not provide appropriate procedures for SCEG Board or SCA Board and senior management oversight of the Risk Assessments for the purposes of identifying and recognising significant changes in risk.

Particulars

See *Approval and oversight of the Standard Part A Programs.*

155. At no time did the Standard Part A Programs include appropriate risk-based systems and controls to identify, mitigate and manage any ML/TF risks arising from:

a. all new designated services prior to introducing them;

b. all new methods of designated service delivery (channel) prior to adopting them; and

c. all new and developing technologies for the provision of designated services prior to introducing them.

Particulars

Rule 8.1.5(5) of the Rules.

The lack of risk-based systems and controls to identify, mitigate and manage any ML/TF risks arising from new designated services prior to introducing them resulted in new designated services and channels for designated services, such as the Horizon Tourism account, being introduced without any risk assessment being undertaken in relation to them.

See paragraphs 257 to 261.

Approval and oversight of the Standard Part A Programs

Approval of the Standard Part A Programs

156. At all times, SCA was the reporting entity providing designated services through the SkyCity Adelaide casino.

Particulars

See paragraph 6.

157. At all times:

a. the governing Board of SCA; and

b. SCA senior management

were each required to approve the SCA Standard Part A Programs.

Particulars

Sections 81(a), 84(2)(a) and (c) of the Act and rule 8.4.1 of the Rules.

158. The SkyCity Entertainment Group (**SCEG**) was the parent company of SCA.

159. From 7 December 2016 to 27 October 2021, the Standard Part A Programs provided that the SCEG Board was the governing board of SCA.

Particulars

Section 19 of the 2015 Standard Part A Program.

Section 6 of the 2017, Amended 2017, 2018, 2019, February 2021 and June 2021 Standard Part A Programs.

160. The 2015 Standard Part A Program provided that the Audit and Financial Risk Committee (the **AFRC**) of the SCEG Board must approve any amendment to the program.

Particulars

Section 3 of the 2015 Standard Part A Program.

161. At no time did the 2015 Standard Part A Program require both the SCEG Board or the AFRC and SCA senior management to approve the Standard Part A Program.

Particulars

Rule 8.4.1 of the Rules.

162. In accordance with the specification in SCA's Standard Part A Program referred to in paragraph 161 above, the 2015 Standard Part A Program was approved by the AFRC.

163. In contravention of r 8.4.1 of the Rules and s 84(2)(c) of the Act, the 2015 Standard Part A Program was not approved by SCA senior management.

164. The 2017-June 2021 Standard Part A Programs provided that the SCEG Board or the AFRC and the AML/CTF Senior Management Group shall approve any amendments to the Part A Program.

Particulars

Section 6 of the 2017-June 2021 Standard Part A Programs.

From the February 2021 Program, the AFRC was known as the Audit and Risk Committee, and the AML/CTF Senior Management Group was known as the AML/CTF Committee.

The AML/CTF Senior Management Group was a group of SCA senior staff from relevant departments.

165. In accordance with the specification in SCA's Standard Part A Program referred to in paragraph 164 above, the 2017-June 2021 Standard Part A Programs were approved by the AFRC or the SCEG Board, or both.

166. In contravention of r 8.4.1 of the Rules and s 84(2)(c) of the Act, the 2017-2021 Standard Part A Programs were not approved by SCA senior management, including the AML/CTF Senior Management Group.

Oversight of the Standard Part A Programs

167. The Standard Part A Program was required to be subject to the ongoing oversight of SCA's governing Board and senior management.

Particulars

Sections 84(2)(a) and (c) of the Act and rule 8.4.1.

168. The oversight required of SCA's governing Board and SCA senior management included oversight of how, and the extent to which, the Standard Part A Programs were achieving the primary purpose of identifying, mitigating and managing ML/TF risk.

Particulars

Sections 84(2)(a) and (c) of the Act and rule 8.4.1 of the Rules.

169. In the absence of an appropriate oversight framework, a Part A program will not be capable, by design, of:

a. identifying, mitigating and managing the ML/TF risks reasonably faced by a reporting entity; and

b. being subject to the ongoing oversight of the reporting entity's governing Board and senior management.

170. A reporting entity of the nature, size and complexity of SCA will not be in a position to have an appropriate oversight framework, for the purposes pleaded at paragraph 169, unless its Part A Program has established an appropriate framework for the governing Board and senior management to:

a. determine and set the reporting entity's ML/TF risk appetite;

b. set controls to ensure designated services are provided to customers consistent with that ML/TF risk appetite;

c. appropriately monitor management's performance against an appropriate ML/TF risk management framework, including ML/TF risk appetite;

d. ensure the governing Board receives and reviews management reports about new and emerging sources of ML/TF risk and about the measures management are taking to deal with those risks; and

e. establish appropriate ML/TF risk management capability frameworks, including with respect to:

i. roles and accountabilities;

ii. operational procedures;

iii. reporting lines;

iv. escalation procedures;

v. assurance and review; and

vi. information management.

Particulars

Sections 81, 84(2)(a) and 84(2)(c) of the Act, rr 8.1.3, 8.1.5(4) and Part 8.4 of the Rules.

171. Each of the features pleaded at paragraphs 170.a to 170.e were fundamentally absent from the Standard Part A Programs for all or most of the period from 7 December 2016 to about 17 November 2022, although some independent review was conducted.

Particulars

See paragraphs 172 to 193 with respect to the 2015 to June 2021 Standard Part A Programs.

See paragraphs 194 to 197 with respect to the October 2021 Standard Part A Program.

Between 3 August 2016 and 6 August 2021, three external independent reviews were completed.

The 2015-June 2021 Standard Part A Programs

172. The 2015-June 2021 Standard Part A Programs provided that the AFRC and the AML/CTF Senior Management Group would have oversight of the Standard Part A Programs.

Particulars

Section 3 of the 2015 Standard Part A Program.

Section 6 of the 2017-June 2021 Standard Part A Programs.

ML/TF risk appetite

173. At no time did the 2015-June 2021 Standard Part A Programs include or incorporate appropriate systems and controls for the SCEG Board, including the AFRC to:

a. set SCA's ML/TF risk appetite; and

b. ensure that the SCA business was managed consistent with ML/TF risk appetite.

Particulars

In February 2020, SCEG introduced a risk appetite statement specifying the risk appetite or risk tolerance SCEG was willing to bear in relation to categories of key risk. Between February 2020 and July 2021, AML compliance risk was identified as an area of risk. From February 2021, AML was subsumed into the area of regulatory and compliance risk. However, the risk metrics were not appropriately representative for a business of the nature, size and complexity of SCEG or SCA such that the SCEG Board would not have been able to consistently ensure where SCA was operating against risk appetite and tolerance.

The SCEG Board or the AFRC did not have any appropriate processes in place to ensure that SCA was managed consistently with any ML/TF risk appetite.

At no time did the 2015-June 2021 Standard Part A Programs include or incorporate any other process for ML/TF risk appetite to be appropriately determined with respect to SCA.

In March 2022, as part of SCA's AML Enhancement Program, SCA identified that it had engaged a third party to develop an AML/CTF Board risk appetite statement.

Monitoring management performance

174. At no time did the 2015-June 2021 Standard Part A Programs include or incorporate appropriate systems and controls for the SCEG Board, including through the AFRC, to appropriately monitor management's performance against an appropriate ML/TF risk management framework, including as against ML/TF risk appetite.

175. The SCEG Board, including through the AFRC, was unable to have oversight of senior management's performance in mitigating and managing ML/TF risk because:

a. the SCEG Board or the AFRC had not set a ML/TF risk appetite;

b. the 2015-June 2021 Standard Part A Programs did not include or incorporate appropriate qualitative and quantitative metrics triggering reporting for material ML/TF risk categories;

c. the 2015-June 2021 Standard Part A Programs did not include or incorporate processes for monitoring and reporting of SCA's risk profile relative to quantitative parameters (risk tolerances) against material risk categories; and

Particulars

See particulars at paragraph 173.

d. the 2015-June 2021 Standard Part A Programs did not include or incorporate a documented process to ensure in-depth discussion of ML/TF risk as against measurable criteria at regular intervals as part of a rolling agenda for the SCEG Board or the ARFC.

176. The SCEG Board, including the AFRC, and senior management were unable to determine whether SCA's risk-based systems and controls required any revision for the purposes of the 2015-June 2021 Standard Part A Programs because:

a. at no time did the 2015-June 2021 Standard Part A Programs include appropriate systems and controls for the SCEG Board or the AFRC to receive and review management reports about new and emerging sources of ML/TF risk or the measures management were taking to deal with those risks;

b. the 2015-June 2021 Standard Part A Programs did not include appropriate systems and controls to detect changes in ML/TF risks reasonably faced by SCA, including in both the external and internal environment;

Particulars

See paragraph 147.

c. the 2015-June 2021 Standard Part A Programs did not establish an appropriately resourced and expert AML/financial crime function. This meant that material changes in ML/TF risk could not be consistently identified and escalated to senior management; and

Particulars

See paragraph 185.

The September 2021 external review identified the following key themes with respect to the June 2021 Standard Part A Program's design adequacy and operational effectiveness:

i. AML/CTF Program operationalisation has not been adequately designed, appropriately resourced, or satisfactorily monitored for effectiveness, and the AML/CTF Program is therefore reactive rather than proactive.

ii. Whilst current AML/CTF resources are capable, the demands and requirements placed on those resources significantly impact SCA's ability to implement and operate an appropriate AML/CTF Program and ensure it continues to be effective.

iii. Designing and implementing any new process requires a detailed and comprehensive resourcing and capacity assessment to ensure that the function carrying out the process is appropriately resourced to ensure compliance with the Part A AML/CTF Program.

See particulars at paragraph 453.

d. the 2015-June 2021 Standard Part A Programs did not include appropriate systems and controls to ensure that material changes in ML/TF risk, once identified, were escalated by senior management to the SCEG Board or the AFRC.

Particulars

In the absence of regular ML/TF risk assessments using an appropriate methodology, it was not possible to consistently detect material changes in ML/TF risk.

Senior management accountabilities

177. The 2015-June 2021 Standard Part A Programs provided for the AML/CTF Senior Management Group to have oversight of the Standard Part A Program.

Particulars

See section 3 of the 2015 Standard Part A Program. The AML/CTF Senior Management Group was known as the AML Committee in the 2015 Standard Part A Program.

See section 6 of the 2017-June 2021 Standard Part A Programs.

178. The 2015-June 2021 Standard Part A Programs provided that the AML/CTF Senior Management Group would receive updates with respect to specific parts of the Program and review aspects of the Program.

Particulars

Sections 3, 4, 8, 12, 13, 14, 15 and 17 of the 2015 Standard Part A Program.

Sections 3, 4, 5, 6, 7, 8, 9, 11 and 13 of the 2017-2021 Standard Part A Programs.

179. The 2015-June 2021 Standard Part A Programs did not clearly establish a mandate for the AML/CTF Senior Management Group to make or recommend decisions with respect to AML/CTF matters.

Particulars

In the absence of a clear role to meaningfully assess information and challenge the management of ML/TF risk, and in the absence of a clearly set ML/TF risk appetite, the AML/CTF Senior Management Group was not capable of identifying weaknesses in SCA's risk management systems and controls. Nor were they capable of identifying and escalating material matters to the AFRC or SCEG Board.

The September 2021 external review identified that the minutes of the various forums, which included the AML/CTF Senior Management Group, did not evidence a culture of challenge, meaningful assessment and implications of findings, as would normally be expected from an organisation the size and complexity of SCA.

180. The AML/CTF Senior Management Group completed AML/CTF training, but the training was not adequate.

Particulars

Rule 8.2 of the Rules.

SCA employees did not receive adequate ML/TF risk awareness training because as SCA did not carry out appropriate ML/TF risk assessments, their risk awareness training was not capable of covering the ML/TF risks reasonably faced with respect to all designated services.

181. The 2015-June 2021 Standard Part A Programs did not establish clear or appropriate accountabilities within SCA senior management or SCEG senior management, to ensure that all decisions had appropriate regard to ML/TF risk, including within SCA's ML/TF risk appetite.

Particulars

See *ECDD triggers in respect of Customer 11*, below.

See *Customer 1's risk profile*, below.

See *ECDD triggers in respect of Customer 14*, below.

See paragraph 343.a to 343.b.

The 2017-June 2021 Standard Part A Programs provided that the role of Group General Manager, being the Group General Manager, Regulatory Affairs and AML (SCEG), included receiving reports of any material event relevant to the discharge of SCA's AML/CTF obligations and reporting to the AFRC: sections 6, 7 and 9 of the 2017-June 2021 Standard Part A Programs. However, there was no documented guidance in relation to the circumstances in which a material event relevant to the discharge of SCA's AML/CTF obligations should be reported from the AMLCO to the Group General Manager, Regulatory Affairs and AML (SCEG).

Operational procedures and training for front line business functions

182. At no time did the 2015-June 2021 Standard Part A Programs establish a framework for operational procedures to ensure the Standard Part A Program was capable of being consistently applied by business divisions.

Particulars

There were no appropriately risk-based operational procedures to consistently detect transactions consistent with ML/TF typologies (paragraphs 446 to 450); or to consistently undertake ECDD (paragraphs 512 to 513); or to trigger an assessment of a customer's risk rating to determine if they were not low risk by default (paragraphs 133 to 137).

183. In the absence of a framework for the consistent application of the Standard Part A Programs, the SCEG Board and senior management, including the AFRC and the AML/CTF

Senior Management Group, were unable to provide appropriate ongoing oversight of the 2015-June 2021 Standard Part A Programs.

Particulars

Management cannot appropriately identify, assess, manage and monitor ML/TF risks reasonably faced by the reporting entity in a manner consistent with ML/TF risk appetite if the Part A program does not include or incorporate appropriate policies, processes, systems and internal controls to support and guide business decision-making.

In late 2019, a number of SCA's SOPs, which purported to outline the process by which certain AML/CTF functions or obligations were to be discharged were drafted. However, not all of those SOPs were appropriately risk-based: see particulars at paragraphs 85 and 512.

The September 2021 external review found that operationally, the ECDD process appears ad-hoc and discretionary, with no formal process or procedure setting out the relevant measures to be undertaken when completing ECDD based on the level of ML/TF risk faced.

See particulars at paragraph 176.c.

184. At no time did the 2015-June 2021 Standard Part A Programs establish appropriate AML/CTF risk awareness training for front line business functions.

Particulars

Rule 8.2 of the Rules.

SCA employees did not receive adequate ML/TF risk awareness training because as SCA did not carry out appropriate ML/TF risk assessments, their risk awareness training was not capable of covering the ML/TF risks reasonably faced with respect to all designated services.

Roles, accountabilities and reporting for the ML/TF risk management and compliance function

185. At no time did the 2015-June 2021 Standard Part A Programs establish an appropriate framework for roles, accountabilities and reporting lines for ML/TF risk management and compliance, for the reasons pleaded at paragraphs 186 to 189.

186. The 2015-June 2021 Standard Part A Programs did not set out an appropriate framework for end-to-end accountabilities or processes for ML/TF risk management or compliance.

Particulars

The Standard Part A Programs did not establish a framework for senior business ownership with respect to AML/CTF processes across all products, customer groups and channels.

For example, there was no clear accountability with respect to transactions through the SCEG Customer account channel to inform SMR reporting: See paragraph 533.

The September 2021 external review recommended that:

i. SCA undertake an end-to-end review of ECDD process and associated systems to consider where enhancements could be made to the ECDD process.

ii. SCA undertake an end-to-end review of the transaction monitoring program and associated systems to ensure the transaction monitoring program is appropriately enhanced.

iii. The end-to-end process of investigating unusual activity, gathering information, forming a suspicion and ultimately filing a report with AUSTRAC should be the subject of a targeted system, resourcing and capacity review in order to understand where efficiencies and enhancements in the process could be delivered.

iv. SCA should consider undertaking an end-to-end review of the TTR reporting process and associated systems to consider where enhancements could be made to reduce inefficiencies and capacity constraints.

187. The 2015-June 2021 Standard Part A Programs did not set out a framework for an appropriately resourced and expert central ML/TF risk management function to monitor, support and challenge the business on ML/TF risk-related matters.

Particulars

The AML team was under-resourced and did not receive adequate AML/CTF training. AML/CTF obligations under the Standard Part A Programs were delegated to roles outside the AML team (as to which see paragraph 451.c), which did not have adequate AML/CTF training to undertake those tasks.

The September 2021 external review stated that the AML team appeared to operate in an enabling capacity, which lends itself to governance being along the lines of updates rather than challenge and enquiry. The report recommended that SCA should review and ensure a clear delineation of the roles to ensure there is appropriate check and challenge.

188. The 2015-June 2021 Standard Part A Programs did not set out a framework for appropriate assurance and audit functions for AML/CTF matters.

Particulars

SCA did not conduct any assurance or implement reviews at appropriate intervals to test the design, effectiveness or implementation of its transaction monitoring program: see paragraph 455.b.

189. At no time did the 2015-June 2021 Standard Part A Programs establish appropriate AML/CTF risk awareness training to support the AML/CTF functions, including at the AMLCO and AML Analyst levels.

Particulars

Rule 8.2 of the Rules.

SCA employees did not receive adequate ML/TF risk awareness training because as SCA did not carry out appropriate ML/TF risks assessments, their risk awareness training was not capable of covering the ML/TF risks reasonably faced with respect to all designated services.

Escalation and emerging risks

190. At no time did the 2015-June 2021 Standard Part A Programs include appropriate processes to escalate, mitigate and manage material ML/TF risks.

Particulars

See particulars at paragraph 286.

There were no appropriate processes to escalate high risk customers where their occupation (where known) was inconsistent with their gambling.

For example, between 17 December 2016 and 22 March 2021, Customer 29 recorded a buy-in exceeding $13,400,000. At all times, SCA understood Customer 29 to be a meat packer. At no time was Customer 19's source of wealth or stated occupation consistent with their gaming activity. It was not until 31 March 2021 that SCA issued a ban in respect of Customer 19.

Between January 2018 and November 2021, Customer 40 recorded a cash buy-in exceeding $2,800,000. SCA understood Customer 40's occupation variously to be as a waitress or as a homemaker. At no time was Customer 40's source of wealth or stated occupation consistent with their gaming activity. It was not until 26 November 2021 that SCA issued a ban in respect of Customer 40.

Between 18 March 2017 and 13 January 2020, Customer 44 recorded a buy-in exceeding $3,500,000. SCA understood Customer 44's occupation variously to be as a grape picker or as a chef. At no time was Customer 44's source of wealth or stated occupation consistent with their gaming activity. It was not until 29 March 2022 that SCA issued a ban in respect of Customer 44.

Between 2016 and 2021, Customer 46 recorded a buy-in exceeding $3,000,000. At all times, SCA understood Customer 46 to be a plumber. At no time was Customer 46's source of wealth or stated occupation consistent with their gaming activity. It was not until 29 March 2022 that SCA issued a ban in respect of Customer 46.

Between 7 December 2016 and 8 August 2021, Customer 32 recorded a turnover at SCA exceeding $44,000,000. At all times, SCA understood Customer 32 to be a truck driver. At no time was Customer 32's source of wealth or stated occupation consistent with

their gaming activity. It was not until 9 August 2021 that SCA issued a ban in respect of Customer 32.

See *Customer 29's risk profile*, *Customer 32's risk profile*, *Customer 40's risk profile*, *Customer 44's risk profile* and *Customer 46's risk profile* below.

There were no appropriate processes to mitigate and manage known material ML/TF risks with respect to high risk customers. Prior to August 2017, Customer 14 had been excluded from SCEG casinos. In August 2017, International Business approved Customer 14's attendance on a junket notwithstanding the exclusion that was in place. Between August 2017 and December 2018, Customer 14 played on junkets at SCA operated by Customer 1 and Customer 9. Between July and August 2019, media reporting identified a number of material ML/TF risks in respect of Customer 14, including that they had links to organised crime, were the subject of law enforcement inquiries and had been charged with financial crimes in a foreign country.

Despite this, in August 2019, the SCEG General Manager of Regulatory Affairs determined that: it was "not necessary" to conduct ECDD in respect of Customer 14; SCEG would invite Customer 14 to comment on the allegations in the media reports; in the meantime, Customer 14's business relationship with SCEG could continue.

In November 2019, SCEG determined to cease doing business with Customer 14 because an operator of a junket funded by Customer 14 was suing SCEG over disputed costs relating to a jet charter. This decision did not consider the higher ML/TF risks posed by Customer 14, including with regard to SCA's ML/TF risk appetite.

In February 2020, Customer 14 was arrested in a foreign country in connection with money laundering and corruption offences.

It was not until 30 September 2020 that SCA issued a ban in respect of Customer 14.

191. The 2015-June 2021 Standard Part A Programs did not have any clear process or procedures to appropriately consider, act on or escalate applicable recommendations or guidance disseminated or published by AUSTRAC.

Particulars

Rule 8.7 of the Rules.

From 2018, section 9 of the Standard Part A Program required the AMLCO to review all casino-related and other applicable guidance material disseminated or published by AUSTRAC. There were no clearly documented processes to ensure that this consistently occurred, and there were no written processes in place to escalate AUSTRAC recommendations or guidance to SCA or SCEG senior management.

On 1 July 2013 and 3 June 2014, AUSTRAC recommended that SCA amend its transaction monitoring program to ensure that it was capturing and escalating potentially suspicious transactions. An external review in 2016 observed that that SCA's transaction monitoring program had not identified any suspicious matters for escalation, and the underlying reports did not demonstrate analysis of transactions (the **2016 external review**).

On 10 November 2016, AUSTRAC recommended that SCA immediately address the findings in respect of deficiencies identified with SCA's transaction monitoring program in the 2016 external review.

The 2018 external review again raised that SCA's transaction monitoring activities may not be effective in identifying suspicious matters and investigating in a timely manner.

The September 2021 external review found that SCA's transaction monitoring program was operationally ineffective and required enhancement.

192. At no time did the 2015-June 2021 Standard Part A Programs include appropriate systems and controls to ensure that emerging risks identified through Part A program processes such as transaction monitoring, SMR reporting and ECDD were appropriately escalated to management for the purposes of the ongoing assessment and management of ML/TF risks reasonably faced.

Particulars

The transaction monitoring reports and SMR, TTR and IFTI overview reports provided to the AML/CTF Senior Management Group were not capable of appropriately identify emerging risks through Part A program processes.

See paragraphs 177 to 180.

Information management and records

193. Deficiencies with SCA's information management systems and record-keeping procedures limited the ability of SCA's transaction monitoring and ECDD to operate as intended.

Particulars

See paragraph 62.

The October 2021 Standard Part A Program

194. The October 2021 Standard Part A Program provided that:

a. the SCA Board was responsible for approval and ongoing oversight of the Standard Part A Program;

b. the SCA Board delegated the primary responsibility for certain function to the AMLCO (or their delegate);

c. the SCEG Board generally held the SCA Board accountable for its performance;

d. the AFRC will monitor the performance of the SCA Board in relation to oversight of the program; and

e. the program (including Part A) shall also be subject to the ongoing oversight of the AML/CTF Committee and (on an advisory basis) the AFRC.

Particulars

Section 6 of the October 2021 Standard Part A Program.

Prior to February 2021, the AML/CTF Committee was known as the AML/CTF Senior Management Group.

From 26 August 2022, a newly established Risk and Compliance Committee had responsibility for, amongst other things, monitoring SCEG's compliance with AML/CTF requirements in New Zealand and Australia.

195. In the absence of an appropriate risk assessment of the ML/TF risks reasonably faced by SCA with respect to the provision of designated services, the 2021 October Program was not aligned to the ML/TF risks reasonably faced.

196. As a result of the matters pleaded at paragraph 195, the 2021 October Program did not include an appropriate oversight framework because the SCA Board was not able to:

a. set its ML/TF risk appetite (as the ML/TF risks reasonably faced had not been appropriately identified with respect to all designated services and channels).

b. set controls to ensure designated services were provided to customers consistent with ML/TF risk appetite;

c. appropriately monitor management's performance against an appropriate ML/TF risk management framework, including ML/TF risk appetite; and

d. appropriately report to the AFRC on matters relevant to the oversight of the Standard Part A Program, including with respect to emerging ML/TF risks and whether designated services were being provided within ML/TF risk appetite.

Particulars

See *The risk assessment* above.

Sections 81, 84(2)(a) and 84(2)(c) of the Act, rr 8.1.3, 8.1.5(4) and Part 8.4 of the Rules

197. The October 2021 Standard Part A Program did not include an appropriate oversight framework because it did not include:

a. an appropriately resourced and expert AML/financial crime function;

b. appropriate operational procedures to ensure the Standard Part A Program was capable of being consistently applied by business divisions;

c. an appropriate framework for end-to-end accountabilities or processes for ML/TF risk management or compliance;

d. appropriate controls to detect and escalate material changes in ML/TF risk; and

e. appropriate controls for assurance and audit.

Particulars

Sections 81, 84(2)(a) and 84(2)(c) of the Act, rr 8.1.3, 8.1.5(4) and Part 8.4 of the Rules.

See particulars at 176c. and 186.

The oversight failures – the failure to adopt and maintain a Part A program

198. The absence of a framework for appropriate oversight of ML/TF risk management in the Standard Part A Programs, as pleaded at paragraphs 156 to 197, meant that the SCA Board and the SCEG Board and senior management, including the AFRC and AML/CTF Senior Management Group (as relevant), had no basis to be satisfied that the Standard Part A Program was operating as intended and that it had the primary purpose of identifying, mitigating and managing the ML/TF risks reasonable faced by the provision of designated services.

Particulars

Section 84(2)(a) of the Act.

199. The absence of a framework for appropriate oversight of ML/TF risk management in the Standard Part A Programs meant that the SCA Board and SCEG Board and senior management, including the AFRC and AML/CTF Senior Management Group (as relevant), were unable to exercise ongoing oversight of the Standard Part A Programs.

Particulars

Section 84(2)(c) of the Act and r 8.4 of the Rules.

Appropriate risk-based systems and controls

Controls to manage residual risks within appetite

200. Once a reporting entity identifies and assesses its inherent ML/TF risks and determines its ML/TF risk appetite, the reporting entity must ensure that its Part A program includes appropriate risk-based systems and controls to mitigate and manage residual risks within appetite.

201. These systems and controls must be aligned to and proportionate to the ML/TF risks reasonably faced by the reporting entity with respect to the provision of designated services.

Particulars

Rules 8.1.3 and 8.1.4 of the Rules.

202. SCA did not determine its ML/TF risk appetite and did not determine appropriate Part A program controls to enable designated services to be provided within ML/TF risk appetite.

Particulars

See paragraph 173.

203. From 7 December 2016 to about 17 November 2022, the Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of mitigating and managing the ML/TF risks reasonably faced by SCA with respect to designated services they provide for the reasons pleaded at paragraphs 204 to 430 below.

Particulars

Section 84(2)(a) of the Act and rr 8.1.3 and 8.1.5(4) of the Rules.

See paragraphs 91 to 155 above.

Preventative controls

204. From 7 December 2016 to about 17 November 2022, the Standard Part A Programs had very few preventative controls designed to enable SCA to mitigate and manage their ML/TF risks.

Particulars

Preventative controls are those that limit the ability to use a product or channel in a way that would increase the ML/TF risk.

Examples of preventative controls include: setting transaction limits, including daily limits; having management approval for high risk customers, products or countries; applying different identification processes for customers not dealt with in person; or not accepting customers who are deemed too high risk.

The preventative controls included or incorporated in the Standard Part A Programs were not appropriately risk-based and were not capable of consistently mitigating or managing ML/TF risks: see, for example, paragraphs 138, 262.j, 353.d, 355.b and 361.c.

205. At all times, the controls in the Standard Part A Programs were predominately detective and focused on surveillance for unusual activity that may require SMR reporting to AUSTRAC.

Particulars

Detective controls only seek to monitor activity through a product or channel. Examples of detective controls include: gathering information about how products or channels are used; and reviewing information from internal records, such as transaction monitoring and suspicious matter reporting.

Detective controls do not, of themselves, reduce inherent risks.

The detective controls in the transaction monitoring program were not appropriately risk-based and did not comply with the Act and Rules: see paragraphs 431 to 495.

Gaming accounts – items 11 and 13, table 3, s 6

206. The Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by SCA with respect to item 11 and 13, table 3, s 6 designated services for the reasons pleaded at paragraphs 207 to 312.

Front Money accounts (FMAs)

207. At all times, SCA provided customers with FMAs.

208. FMAs were used by customers for day-to-day transactions involving designated services under table 3, s 6 of the Act.

209. FMAs could be linked to a customer's loyalty card and allowed customers to deposit and withdraw funds as to which see the matters pleaded at paragraph 210.

210. At all times, a customer or their representative could deposit value into their FMA or withdraw value from their FMA by way of:

a. money in the form of:

i. cash;

ii. a transfer to or from a bank account;

iii. a transfer to or from another FMA (held by either the customer or a third party) in the circumstances pleaded at paragraph 307;

b. chips or other CVIs;

c. a transfer to or from an electronic gaming machine (**EGM**) or automated table game (**ATG**) through the customer's membership card during play;

d. a transfer of cash or ticket-in ticket out (**TITO**) through a cash redemption terminal (**CRT**); and

e. cheques, including from another casino subject to approval.

Particulars

See paragraph 220.b.

211. FMA transactions were recorded in Bally.

212. The opening of FMAs constituted item 11, table 3, s 6 designated services.

213. Transactions on FMAs constituted item 13, table 3, s 6 designated services.

214. FMAs were a channel through which other table 3, s 6 designated services were provided by SCA.

a. A customer could exchange money in an FMA for chips or other CVIs (item 7, table 3); or

b. A customer could deposit chips or other CVIs (item 8, table 3) into an FMA.

215. FMAs were a channel through which table 1, s 6 designated serviced were provided by SCA.

a. SCA provided customers with items 31 and 32, table 1, s 6 designated services (remittance services) through FMAs.

Particulars

See *Remittance services – items 31 and 32 table 1, s 6 designated services*.

b. Credit (by way of a drawdown under a loan) provided to a customer by SCA could be deposited into a customer's FMA, being item 7, table 1, s 6 designated services.

Particulars

See *Loans – items 6 and 7, table 1, s 6 designated services* below.

c. Loan repayments could also be credited to a customer's FMA, being items 7 and 32, table 1, s 6 designated services.

Particulars

See *Loans – items 6 and 7, table 1, s 6 designated services* below.

216. At all times, designated services provided through FMAs involved higher ML/TF risks, including:

a. FMAs facilitated the movement of money into and out of the casino environment, including through complex transaction chains involving the provision of both table 1 and table 3, s 6 designated services.

b. Money could be deposited into FMAs via the SCEG Customer account channel (as defined in paragraph 239), which involved the higher ML/TF risks pleaded at paragraphs 255 to 259.

c. Money could be deposited into FMAs via the SCA Customer account channel (as defined in paragraph 269), which involved the higher ML/TF risks pleaded at paragraph 283.

d. Money could be deposited into FMAs via the SkyCity New Zealand channel (as defined in paragraph 293), which involved the higher ML/TF risks pleaded at paragraph 302.

e. Third parties could deposit funds into a customer's FMA.

Particulars

See paragraph 220.

f. Funds in FMAs could be transferred to third parties in certain circumstances, including by domestic or international telegraphic transfer.

Particulars

See paragraphs 228.b and 228.c.

g. Funds could be transferred to or from other casinos including non-SCEG casinos and casinos located outside of Australia.

Particulars

See paragraphs 222.e, 222.f, 228.d and 228.e.

h. Funds could also be transferred from one customer's FMA to another customer's FMA in certain circumstances.

Particulars

See paragraph 307.

i. A customer could withdraw cash from their FMA including when the customer had applied the funds to minimal or no gaming.

j. Customers (or third parties) could deposit or withdraw funds from FMAs through non-face-to-face channels, without being present at the Cage.

Particulars

A customer could request the withdrawal of funds from their FMA while not onsite at SCA by requesting and completing a TT Request Form for an electronic transfer to their personal bank account, the

bank account of another casino (including non-SCEG casinos) or a third party bank account: paragraphs 228.b, 228.c, 228.d and 228.e.

A customer could also request a casino cheque be paid to the customer only and mailed to their address.

k. At all times, a premium customer of SCA could leave unlimited funds in an FMA for an unlimited period without applying those funds to gambling (**parked or dormant funds**).

Particulars

From February 2017, FMAs containing $10,000 or more were included in a monthly Front Money Balances Report and were provided to the AML/CTF Senior Management Group for noting and discussion as required.

There were no other processes, procedures or controls in place to manage dormant FMAs. There was no documented review criteria or guidance with respect to considering the Front Money Balances Report.

See particulars at paragraph 218.b.

217. SCA did not conduct an appropriate assessment of the ML/TF risks pleaded at paragraph 216.

Particulars

See *The risk assessments* above.

218. The Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by SCA with respect to designated services provided through FMAs.

a. The Standard Part A Programs did not include appropriate risk-based systems and controls to identify, mitigate and manage the ML/TF risks identified at paragraph 216 above.

b. SCA did not impose appropriate limits on the amount of money that a premium customer could hold in an FMA.

Particulars

Premium customers were customers who were members of SCA's loyalty program and included the following membership levels: Gold Provisional, Gold, Platinum, Black, Ultra Black, Gold Interstate, Platinum Interstate, Black Interstate, Grange Interstate and Grange International.

A player had to satisfy the requirements of a membership level to receive the benefits applicable to that level. For example, to access the Platinum membership level, a customer must have a minimum theoretical spend of $6,000 within a six month period, with a minimum average daily theoretical spend of $200.

c. There were no limits on telegraphic transfers into or out of an FMA, or on cash withdrawals.

d. There were no limits on cash deposits into a customer's FMA subject to the source of funds declaration process from 23 December 2019, which was not an appropriate risk-based procedure.

Particulars

See paragraph 138.b.

e. There were no limits on the amount of money that one customer could transfer from their FMA to the FMA of another customer.

f. Prior to 23 December 2019, there was no requirement for customers to complete a source of funds declaration form and it was optional to provide occupation information.

Particulars

See paragraph 138.a.

g. There were no appropriately risk-based controls in relation to third party transactions.

Particulars

See paragraphs 227 and 231.

219. The failure to appropriately identify, mitigate and manage the ML/TF risks of FMAs exposed SCA to ML/TF risks.

Third party deposits

220. From 7 December 2016, a third party could deposit money into an SCA customer's FMA by:

a. a cash deposit at the SCA Cage;

b. deposit of chips or other CVI at the SCA Cage transfer from another FMA held by the third party via the Funds authorisation form in the circumstances pleaded at paragraph 307;

c. transfer from a bank account via the SCA Customer account channel;

d. until September 2022, transfer from a bank account via the SCEG Customer account channel; or

e. depositing funds into an FMA via the SkyCity New Zealand channel.

Particulars to f.

See *The SkyCity New Zealand channel* below.

(**third party deposits**)

221. For most of the period from 7 December 2016 to about 17 November 2022, SCA's informal policies that purported to limit third party deposits into FMAs:

a. were not supported by documented procedures such that they were not capable of being reliably or consistently applied;

b. were not supported by appropriate documented procedures with respect to all the ways in which a third party could deposit money or funds into an SCA customer's FMA as pleaded at paragraph 220; and/or

c. did not have appropriate regard to ML/TF risks.

Particulars

In the absence of appropriate documented procedures, staff exercised their discretion in relation to whether a third party deposit should be processed, including when third party deposits should be escalated to the AML team.

In the absence of an appropriate ML/TF risk assessment, SCA was not able to understand and manage the ML/TF risks relating to source of funds of third party deposits.

SCA staff engaged in a variety of practices, often ad hoc, to deal with unusual deposits, including third party deposits.

See paragraphs 223 and 224.

222. In the absence of appropriate documented policies with respect to third party deposits:

a. SCA permitted third parties to deposit funds into an SCA customer's FMA where written authorisation via a Funds Authorisation Form was in place;

Particulars

See paragraph 307.

b. the Funds Authorisation Forms that were used by SCA in the circumstances pleaded in paragraph 307 were not used to:

i. understand the source of funds relating to third party transactions; or

ii. understand the nature of the relationship between the customer and the third party.

Particulars

The purpose of a Funds Authorisation Form was to facilitate movement of funds between customers' FMAs: see paragraph 307.

Rule 8.1.5 of the Rules.

c. until September 2022, funds were permitted to be deposited into SCEG Customer accounts (see paragraph 239 below) by third parties for the benefit of another customer, including via:

i. money remitters and corporate entities run by junket operators; and

ii. cash deposits (until September 2021).

Particulars

From on or about April 2021, the SCEG Board approved a policy, which included that only approved international money remitters for international customers attending SCA casino could be used to deposit funds into the SCEG Customer accounts or SCA Customer accounts (see paragraph 269 below). However, SCA had no risk-based processes in place to understand source of funds with respect to deposits through remitters.

See paragraphs 223 and 224.

Transaction receipts or account statements relied on by SCA did not consistently or reliably identify if a deposit had been in cash and, if so, the identity of the person making the deposit.

For example, on 18 January 2018:

a. Company 7, acting on behalf of Customer 15, transferred $626,792 to SCA through the SCEG Customer account channel;

b. Customer 15 transferred $626,792 to Customer 11's FMA; and

c. HKD4,000,000 was transferred into an overseas SCEG account on behalf of Customer 15, which SCA deposited into Customer 15's FMA.

See *Customer 15's risk profile* below.

On 22 January 2019, a foreign company connected to Suncity deposited HKD$4,876,545 into SCEG Customer account. The funds were credited from Customer 1's FMA at a SCEG New Zealand casino to Customer 1's SCA FMA and made available to Customer 1 in the amount of AUD$873,917.

d. SCA permitted funds to be deposited into SCA Customer accounts (see paragraph 269 below) by third parties for the benefit of another customer, including via:

i. money remitters and corporate entities run by junket operators; and

ii. cash deposits.

Particulars

See particulars at paragraph 222c in relation to money remitters.

For example, between 23 December 2016 and 23 July 2019, third parties acting on behalf of Customer 17 transferred a total of $3,600,629 to SCA through the SCA Customer account channel: see *Customer 17's risk profile*, below.

On or around 20 March 2018, Customer 2 engaged the services of Company 1 to transfer $300,000 to one of the SCA Customer accounts. Once SCA received the funds, SCA credited them to Customer 11's FMA in circumstances where the connection between Customer 2 and Customer 11 regarding the funds was not clear. Between 22 February 2017 and 27 November 2017, Customer 2's mining company, Company 2, transferred a total of $1,630,100 to Customer 2's SCA FMA, via the SCA Customer account, over 15 transactions.

See *Customer 2's risk profile* below.

See *Customer 11's risk profile* below.

SCA had no risk-based processes in place to understand source of funds with respect to deposits through remitters.

Transaction receipts or account statements relied on by SCA did not consistently or reliably identify if a deposit had been in cash and, if so, the identity of the person making the deposit.

From September 2021, SCA had an undocumented policy to the effect that it would cease accepting cash deposits through SCA Customer accounts. As this policy was not documented, it was not capable of being reliably or consistently applied. Nor did the policy clearly articulate how cash deposits would be consistently identified and returned.

e. until at least February 2022, SCA accepted transfers of funds from other casinos into a customer's SCA FMA via one of the SCEG Customer accounts, including non-SCEG casinos and casinos located outside of Australia.

Particulars

In December 2021, SCEG introduced the International Business patron accounts standard operating procedure (**International Business SOP**).

In May 2022, the International Business SOP was updated to state that after February 2022 payment to another casino is not permitted and payments from other casinos were not accepted. Transfers to and from FMAs at SCA to a customer's FMA at a SCEG casino were still permitted.

In two transactions on 18 January 2017 and 11 September 2017, SCA accepted transfers totalling $85,469 from overseas casinos on Customer 16's behalf.

See paragraph 247.c.

f. SCA permitted other casinos to transfer funds into an SCA customer's FMA via one of the SCA Customer accounts, including non SCEG casinos and casinos located outside of Australia.

g. third parties were permitted to deposit funds into FMAs at SkyCity New Zealand, which could then be transferred to FMAs held at SCA.

Particulars

See paragraph 220.e.

h. third parties could deposit funds via the SCA Customer account or SCEG Customer account to repay a customer's CCF.

Particulars

SCA permitted loyalty customers to transfer funds from other casinos to repay or redeem an amount owing in relation to the provision of credit.

Third parties were permitted to pay down a debt with respect to the repayment of loans or the redemption of credit. SCA did not have any processes to identify or limit such third party payments.

Third party deposits to redeem credit or repay a loan involved ML/TF risks related to offsetting.

See paragraph 24.

223. Prior to late 2021, there were no appropriate policies or procedures in place to identify or limit cash deposits made into the SCEG Customer accounts.

Particulars

Transaction receipts or account statements relied on by SCA did not consistently or reliably identify whether a deposit had been in cash and, if so, the identity of the person making the deposit.

It was not until late 2021 that an alert was raised on one of the SCEG Customer accounts whenever a teller attempted to process a cash deposit on that account. The alert would attempt to notify the branch teller that cash deposits should not be accepted into the account and that the cash should be returned to the customer. However, the bank was unable to physically prevent cash deposits from occurring.

The December 2021 International Business SOP included in Appendix 2 payment rules for SCEG Customer accounts. It stated that it had been confirmed with Bank 2 that third party cash deposits were no longer accepted by that bank after September 2021. In relation to another of the SCEG Customer accounts, it recorded that third party cash deposits were not accepted by that bank.

224. At no time did SCA have appropriate policies or procedures in place to identify or limit cash deposits made into the SCA Customer accounts.

Particulars

Transaction receipts or account statements relied on by SCA did not consistently or reliably identify if a deposit had been in cash and, if so, the identity of the person making the deposit.

225. It was not until September 2022 that SCEG introduced a documented policy setting out the process for rejecting third party deposits made into SCEG Customer accounts.

Particulars

The policy stated that payments received from third parties were no longer accepted from June 2021. The policy provided for the process for identifying and rejecting third party deposits.

There were some exceptions to this policy relating to joint accounts, approved International Business money remitters, and approval from Compliance or the Financial Crime team for third party payments in exceptional circumstances.

After December 2021 and prior to September 2022, SCEG introduced some documented policies with respect to third party deposits into SCEG Customer accounts. However, they did not provide for any clear procedure for staff to return third party remittance in circumstances in which they were identified.

226. Deposits by third parties into FMAs involved higher ML/TF risks, including:

a. a lack of transparency as to source of funds;

b. a lack of transparency as to the purpose of the transaction; and

c. risks of smurfing, cuckoo smurfing or offsetting.

Particulars

See paragraph 24.

227. At no time did the Standard Part A Programs include appropriate risk-based procedures to:

a. verify the identity of third parties depositing funds into the SCA Customer accounts and SCEG Customer accounts;

b. understand the source of funds relating to third party deposits; or

c. understand the nature of the relationship between the customer and the third party.

Particulars

Rules 8.1.5, 15.2 and 15.3; and paragraphs (l) and (m) of the definition of KYC information in r 1.2.1 of the Rules.

See paragraphs 221 and 222.b.

See, for example, paragraphs 396.g, 396.h, 396.i and 396.j.

Third party transfers

228. For most of the period from 7 December 2016 to about 17 November 2022, SCA would process a transfer of funds from a customer's FMA to a third party (**third party transfer**) in the following circumstances:

a. SCA permitted a customer to transfer from their FMA to a third party's FMA where written authorisation via the Funds Authorisation Form was in place;

Particulars

See paragraph 307.

Policies purporting to limit third party transfers on and from January 2022 were not documented and were not capable of consistent application.

b. until at least June 2021, SCA permitted a customer to transfer funds from their FMA to a personal bank account, which was not in the customer's name, via the SCEG Customer account channel, but this was not the subject of a documented process until December 2021;

Particulars

The December 2021 IP SOP stated that from June 2021 third party transfers were not accepted except for joint accounts or for payments to another casino provided that the payment is directly credited into the same customer's FMA at that casino, or for one of the SCEG Customer accounts they were accepted with the condition that

SkyCity was able to establish relationship subject to that bank's AML approval.

c. SCA permitted a customer to transfer funds from their FMA to a personal bank account, which was not in the customer's name, via the SCA Customer account channel;

Particulars

Policies purporting to limit third party transfers on and from January 2022 were not documented and were not capable of consistent application.

d. until at least February 2022, SCA permitted customers to transfer funds from their FMA to other casinos via one of the SCEG Customer accounts, including non-SCEG casinos and casinos located outside of Australia; and

Particulars

In May 2022, the International Business SOP was updated to state that after February 2022, payments to another casino was not permitted and payments from other casinos were not accepted. Transfers to and from FMAs at SCA to a customer's FMA at a SCEG casino were still permitted.

In three transactions between 16 January 2017 and 6 September 2017, SCA transferred a total of $223,000 from one of the SCA Customer accounts to other overseas casinos on Customer 16's behalf.

e. SCA permitted loyalty members to transfer funds from their FMA to another casino's bank account via the SCA Customer accounts, including non-SCEG casinos and casinos located outside of Australia.

229. For most of the period from 7 December 2016 to on or about 17 November 2022, SCA's informal policies that purported to limit third party transfers from FMAs:

a. were not supported by documented procedures such that they were not capable of being reliably or consistently applied; and/or

b. were not supported by appropriate documented procedures with respect to all the ways in which third party transfers could be processed.

Particulars

In the absence of appropriate documented procedures, staff exercised their discretion in relation to whether a third party transfer should be processed, including when proposed third party transfers should be escalated to the AML team.

230. Transfers from FMAs to third parties involved higher ML/TF risks, including:

a. they often formed part of a complex transaction chain;

b. a lack of transparency as to the purpose of the transaction; and

c. risks of smurfing, cuckoo smurfing or offsetting.

Particulars

See paragraph 24.

231. From 7 December 2016, the Standard Part A Programs did not include any written policies or procedures to appropriately limit or monitor third party transfers from FMAs, having regard to ML/TF risks.

a. There were no policies or procedures to appropriately limit or monitor the transfer of money from one customer's FMA to another customer's FMA.

Particulars

See paragraphs 221 to 225.

b. There were no daily or transaction limits applying to FMAs with respect to outward funds transfers to third parties.

c. There were no risk-based controls to understand the nature of the relationship between the customer and the third party.

Particulars

Rules 8.1.5, 15.2 and 15.3; and paragraphs (l) and (m) of the definition of KYC information in r 1.2.1 of the Rules.

Remittance services - items 31 and 32 table 1, s 6 designated services

232. SkyCity Adelaide was a non-financier.

Particulars

Section 5 of the Act.

233. At all times, with respect to each of the transactions pleaded at paragraphs 249.a, 278.b, 298 and 308.b, SCA made money available, or arranged for it to be made available to customers as a result of transfers under a designated remittance arrangement.

234. At all times, SCA provided designated services at paragraph 233 in the capacity of a non-financier in the course of carrying on a business of giving effect to remittance arrangements.

Particulars

Table 1, s 6 remittance services were regularly provided to customers as part of SCA's business.

The provision of remittance services facilitated gambling (table 3, s 6), including high value gaming and the generation of gambling revenue.

Remittance services were provided and recorded through SCA's systems, including those used for FMAs.

235. At all times, SCA provided designated services within the meaning of item 32, table 1, s 6 when it provided the services described at paragraph 233.

236. At all times, with respect to reach of the transactions pleaded at paragraphs 253, 265.e, 282, 287 and 308.a SCA accepted instructions from the customer for the transfer of money under a designated remittance arrangement.

237. At all times, SCA provided the services described at paragraph 236 in the capacity of a non-financier in the course of carrying on a business of giving effect to remittance arrangements.

Particulars

See particulars at paragraph 234.

238. At all times, SCA provided designated services within the meaning of item 31, table 1, s 6 when it provided the services described at paragraph 236.

The SCEG Customer account channel

239. SCEG maintained bank accounts (**SCEG Customer accounts**) to facilitate the transfer of funds into and out of FMAs for SCA customers or prospective customers.

240. At all times, SCEG maintained up to:

a. 5 accounts in Australian dollars; and

b. 18 foreign currency accounts.

241. The SCEG Customer accounts were a channel through which SCA provided designated services (the **SCEG Customer account channel**).

Particulars

See paragraphs 242 to 268.

Transfers into FMAs through the SCEG Customer account channel

242. At all times, an SCA customer could deposit money, or arrange for money to be deposited into a SCEG Customer account to:

a. transfer front money for a visit to the SCA casino; or

b. repay an amount owed to SCA under a CCF, including;

i. through the transfer of funds from a customer's FMA held at a SCEG New Zealand casino to SCA as pleaded at paragraphs 292 to 300; and/or

ii. by telegraphic transfer, cheque or cash deposit (for certain accounts).

243. SCEG Customer accounts were used by both domestic and international customers of SCA to move money into the SCA casino.

244. SCEG Customer accounts were used by some corporate entities to make deposits on behalf of SCA customers:

a. corporate entities run by junket operators insofar as the customer was a participant in that particular junket program;

b. remittance service providers to deposit funds on behalf of customers; and

c. other corporate entities, including other casinos.

Particulars

See paragraphs 216, 222.c and 222.e.

245. Customers could deposit funds into SCEG Customer accounts by non-face-to-face direct transfer, both from:

a. within Australia; or

b. another country.

246. Funds could be deposited into SCEG Customer accounts by cash, cheque or telegraphic transfer, in either Australian dollars or a foreign currency depending on the account.

247. A customer of SCA could:

a. deposit funds personally into a SCEG Customer account;

b. until September 2022, arrange for a third party to deposit funds into a SCEG Customer account, including money remitters;

Particulars

See paragraph 222.c.

c. until at least February 2022, instruct another casino, including non-SCEG casinos, to transfer funds into one specific SCEG Customer account.

Particulars

Paragraph 222.e.

Only one of the SCEG Customer accounts would receive funds from another casino.

248. SCA customers who wanted to deposit front money into the SCEG Customer accounts were:

a. provided with the SCEG Customer account details by SCA representatives, which included the International Business Sales team; and

b. advised to reference their name and SCA membership number (where the customer had a membership number) as the payment reference (**payment descriptor**).

249. Deposits by or on behalf of customers into SCEG Customer accounts were attributed to a customer of SCA in the following way:

a. a customer provided the SCEG International Business Sales team with a copy of the transaction receipt from the bank as evidence of the deposit, which was forwarded to either the SCEG International Business Patron Accounts team or a SCEG New Zealand casino Cage to reconcile against the bank statements for the SCEG Customer account;

b. details of the deposit were then communicated to SCA, including the transaction receipt;

c. the funds were not physically transferred from the SCEG Customer Account to an SCA Customer account, but remained in the SCEG Customer account until the end of the customer's visit and when settlement occurred; and

d. SCA credited the funds to the customer's FMA when the customer was onsite at the SCA casino.

Particulars

In circumstances where the payment descriptor was not provided in the bank statement of the SCEG Customer account, SCEG and/or

SCA would rely on the details recorded in the transaction receipt from the customer to allocate the funds to the relevant FMA.

250. SCA made money available to a customer when it credited the customer's FMA with the money that had been deposited into the SCEG Customer account.

251. The credit to an FMA, as pleaded at paragraph 250, was a designated service provided by SCA under:

a. item 32, table 1, s 6 of the Act; and

b. item 13, table 3, s 6 of the Act.

Particulars

See paragraph 235.

252. Once the process described at paragraphs 248 and 249 had been completed, an SCA customer could access funds deposited into a SCEG Customer account via their FMA by:

a. obtaining chips or other CVIs, including TITO tickets and casino cheques (items 7 and 13, table 3, s 6 designated services) at the SCA Cage;

b. withdrawing cash in Australian dollars (item 13, table 3, s 6 designated services) at the SCA Cage;

c. accessing the funds by inserting their membership card at an EGM/ETG for the purposes of cashless gaming, including transferring funds from their FMA onto an EGM/ETG as credits (item 13, table 3, s 6 designated service); and

d. withdrawing the funds (in cash or in the form of a TITO) from their FMA by inserting their membership card at a CRT subject to the limits pleaded at paragraphs 348.b and 353.p (item 13, table 3, s 6 designated service).

253. Once the funds had been deposited into an FMA, including via the SCEG Customer account channel, a customer could instruct SCA to transfer the funds out of the FMA to:

a. the customer's personal bank account or to a third party bank account;

b. the bank account of another casino (Australian or foreign) until at least February 2022;

Particulars

See paragraph 228.d.

c. a SCEG casino in New Zealand in circumstances where the customer held an FMA at that SCEG casino in New Zealand; and

d. another customer's FMA where a Funds Authorisation Form was in place;

Particulars

See paragraphs 228 and 307.

254. The acceptance by SCA of each of the instructions pleaded at paragraphs 253.a to 253.d was an item 31, table 1, s 6 designated service and an item 13, table 3, s 6 designated service.

Particulars

See paragraphs 237 and 238

See the particulars at paragraph 234.

255. The provision of item 13, table 3 and item 32, table 1, s 6 designated services through the SCEG Customer account channel involved higher ML/TF risks, including risks arising by reason of the following:

a. Designated services provided through the SCEG Customer account channel were facilitated through FMAs, which involved the ML/TF risks pleaded at paragraph 218.

b. Money was deposited into SCEG Customer accounts through non-face-to-face channels.

c. Most of the SCEG Customer accounts were located offshore and SCA customers could deposit money into the SCEG Customer accounts offshore, including in foreign currencies.

d. Money could be made available to an SCA customer in Australia through the SCEG Customer account channel without the need for a cross-border transfer of funds.

Particulars

See paragraph 249(c).

e. SCA accepted cash deposits through some of the SCEG Customer accounts.

f. SCA accepted deposits into some SCEG Customer accounts from third parties (both telegraphic and cash) including some corporate third party entities.

Particulars

For example, on 18 January 2018, Company 7 acting on behalf of Customer 15 transferred $626,792 to SCA through the SCEG Customer account channel. HKD4,000,000 was transferred into an overseas SGEG account on behalf of Customer 15, which SCA deposited into Customer 15's FMA.

On 18 January 2018, Customer 15 transferred $626,792 from their SCA FMA to Customer 11's SCA FMA.

SCA determined the originator of funds was Customer 11, who used Company 7 to move funds out of a foreign country without government detection and Customer 15's account was used to further distance Customer 11 from the transaction. See *Customer 15's risk profile* below.

See paragraphs 222.c and 223.

g. Deposits from overseas remitters were accepted for or on behalf of SCA customers.

Particulars

From on or about April 2021, the SCEG Board approved a policy, which included that only approved international money remitters for international customers attending SCA casino could be used to deposit funds into the SCEG Customer accounts or SCA Customer accounts.

h. Money could be received from other casinos to one of the SCEG Customer accounts, including non-SCEG casinos and casinos located outside of Australia until at least February 2022.

Particulars

See paragraph 222.e.

See the particulars at paragraph 247.c.

i. Money could be moved across international borders through SCEG Customer accounts.

j. Money could be remitted across international borders without the physical movement of funds into Australia, including by junket operators (including corporate junket operators), overseas remitters and other third parties.

k. A third party could deposit money into SCEG Customer accounts to redeem a debt owed by an SCA customer under an CCF by first crediting the FMA.

l. A junket operator could disburse funds transferred through the SCEG Customer account channel, and credited to their FMA, to third parties including junket players

Particulars.

See paragraph 412.d.

m. The ML/TF risks posed by the matters pleaded at b. to m above were exacerbated because money could be remitted from an FMA to a third party.

Particulars

See paragraph 267.f.

256. The features pleaded at sub-paragraphs 255 a. to 255.m:

a. reduced the transparency of transactions;

b. allowed opportunities for layering transactions across multiple accounts and currencies; and

c. created distance between the ultimate source of funds and the ultimate designated service provided by SCA.

Particulars

For example, see the risks pleaded at paragraph 24c, e, f and i.

See paragraphs 480-481.

257. From 24 May 2019, one of the SCEG Customer accounts was in the name of Horizon Tourism (New Zealand) Limited (the **Horizon Tourism account**).

Particulars

At all material times, the ultimate holding company of Horizon Tourism (New Zealand) Limited is SCEG.

Prior to July 2019, Horizon Tourism (New Zealand) Limited was known as SkyCity Wellington Limited.

258. The Horizon Tourism account was a channel through which SCA provided designated services (the **Horizon Tourism account channel**).

259. The Horizon Tourism account channel posed particularly high ML/TF risks:

a. the Horizon Tourism accounts were in the name Horizon Tourism (New Zealand) Limited and were used or capable of being used by SCA customers for debt repayments, including by third parties on behalf of SCA customers;

b. junket operators used these accounts, as did individuals residing in Australia or outside of Australia;

c. the accounts were not transparent because their connection to SCA was not apparent on their face; and

d. deposits from overseas remitters were accepted for or on behalf of SCA customers.

Particulars

Based on its records, SCA understood that Customer 2 deposited funds into the Horizon Tourism account for gambling at SCA due to concerns about his bank closing his account as a result of transactions with casinos.

On 10 September 2019, a third party company overseas transferred $300,000 on behalf of Customer 2 to the Horizon Tourism account. A SCEG New Zealand casino then transferred the funds to Customer 2's SCA FMA.

260. SCA failed to appropriately assess the ML/TF risks of providing item 13, table 3, s 6 designated services through the SCEG Customer account channel.

261. SCA failed to assess the ML/TF risks of providing item 32 and item 31, table 1, s 6 designated services through the SCEG Customer account channel.

262. The Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by SCA with respect to designated services provided on FMAs through the SCEG Customer account channel, including for the following reasons:

a. The Standard Part A Programs did not include appropriate risk-based controls to identify, mitigate and manage the ML/TF risks pleaded at paragraphs 255 and 257.

b. There were no appropriate risk-based controls to understand the source of funds deposited into SCA FMAs through the SCEG Customer account channel.

c. SCA did not have appropriately risk-based controls in relation to third party transactions.

Particulars

See paragraphs 227 and 231.

d. There was no requirement or process to ensure the person who deposited funds into the SCEG Customer account was the same person who would use those funds for gambling at SCA.

e. There were no appropriate systems and controls to identify and record the source of funds for deposits into SCEG Customer accounts by overseas remitters for or on behalf of SCA customers.

Particulars

Evidence of deposits into SCEG Customer accounts by overseas remitters (such as a receipt) would be emailed by the International Business Patron Accounts team to the SCA Cage with details of the customer and the customer's trip. SCA Cage staff would print hard copies of the email and store them in an individual packet relating to the specific trip. At all times, the packets were stored in hard copy and after October 2018, the packets were also scanned into network drives.

From on or about April 2021, the SCEG Board approved a policy, which included that only approved international money remitters for international customers attending SCA casino could be used to deposit funds into the SCEG Customer accounts or SCA Customer accounts. However, SCA had no risk-based processes in place to understand source of funds with respect to deposits through remitters

f. Prior to December 2021, there were no controls or procedures to identify or limit cash deposits into SCEG customer accounts.

Particulars

See paragraph 223.

g. There was no requirement that a source of funds check be applied to customers that deposited cash into SCEG Customer accounts.

h. There were no appropriately documented policies or procedures in relation to accepting third party deposits, including guidance as to how staff should exercise their discretion to accept funds from a third party or providing for senior management approval or escalation in relation to processing third party deposits.

Particulars

See paragraph 221.

i. SCA did not have appropriate systems in place to ensure the name of the person who deposited the funds would be recorded in Bally when a customer's FMA was credited with respect to third party deposits.

j. There were no transaction or daily limits on the amount of money that could be transferred by or on behalf of a premium customer through the SCEG Customer account channel and subsequently credited to a customer's FMA.

Particulars

See paragraph 218.c.

Transfers out of FMAs through the SCEG Customer account channel

263. At all times, SCA accepted instructions from its customers to transfer money from customers' FMAs to bank accounts via the SCEG Customer accounts, including for the purposes of:

a. returning front money to customers; and

b. paying a customer winnings.

Particulars

In circumstances where a customer had deposited funds into the SCEG Customer accounts for the purposes of gambling at SCA, the funds were held in that account until the end of the visit, at which time settlement took place. Any money remaining in the SCEG Customer account from the customer's original deposit was transferred to the customer's nominated bank account.

At the completion of an international customer's visit to the SCA casino, a customer could request that their winnings to be paid via the SCEG Customer accounts depending on the currency the customer wished to be paid.

264. Transfers out of FMAs, via the SCEG Customer account channel, as pleaded at paragraph 263, involved the provision of:

a. item 31, table 1, s 6 designated services by SCA; and

b. item 13, table 3, s 6 designated services on FMAs.

Particulars

See paragraph 238.

265. A customer could request to withdraw funds from their FMA and transfer them to a personal bank account while onsite at SCA or not on site at SCA. For international bank transfers in foreign currencies:

a. the customer was required to complete a TT Request Form to authorise the transfer;

b. the TT Request Form recorded details relating to the transaction, including details of the receiving bank account to which the funds would be transferred.

c. the SCA Cage team would send the completed TT Request Form to the International Business Patron Accounts team to action.

d. the International Business Patron Accounts team would then:

i. review the TT Request Form;

ii. convert the funds to the relevant foreign currency; and

iii. email a SCEG New Zealand casino Cage team the details of the transfer and any other supporting paperwork (including evidence of winnings at the SCA casino).

e. the payment would then be approved, and the customer's instruction for the transfer of money accepted, in accordance with the Group Bank Signatory Policies prior to being processed into the customer's nominated bank account;

f. The SCA Finance team and a SCEG New Zealand casino Finance team would then complete an inter-company journal entry to reflect the movement of funds.

266. For international bank transfers in Australian dollars:

a. the customer was required to complete a TT Request Form to authorise the transfer;

b. the SCA Cage team would provide the SCA Finance team or the International Business Patron Accounts team with details of the transfer (including a copy of the TT Request Form);

c. upon receiving the relevant details relating to the transaction, the SCA Finance team would make payment to the customer or the payment would then be approved in accordance with the Group Bank Signatory Policies prior to being processed into the customer's nominated bank account; and

d. SCA accepted the customer's instructions for the transfer of money when the transfer was approved for processing.

267. The provision of item 31, table 1, s 6 designated services through the SCEG Customer channel involved higher ML/TF risks, including risks arising by reason of the following:

a. Designated services provided through the SCEG Customer account channel were facilitated through FMAs, which involved the higher ML/TF risks pleaded at paragraph 216.

b. Remittance services were often provided as part of a complex chain of different designated services under table 1 and 3, s 6 of the Act.

c. There were no transaction limits on telegraphic transfers out of an FMA as pleaded at paragraph 218.c.

d. A customer could access funds through non-face-to-face channels by requesting a transfer of their funds from their FMA to another bank account, including the bank account of a third party.

e. Money could be remitted out of Australia through the SCEG Customer account channel without the need for a cross-border transfer of funds.

Particulars

See paragraphs 249(c).

f. Funds could be transferred from a customer's FMA to a bank account in the name of a third party via the SCEG Customer account channel until at least June 2021.

Particulars

See paragraph 228.b.

g. Funds could be transferred to the bank account of another casino via one of the SCEG Customer accounts, including non-SCEG casinos and casinos located outside of Australia until May 2022.

Particulars

See paragraph 228.d.

h. Funds sourced from FMAs could be moved across international borders through the SCEG Customer account channel.

268. The Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by SCA with respect to item 31, table 1, s 6 designated services provided on FMAs through the SCEG Customer account channel, including for the following reasons.

a. The Standard Part A Programs did not include appropriate risk-based controls to identify, mitigate and manage the ML/TF risks pleaded at paragraph 267.

b. The Standard Part A Programs did not include appropriate preventative controls to mitigate and manage ML/TF risks, such as:

i. controls to restrict remittance to third parties; or

Particulars

See paragraph 267.f.

ii. transaction limits on telegraphic transfers out of an FMA as pleaded at paragraph 218.c; or

iii. providing for senior management approval or escalation in relation to processing third party transactions,

c. The Standard Part A Programs did not include appropriate risk-based controls to identify, mitigate and manage the ML/TF risks of remittance services provided through junket channels.

Particulars

See paragraph 412.

d. SCA did not have appropriate risk-based systems and controls to identify customers who had requested to withdraw funds from FMAs who had engaged in minimal or no gaming.

Particulars

Staff observation and the largely manual transaction monitoring processes would not have been able to consistently identify customers requesting a withdrawal of funds from their FMA who had engaged in minimal or no gaming.

See The Standard Part A Programs – Transaction monitoring program below.

The SCA Customer account channel

269. SCA operated two bank accounts in Australian dollars (**SCA Customer accounts**) to facilitate the transfer of funds into and out of FMAs.

270. SCA Customer accounts were used by both domestic and international customers of SCA to move money into and out of the casino.

271. The SCA Customer accounts were a channel through which SCA provided designated services (the **SCA Customer account channel**).

Particulars

See paragraph 272 to 291.

Transfers into FMAs through the SCA Customer account channel

272. At all times, an SCA customer could deposit money, or arrange for money to be deposited into an SCA Customer account including for the purposes of:

a. Making front money available to the customer for gaming; or

b. repaying an amount owed to SCA under a CCF.

273. SCA Customer accounts were used by some corporate entities to make deposits on behalf of SCA customers, including by:

a. corporate entities run by junket operators insofar as the customer was a participant in that particular junket program;

b. remittance service providers to deposit funds on behalf of customers; and

c. other corporate entities, including other casinos.

Particulars

See paragraphs 216, 222.d and 222.f.

274. Customers could deposit funds into SCA Customer accounts by non-face-to-face direct transfer, both from:

a. within Australia; or

b. another country.

275. Funds could be deposited into SCA Customer accounts by cash, cheques or telegraphic transfer, in Australian dollars.

276. A customer of SCA could:

a. deposit funds personally into an SCA Customer account;

b. arrange for a third party to deposit funds into an SCA Customer account in certain circumstances, including via money remitters; and

Particulars

See paragraph 222.d.

c. instruct another casino to transfer funds into an SCA Customer account to be credited to the customer's FMA, including non-SCEG casinos and casinos located outside of Australia.

277. Customers who wanted to deposit front money into the SCA Customer accounts were:

a. provided with the SCA Customer account details by SCA staff; and

b. advised to reference their name and SCA membership number (whether the customer had a membership number) as the **payment descriptor**.

278. Deposits by or on behalf of customers into SCA Customer accounts were attributed to a customer of SCA by:

a. A customer would notify SCA staff of a deposit being made in the SCA Customer account and provide evidence of the deposit, including bank transfer receipts.

b. Once SCA had confirmed the amount had been received from the customer, SCA would credit the funds to the customer's FMA.

Particulars

In circumstances where the payment descriptor was not provided in the bank statement, SCA would rely on the details recorded in the transaction receipt from the customer to allocate the funds to the relevant FMA.

279. SCA made money available to a customer when it credited the customer's FMA with the money that had been deposited into the SCA Customer account.

280. The credit to a customer's FMA, as pleaded at paragraph 279, was a designated service provided under:

a. item 32, table 1, s 6 of the Act; and

b. item 13, table 3, s 6 of the Act.

Particulars

See paragraph 235.

281. Once the process at paragraph 278 had been completed, a customer of SCA could access funds deposited into an SCA Customer account via their FMA as follows:

a. obtaining chips or other CVIs (items 7 and 13, table 3, s 6 designated services) at the SCA Cage;

b. withdrawing cash in Australian dollars (item 13, table 3, s 6 designated services) at the SCA Cage;

c. accessing the funds by inserting their membership card at an EGM/ETG for the purposes of cashless gaming, including transferring funds from their FMA onto an EGM/ETG as credits (item 13, table 3, s 6 designated service); and

d. withdrawing the funds (in cash or in the form of a TITO) from their FMA by inserting their membership card at a CRT subject to the limits pleaded at paragraphs 348.b and 353.p (item 13, table 3, s 6 designated service).

282. Once funds had been deposited into an FMA, including via the SCA Customer account channel, a customer could instruct SCA to transfer the funds to:

a. the customer's personal bank account or to a third party account;

b. another casino, including non-SCEG casinos and casinos located outside of Australia;

c. another customer's FMA where written authorisation via the Funds Authorisation Form was in place;

Particulars

See paragraph 307.

d. a SCEG casino in New Zealand in circumstances where the customer held an FMA at that SCEG casino in New Zealand.

Particulars

The acceptance by SCA of each of the instructions pleaded at paragraphs 282a. to 282d. was an item 31, table 1, s 6 designated service and an item 13, table 3, s 6 designated service.

See paragraphs 234, 237 and 238.

283. The provision of item 13, table 3 and item 32, table 1, s 6 designated services through the SCA Customer account channel involved higher ML/TF risks, including risks arising by reason of the following.

a. Designated services provided through the SCA Customer account channel were facilitated through FMAs, which involved the ML/TF risks pleaded at paragraph 218.

b. Funds could be deposited into SCA Customer accounts through non-face-to-face channels.

c. Customers deposited funds into the SCA Customer account from overseas.

d. Deposits from overseas remitters were accepted for or on behalf of SCA customers and could be used to facilitate the movement of funds into the SCA Customer accounts from international jurisdictions.

Particulars

From on or about April 2021, the SCEG Board approved a policy, which included that only approved international money remitters for international customers attending SCA casino could be used to deposit funds into the SCEG Customer accounts or SCA Customer accounts. However, SCA had no risk-based processes in place to understand source of funds with respect to deposits through remitters

e. Money could be received from other casinos to the SCA Cage Account.

f. SCA accepted deposits into the SCA Customer accounts from third parties, including some corporate third parties.

g. SCA accepted cash deposits through the SCA Customer accounts.

284. SCA failed to assess the ML/TF risks of providing item 13, table 3, s 6 designated services through the SCA Customer account channel.

Particulars

See *The risk assessments* above.

285. SCA failed to assess the ML/TF risks of providing item 32, table 1, s 6 designated services through the SCA Customer account channel.

Particulars

See *The risk assessments* above.

286. The Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by SCA with respect to designated services provided on FMAs through the SCA Customer account channel, including for the following reasons.

a. There were no appropriate risk-based policies or procedures to understand the customer's source of funds.

b. There were no controls or procedures to identify or limit cash deposits into SCA Customer accounts, which were subsequently credited to a customer's FMA.

c. SCA did not have any appropriately documented policies or procedures in relation to accepting third party transactions, including appropriate risk-based policies or procedures.

Particulars

See paragraphs 221 and 227.

In about September 2021, representatives of the bank at which the SCA Customer accounts were held informed representatives of SCA that it had undertaken a review of transactions conducted on the one of the SCA Customer accounts (the SCA Cage account) during the period between September 2019 and May 2021 and had concerns about the transactions that had occurred on that account, including in relation to structuring and layering of transactions to avoid threshold reporting obligations and the inability to satisfactorily link the names of bank account payments to the reference (e.g. customer name) of those payments.

In response to those concerns, the Business Development Executive – Australia Domestic conducted a manual review of a sample of telegraphic transfers into the SCA Cage account between 4 September 2019 and 5 October 2021 at the direction of the AML Compliance Manager. The Business Development Executive – Australia Domestic identified potentially suspicious transactions, which were escalated to the AML Compliance Manager. SCA did not believe the transactions were suspicious and conducted some enhanced due diligence on customers identified by the Business Development Executive – Australia Domestic.

The review was not conducted by reference to any documented methodology with respect to ML/TF risk.

The results of the review were not escalated to the SCEG Board or the AFRC.

Transfers out of FMAs through the SCA Customer account channel

287. At all times, SCA accepted instructions from its customers to transfer money from customers' FMAs, including for the purposes of:

a. returning front money to customers; and

b. paying a customer winnings.

Particulars

The SCA Cage account was not used for outward transfers to overseas recipients.

SCA accepted the customer's instructions for the transfer of money when the transfer was approved for processing.

288. Transfers out of FMAs, via the SCA Customer account channel, as pleaded at paragraph 287, involved the provision of:

a. item 31, table 1, s 6 designated services by SCA; and

b. item 13, table 3, s 6 designated services on FMAs.

Particulars

See paragraphs 234 and 236 to 238.

289. The provision of item 31, table 1, s 6 designated services through the SCA Customer account involved higher ML/TF risks, including risks arising by reason of the following.

a. Designated services through the SCA Customer account channel were facilitated through FMAs, which involve the ML/TF risks pleaded at paragraph 218.

b. Remittance services were often provided as part of a complex chain of different designated services under tables 1 and 3, s 6 of the Act.

c. There were no daily or transaction limits applying to FMAs with respect to withdrawals.

d. Funds sourced from FMAs could be transferred to third parties.

Particulars

See *Third party transfers* above.

e. SCA did not have appropriate risk-based systems and controls to identify customers requesting a withdrawal of funds from FMAs who had engaged in minimal or no gaming.

290. SCA failed to assess the ML/TF risks of providing item 31, table 1, s 6 designated services through the SCA Customer accounts.

Particulars

See *The Risk assessments* above.

291. The Standard Part A Programs did not include appropriate risk-based systems and controls that were capable, by design, of identifying, mitigating and managing the ML/TF risks reasonably faced by SCA with respect to item 31, table 1, s 6 designated services provided on FMAs and through the SCA Customer account channel, including for the following reasons.

a. The Standard Part A Programs did not include appropriate risk-based controls to identify, mitigate and manage the ML/TF risks pleaded at paragraph 289.

b. The Standard Part A Programs did not include appropriate preventative controls to mitigate and manage ML/TF risks, such as controls to:

i. restrict remittance to third parties;

ii. impose daily or transaction limits on remittance; or

iii. provide for senior management approval or escalation in relation to processing third party transactions.

Particulars

See paragraph 218.

c. SCA did not have appropriate risk-based systems and controls to identify customers requesting a withdrawal of funds from FMAs who had engaged in minimal or no gaming.

The SkyCity New Zealand channel

292. At all times, the SCEG had casinos based in New Zealand.

293. From 7 December 2016 to about 17 November 2022, a customer with funds in an FMA at a SCEG casino could request SCEG staff to transfer all or some of those funds to the customer's FMA at SCA (the **SkyCity New Zealand channel**).

294. SCA customers could use the SkyCity New Zealand channel to:

a. make funds available to their FMA at SCA; or

b. repay a debt owed by the customer to SCA under a CCF from their gaming at SCA.

295. A customer would initiate a transfer request by completing a template letter, which identified:

a. their FMA at SCEG New Zealand;

b. the amount to be transferred; and

c. the location that the amount was to be transferred to, being SCA.

296. Once the customer had completed the template letter, the SCEG staff would confirm the value of funds held in that account before proceeding with the request. The International Business Patron Accounts team or a SCEG New Zealand casino Cage team would then provide the details of the transaction to the SCA Cage team by email to facilitate the crediting of the customer's FMA.

297. The transfer of funds from a customer's FMA at a SCEG casino to a customer's FMA at SCA was reflected in an inter-company journal entry.

298. When the customer presented in person at the SCA Cage, SCA credited the funds to a customer's FMA at SCA. An entry was made on the customer's FMA in Bally to record the crediting of the funds.

299. SCA made money available to a customer when it credited the customer's FMA as a result of transfers under a designated remittance arrangement.

300. The credit of funds to the FMA, as pleaded at paragraph 299, was an item 32, table 1, s 6 designated service and an item 13, table 3, s 6 designated service.

Particulars

See paragraphs 234 to 235.

301. Once funds had been credited to a customer's FMA at SCA, a customer could access the by:

a. obtaining chips or other CVIs, including TITOs and casino cheques at the SCA Cage (items 7 and 13, table 3, s 6 designated service);

b. withdrawing cash in Australian dollars at the SCA Cage (item 13, table 3, s 6 designated services);

c. accessing the funds by inserting their membership card at an EGM/ETG for the purpose of cashless gaming, including transferring funds from their FMA onto an EGM/ETG as credits (item 13, table 3, s 6 designated service); and/or

d. withdrawing the funds (in cash or in the form of a TITO) from their FMA by inserting their membership card at a CRT subject to the limits pleaded at paragraphs 348.b and 353.p (item 13, table 3, s 6 designated service).

302. The provision of item 13, table 3 and item 32, table 1, s 6 designated services through the SkyCity New Zealand channel involved higher ML/TF risks, including risks arising by reason of the following:

a. funds could be deposited into SCEG Customer accounts or other accounts held by SCEG entities for the purposes of being made available through the SkyCity New Zealand channel;

b. third parties could deposit funds in SkyCity New Zealand FMAs, including by presenting at the SkyCity New Zealand casino Cage with cash, chips, cheques or other CVIs;

c. a third party could deposit funds into bank accounts held by other SCEG entities for the purposes of having the funds made available to a customer's FMA through the SkyCity New Zealand channel;

d. SCA accepted deposits into some SCEG Customer accounts from third parties (both telegraphic and cash), including some corporate third party entities until September 2022;

e. money could be remitted across international borders in an offsetting process that bypassed the traditional banking system; and

Particulars

The transfer of funds between a customer's SCEG New Zealand FMA and SCA FMA was recognised via an incremental increase in the balance of funds held in the customer's SCA FMA and corresponding decrease in the funds held in the customer's SCEG New Zealand FMA. This was typically done by an inter-company journal entry, rather than a transfer of funds between SCA and SCEG bank accounts at the time the funds transfer took place.

For example, on 22 January 2019, a foreign company connected to Suncity used the SCEG Customer Account channel to deposit HKD$4,876,545 into a SCEG customer account. A SCEG New Zealand casino then used the SkyCity New Zealand channel to transfer the funds from Customer 1's FMA held at the SCEG New Zealand casino to Customer 1's SCA FMA. The funds were made available to Customer 1 in the amount of AUD$873,917, and were used to repay an outstanding line of credit for a Suncity junket.

See *Customer 1's risk profile*, below.

f. there were no appropriate limitations or controls on an SCA customer receiving funds via the SkyCity New Zealand channel, including from a third party's FMA, and cashing out those funds with minimal or no gaming.

Particulars

See particulars to paragraph 306.e.

See Customer 20.

303. The features pleaded at paragraphs 302.a to 302.f

a. reduced the transparency of transactions;

b. allowed opportunities for layering transactions; and

c. created distance between the ultimate source of funds and the ultimate designated service provided by SCA.

Particulars

For example, see the risks pleaded at paragraph 24c, e, f and i.

304. SCA failed to appropriately assess the ML/TF risk of providing item 13, table 3, s 6 designated services via the SkyCity New Zealand channel.

Particulars

See *The risk assessments* above.

305. SCA failed to appropriately assess the ML/TF risk of providing item 32, table 1, s 6 designated services via the SkyCity New Zealand channel.

Particulars

See *The risk assessments* above.

306. The Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by SCA with respect to designated services provided on FMAs through the SkyCity New Zealand channel, including for the following reasons:

a. There were no limits on the funds that could be transferred into an FMA through the SkyCity New Zealand channel.

b. There was no process in place for SCA to satisfy itself as to the source of funds being transferred via the SkyCity New Zealand channel.

c. Prior to October 2020, there was also no process in place for source of funds checks to be applied by the SCEG staff when a customer requested funds to be transferred via the SkyCity New Zealand channel.

d. From October 2020, if SCEG staff considered the transaction to be suspicious it could have resulted in the customer being required to provide verified information about the source of their wealth or funds. There was no documented process in place to communicate those results to the SCA AML team.

e. There were no controls in place requiring the SCA customer to apply the funds to gaming or to the repayment of a debt owed to SCA.

Particulars

On 28 December 2018, at Customer 20's request, SCA facilitated the inter-company transfer of approximately NZD$1,000,000 via the SkyCity New Zealand channel. The funds were part of Customer 20's winnings made as the main player on Customer 8's junket program at the SCEG New Zealand casino. The funds were then transferred to Person 16's SCA FMA. The same day, Person 16 travelled from Melbourne to SCA, purchased a suitcase nearby, withdrew the funds from their FMA in cash and flew back to Melbourne carrying the $1,000,000 in cash.

Between around 9 January 2019 and 25 January 2019, SCA facilitated inter-company transfers totalling over $4,700,000 from Customer 20's FMA at a SCEG New Zealand casino to Person 16's SCA FMA, via Customer 20's SCA FMA, despite neither Customer 20 nor Person 16 gaming at SCA during this period.

f. The limitations or controls on the SCA customer transferring the funds to the FMA of another customer were limited, not supported by appropriate documented policies and not appropriately risk-based.

Particulars

See paragraph 307.

Items 31 and 32, table 1, s 6 designated services – transfers between FMAs

307. SCA could transfer money from one customer's FMA (the **first customer**) to another customer's FMA (the **second customer**) at the first customer's request where written authorisation via a Funds Authorisation Form was in place.

Particulars

SCA permitted the transfers in at least the following circumstances:

i. an individual commission program player from their FMA to another individual commission program player's FMA;

ii. from 14 February 2017, a junket operator provided written authorisation via a Funds Authorisation Form to enable a junket representative to conduct transactions on the junket operator's behalf from the junket operator's FMA;

iii. a junket operator to a junket player's FMA;

iv. a junket player to a junket operator's FMA;

v. a junket representative to another junket representative's FMA;

vi. a junket representative to a junket player's FMA; and

vii. a junket player to a junket representative's FMA.

See paragraph 222.b.

On 31 May 2018, Customer 2 asked SCA staff to issue them a blank cheque for $80,000. SCA staff informed Customer 2 that this was not possible. Shortly after, Customer 2 requested that $80,000 be transferred from their FMA to their spouse's FMA. Once the transfer was completed, Customer 2's spouse asked for a $80,000 cheque to be issued in their name. SCA issued this cheque. SCA noted that the spouse did not game with the funds. On 3 June 2018, Customer 2 again transferred $80,000 to their spouse's SCA FMA. The spouse again did not game with the funds, and requested that a cheque for $80,000 be issued in their name. SCA issued this cheque. SCA noted that Customer 2's spouse was an infrequent visitor to SCA and had no recorded gaming.

308. At all times, when SCA transferred money from the first customer's FMA to the second customer's FMA, SCA:

a. accepted instructions from the first customer for the transfer of money under a designated remittance arrangement; and

b. made money available, or arranged for it to be made available to the second customer as a result of transfers under a designated remittance arrangement.

309. At all times, SCA provided designated services within the meaning of item 32, table 1, s 6 when it provided the services at paragraph 308.a.

Particulars

See paragraph 308.b.

310. At all times, SCA provided designated services within the meaning of item 31, table 1, s 6 when it provided the services described at paragraph 308.b.

Particulars

See paragraph 308.a.

311. At no time did SCA carry out an appropriate ML/TF risk assessment of items 31 and 32, table 1, s 6 designated services.

Particulars

See *The risk assessments* above.

312. The Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by SCA with respect to items 31 and 32, table 1, s 6 designated services provided with respect to transfers between FMAs, including for the following reasons:

a. There were no appropriate preventative controls applied to remittance services to mitigate and manage ML/TF risks, such as controls to:

i. restrict remittance to and from third parties;

Particulars

See paragraphs 221 and 229.

ii. impose daily or transaction limits on remittance; or

iii. appropriately documented policy providing for senior management approval or escalation in relation to processing a third party transactions.

b. There were no appropriate processes in place to understand the reasons for FMA to FMA transfers, including the relationship between the customers and source of funds.

Particulars

See paragraphs 138 and 139.

c. SCA facilitated the distribution of winnings from junket operators or representatives to individual junket players:

i. This could be done by transferring funds from the FMA of a junket operator or representative to the FMA of a junket player;

ii. SCA had very limited or no visibility over how winnings were attributed to junket players.

Particulars

See paragraphs 399 to 405.

Loans – items 6 and 7, table 1, s 6 designated services

313. The Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by SCA with respect to item 6 and 7, table 1, s 6 designated serviced for the reasons pleaded at paragraphs 314 to 343 below.

Cheque cashing facilities – item 6, table 1, s 6 designated services

314. At all times, SCA provided Cheque Cashing Facilities (**CCFs**) to customers.

Particulars

CCFs were available to international and domestic customers, including junket operators where the customer had an FMA.

315. Prior to March 2020, a customer applied for a CCF by completing and signing a 'CCF Standard Application Form' (the **CCF Application**).

316. From March 2020:

a. individual customers were required to complete and sign an 'Individual Credit Application Form' (the **Individual CCF Application**); and

b. junket operators were required to complete and sign the 'Group Operator Credit Application Form' (the **junket operator CCF Application**).

(collectively, the **2020 CCF Application**).

317. Customers either requested a credit limit in their CCF Application or it was negotiated with SCA. The International Business Patron Account Teams determined a suitable credit limit depending on the customer's creditworthiness.

318. If an application and credit limit was approved, an authorised employee signed or approved the application.

319. The CCF Application and 2020 CCF Application, once signed by the applicant, and approved or signed by the authorised employee, operated as an agreement between SCA, and the applicant (the **CCF Agreement**).

320. Once the CCF Agreement was in place, the customer could access funds up to the approved limit at SCA and, in some circumstances, could draw down on the facility on multiple occasions within the approved limit.

321. SCA made a loan to a customer upon the execution or approval of the CCF Agreement with respect to the CCF.

Particulars

A CCF was an advance of money by SCA to the customer.

Paragraph (a) of the definition of 'loan' in s 5 of the Act.

322. At all times, SCA made loans as described at paragraphs 320 and 321 in the course of carrying on a loans business.

Particulars

The provision of CCFs as loans was a core activity of SCA's that facilitated gaming (table 3, s 6 designated services) and the generation of gaming revenue.

CCFs were provided to international business customers, including individual players and junket operators. From 1 January 2017 to December 2020, SCA made over $23,000,000 in junket revenue.

In the 2017, 2018, and 2019 calendar years the total value of approved CCFs for SCA international business individual players was $253,400,000 and $1,200,000,000 for junket operators.

In 2020, in which gaming activity was reduced due to COVID-19-related travel restrictions and lockdowns, the total value of approved CCFs for SCA international business individual players was $60,400,000 and $42,000,000 for junket operators.

These services were provided and recorded through SCA's systems and were the subject of documented processes and procedures.

323. At all times the execution or approval of the CCF Agreement included the provision of an item 6, table 1, s 6 designated service.

Cheque cashing facilities – item 7, table 1, s 6 designated services

The drawdown of funds under a CCF

324. A customer could draw on an approved CCF at the SCA casino premises.

325. Once the CCF had been approved, the funds were credited to a customer's FMA. (**the drawdown of funds under a CCF**)

326. A customer could then apply those funds in a number of ways:

a. a customer could be issued with cash in the amount of 5% of their approved CCF up to a maximum of $25,000 (unless approved by SCA management);

b. a customer could be issued with chips or a CPV;

Particulars

Junket operators, junket representatives and individual commission program players were issued specific gaming chips, being non-negotiable and commission branded gaming chips. Cage staff would not cash out these chips without international business management approval.

c. customers (other than individual commission program players, junket operators and junket representatives) could use their SCA loyalty card at any EGM, CRT or ATG.

327. Before a customer drew down on funds from their CCF by any one of the means pleaded at paragraph 325:

a. The customer would present a personal cheque to SCA Cage staff or to the International Business Patron Accounts team at a SCEG New Zealand casino. The cheque was required to be a signed blank personal cheque.

b. During the period 7 December 2016 to on or about 17 November 2022, SCA accepted foreign drafts as the personal cheque required to be presented.

c. The customer would be issued with a 'credit marker' or 'counter cheque' by SCA in substitution for a personal cheque.

d. From 3 March 2020, a credit marker could be used rather than a customer providing SCA with a cheque.

Particulars

A credit marker refers to the practice of creating counter cheques to debit FMAs.

328. A counter cheque was a document issued by SCA that:

a. included a customer's bank account details, including BSB, account number and account name;

b. was required to be signed by the customer;

c. was bankable;

d. was drawn against a customer's CCF at buy-in in the case of Australian domestic customers who held an Australian bank account; and

e. was drawn against a customer's approved CCF limit during the course of the gaming visit for international business customers.

329. A drawdown of funds from a CCF was a transaction in relation to a loan where the loan was made in the course of carrying on a loans business.

Particulars

See the particulars at paragraph 322.

330. SCA provided an item 7, table 1, s 6 designated service when it provided a customer with a drawdown of funds from a CCF.

Repayments under a CCF

331. A customer could repay funds owed to SCA under a CCF in the ways pleaded at paragraphs 332 to 339.

332. CCFs were made available to approved applicants on the condition that any debit balances would be settled by a fixed date.

Particulars

From March 2020, the advance of credit forms provided that all credit advanced must be repaid within 5 working days for local or interstate customers or 20 working days for international customers and Group Operators at the end of that trip.

333. If a customer did not repay or settle their outstanding debt under a CCF to SCA by the agreed due date following the customer's gaming trip, SCA reserved the right to insert the outstanding amount in the personal cheque or counter cheque (as applicable) and present

the personal cheque or counter cheque (as applicable) to SCA's bank for payment to extinguish the outstanding cheque.

334. For the purposes of paragraphs 335 to 336, **CCF cheque** refers to a personal cheque or a counter cheque.

335. A customer could redeem a CCF cheque by:

a. cash or chip deposit into a customer's FMA at the SCA Cage;

b. domestic or international telegraphic transfer through an SCA Customer account or SCEG Customer account which was credited to the customer's FMA;

Particulars

The credit to the customer's FMA also involved an item 32, table 1, s 6 designated service.

See paragraphs 239 to 291.

c. domestic or international telegraphic transfer through an SCA Customer account or SCEG Customer account by a third party which was credited to the customer's FMA;

Particulars

The credit to the customer's FMA also involved an item 32, table 1, s 6 designated service.

See paragraphs 239 to 291.

d. providing a cheque issued by another casino;

e. requesting SCEG to transfer funds from the FMA held at a SCEG New Zealand casino to the customer's SCA FMA by way of inter-company transfer;

Particulars

The credit to the customer's FMA also involved an item 32, table 1, s 6 designated service.

See paragraphs 292 to 312.

f. a set-off of winnings by the customer; or

g. applying funds from the customer's FMA at the conclusion of gaming.

336. The banking or redemption of a CCF cheque (or the acceptance of a repayment under a CCF) was a transaction in relation to a loan where the loan was made in the course of carrying on a loans business.

Particulars

See particulars at paragraph 322.

337. SCA provided an item 7, table 1, s 6 designated service when it banked or redeemed a CCF Cheque (or accepted repayment under a CCF).

338. If a cheque under a CCF was dishonoured, SCA would recover payment from the customer in other ways.

339. The recovery of funds owed under a CCF by SCA if a CCF cheque was dishonoured involved a transaction in relation to a loan where the loan was made in the course of carrying on a loans business.

Particulars

See the particulars at paragraph 322.

340. SCA provided an item 7, table 1, s 6 designated service when it recovered funds owed under a CCF.

ML/TF risk assessments of CCFs

341. At no time did SCA carry out an ML/TF risk assessment of the items 6 and 7, table 1, s 6 designated services provided through CCFs.

342. The provision of items 6 and 7, table 1, s 6 designated services by SCA through CCFs involved higher ML/TF risks:

a. Loans under CCFs could be drawn down and repaid as part of a complex chain of different designated services under tables 1 and 3, s 6 of the Act.

b. CCFs enabled funds held by customers in foreign jurisdictions to be used in Australia without the need for a cross-border transfer.

c. CCFs created the opportunity for high volume and high frequency gambling by high risk customers playing through junket programs.

d. A single CCF approved for a junket operator could be drawn down for multiple programs.

e. Loans under CCFs could be drawn down by way of FMA deposit and then withdrawn in cash in the amount of 5% of the CCF to a maximum of $25,000 (unless approved by SCA management).

f. Loans under CCFs could be approved for monthly limits and could be drawn down on multiple occasions within the approved limit.

g. Junket operators and representatives were provided with significant lines of credit through CCFs. Following each drawdown of a CCF by the junket operator or junket representative, gaming chips or CPVs that were issued by SCA would be provided at the junket operator's or representative's discretion to the junket players.

Particulars

See *Customer 1*.

h. Credit could be shared across SCA and SCEG casinos.

i. Loans under CCFs could be repaid through non-face-to-face channels, including by international and domestic telegraphic transfers.

Particulars

On 22 January 2019, a foreign company connected to Suncity used the SCEG Customer Account channel to deposit HKD$4,876,545 into a SCEG customer account. A SCEG New Zealand casino then used the SkyCity New Zealand channel to transfer the funds from Customer 1's FMA held at the SCEG New Zealand casino to

Customer 1's SCA FMA. The funds were made available to Customer 1 in the amount of AUD$873,917, and were used to repay an outstanding line of credit for a Suncity junket.

j. Loans under CCFs could be repaid by domestic or international telegraphic transfer into an SCA Customer account or SCEG Customer account by a third party.

Particulars

See paragraphs 220 to 227 and 239 to 291.

k. The provision and repayments of loans via CCFs created an avenue for money laundering through smurfing, cuckoo smurfing or offsetting.

Particulars

See paragraph 24.

The Part A Programs did not apply appropriate controls to loans – CCFs

343. The Standard Part A Programs did not apply appropriate controls to items 6 and 7, table 1, s 6 designated services that were capable, by design, of identifying, mitigating and managing the ML/TF risks of these designated services.

a. The Standard Part A Programs did not include appropriate systems and controls to ensure that the approval of loans had regard to ML/TF risks.

b. The approval of credit limits under CCFs were subject to credit risk assessments, which did not have appropriate regard to ML/TF risks, and no ML/TF risk assessment was undertaken.

Particulars

The policies or procedures in place in relation to the provision of credit to customers did not provide for appropriate consideration of AML/CTF risk. For example, the credit risk matrices in effect did not have appropriate regard to ML/TF risks.

c. The Standard Part A Programs did not include appropriate risk-based controls to understand the ML/TF risks posed by a customer's source of wealth when approving a CCF for the customer.

Particulars

From 2019, SCA had processes in place for customers to provide some information in relation to their source of wealth and supporting documents. However, the review of this material was not supported by appropriate guidance with respect to AML/CTF risk, including the higher risks at paragraph 342.

d. The Standard Part A Programs did not include appropriate preventative controls to mitigate and manage the ML/TF risks of loans and repayments, such as controls to:

i. impose limits on credit;

ii. identify customers to whom the provision of credit was outside of ML/TF risk appetite;

iii. restrict the ability of third parties to repay loans on behalf of customers until September 2022 in relation to SCEG Customer accounts.

Particulars

See paragraphs 222.h, 225, 226, 519, 520 and 522.

e. The Standard Part A Programs did not include controls to monitor drawdowns under CCFs or to understand the relationship between junket operators and persons playing on programs being funded by the CCF

f. The Standard Part A Programs did not have any processes in place to identify how junket operators or representatives were distributing CVIs to junket players where a CCF was opened in the name of a junket operator.

Exchanging money for casino value instruments, including chips and tokens (and vice-versa)

344. From 7 December 2016 to about 17 November 2022, the Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by SCA with respect to items 7 and 8, table 3, s 6 designated services for the reasons pleaded at paragraphs 345 to 348 below.

345. Customers could use a number of different casino value instruments (**CVIs**) to obtain table 3, s 6 designated services from SCA, including those pleaded below:

a. Chips:

i. The exchange of money for chips was an item 7, table 3, s 6 designated service;

ii. The exchange of chips for money was an item 8, table 3, s 6 designated service;

iii. Chips could be used to enter into a game within the meaning of item 6, table 3, s 6;

iv. A customer could be paid chips as winnings for the purposes of item 9, table 3, s 6.

b. Chip purchase vouchers (**CPVs**):

i. This was a voucher that was issued in exchange for funds held in a customer's FMA, which involved an item 13, table 3, s 6 designated service;

ii. A CPV could be redeemed for gaming chips at a gaming table;

iii. A customer could deposit funds held in a CPV into a FMA, which involved an item 13, table 3, s 6 designated service;

iv. A CPV was a channel through which items 6 and 7, table 3, s 6 designated services could be obtained.

c. 'Ticket in ticket out' tickets (**TITO tickets**):

i. A TITO ticket was a barcoded ticket generated by:

A. the Cage in exchange for cash, chips or funds on a customer's FMA;

B. Cash Redemption Terminals (**CRTs**) in exchange for cash or funds on a customer's FMA; or

C. EGMs or ETGs at the completion of play by a customer upon pressing the 'collect button'.

ii. A TITO was a token.

iii. A customer received an item 7, table 3, s 6 designated service when a TITO ticket was issued in accordance with c(i)(A) and (B).

iv. A customer received an item 9, table 3, s 6 designated service when a TITO ticket was generated from an EGM or ETG.

v. A TITO ticket could be used to obtain an item 6, table 3, s 6 designated service on an ETG or EGM.

vi. The redemption of a TITO ticket was an item 8, table 3, s 6 designated service.

d. Hand-pay slips:

i. A hand-play slip was a handwritten slip that was generated by Gaming Attendants for customers who wished to redeem credits on an EGM or ETG at the completion of play.

ii. A hand-pay slip was used when the value of the credits exceeded the amount that could be paid out by a TITO ticket, or the EGM or ETG was not TITO ticket enabled.

iii. The issue of a hand-pay slip was an item 9, table 3, s 6 designated service.

iv. Hand-pay slips were only redeemable at the Cage.

v. The redemption of a hand-pay slip for money at the Cage was an item 8, table 3, s 6 designated service.

Particulars

SCA also referred to hand-pay slips as cancelled credit slips.

346. The use of CVIs to obtain table 3, s 6 designated services from SCA involved the following higher ML/TF risks:

a. Each of the above CVIs either directly involved the provision of table 3 designated services or were a channel through which table 3 designated services were provided.

b. During a visit to the casino, a customer could use CVIs to undertake multiple transactions, such as buying into and cashing out of table games or EGMs (items 6 and 9, table 3, s 6), or transacting on an FMA (item 13, table 3, s 6).

c. Each of the above CVIs were highly transferrable and could be issued in large values.

d. Customers could therefore transfer value from one person to another by passing on the CVIs.

e. CVIs could not always be traced to an account holder or identified customer.

f. The redemption of CVIs could not always be attributable to winnings and could be cashed out with minimal or no play.

g. The issue or redemption of tickets was not always face-to-face.

h. TITO tickets from ETGs and EGMs could be issued in high values.

i. From October 2020 the value of tickets that could be collected by a customer from an EGM or ETG without human intervention was $5,000 on the main gaming floor and $9,999 in premium gaming areas.

j. By reason of a. to h., CVIs could be used to layer funds, as part of a more complex transaction chain of designated services, making it difficult to understand the purpose of transactions, the beneficial owner of funds or the ultimate beneficiary of value moved.

Particulars

Chapter 2 FATF/APG Casino Typologies Report.

See paragraph 24.

347. At no time did SCA conduct an appropriate ML/TF risk assessment of the provision of the full range of table 3, s 6 gambling services through CVIs.

Particulars

Whilst the SCA conducted ML/TF risk assessments relating to a limited number of individual CVIs, at no time did SCA adequately identify and assess all of the risks pleaded at paragraph 346.

348. At no time did the Standard Part A Programs include appropriate risk-based systems and controls to identify, mitigate and manage the ML/TF risks of the provision of table 3 gambling services through CVIs:

a. At no time did the Standard Part A Programs include appropriate risk-based controls to mitigate and manage the ML/TF risks pleaded at paragraph 346.

b. With the exception of some limits on amounts printed on TITOs and transaction limits on cash redemption terminals, controls on CVIs were predominantly detective, not preventative.

Particulars

A TITO risk assessment dated October 2020 recorded that (**TITO Risk Assessment**):

the maximum ticket out without manual intervention on the main gaming room floor for EGMs is $5,000;

b. the maximum value ticket-out value without staff intervention is $5,000 for at ATG on the main gaming room floor;

c. the maximum ticket-out value without staff intervention is $9,999 for an ATG in Premium gaming areas;

d. the maximum value of a ticket that can be inserted into an EGM on the main gaming room floor is $149.99 per transaction;

e. the maximum value TITO ticket that a CRT on the main gaming floor would print was $2,500.

The TITO Risk Assessment also recorded that the maximum ticket out without staff intervention for EGMs in Premium gaming areas is

$2,000. However, the maximum ticket out in premium gaming areas without staff intervention was $9,999 for EGMs.

The 2015 Standard Part A Program stated that TITO tickets may be purchased and redeemed via eCash Kiosks subject to a maximum value of $2,000 (Appendix B, paragraph 93). The Standard Part A Programs did not identify any other limits with respect to TITOs.

c. Cage staff applying detective controls to item 8, table 3, s 6 designated services did not have adequate visibility over complex transaction chains involving CVIs.

Tables games and electronic gaming machines

349. From 7 December 2016 to about 17 November 2022, the Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by SCA with respect to items 6 and 9, table 3, s 6 designated services for the reasons pleaded at 350 to below.

350. SCA provided designated services under items 6 and 9, table 3, s 6 through:

a. table games; and

b. electronic gaming machines (**EGMs**), or pokie machines.

351. SCA offered a range of different table games.

a. Table games included roulette, baccarat, blackjack and poker.

b. Some table games were semi-automated or fully automated (referred to as electronic table games (**ETGs**), which included automated table games (**ATGs**)).

352. Different table games and EGMs have different ML/TF risk profiles depending upon matters including:

a. whether they are face-to-face or not;

b. whether they permit even-money betting;

c. the degree of uncertainty of outcomes;

d. how rapidly money can be processed;

e. ticket limits; and

f. whether they permitted peer-to-peer gaming.

353. Table games and EGMs offered by SCA involved the following ML/TF risks:

a. Money could be moved through table games and EGMs through buying-in and cashing-out using cash, TITO tickets, chips and other CVIs.

b. Chips, TITO tickets and other CVIs were highly transferable.

c. Customers could therefore transfer value from one person to another by passing on chips, TITO tickets and other CVIs.

d. Customers could transfer large amounts of money from their FMA to an EGM, as these transactions were not subject to daily limits.

i. From 7 December 2016 to August 2019, customers could transfer $250 per transaction, and from August 2019, $500 per transaction, from their FMA to an EGM on the main gaming floor by inserting their membership card.

ii. From 7 December 2016, in premium gaming areas, customers could transfer $9,999 per transaction from their FMA to an EGM by inserting their membership card.

iii. A customer could complete multiple transactions from their FMA to an EGM in one sitting, in the amount of the above limits.

e. Customers could transfer a high values of credit from EGM and ETGs directly to their FMA without human intervention by inserting their membership card.

i. From 7 December 2016 to 25 October 2021, customers could transfer $99,999 per transaction from an EGM to their FMA on the main gaming floor.

ii. From 7 December 2016, customers could transfer up to $99,999 from ETGs on the main gaming floor to their FMA.

iii. From 25 October 2021, customers could transfer $5,000 per transaction from an EGM to their FMA on the main gaming floor.

iv. From 7 December 2016, customers could transfer $99,999 per transaction from an EGM to their FMA in premium gaming areas.

v. There were no daily limits on transfers from an FMA to an EGM.

f. EGMs and ETGs were not face-to-face.

g. SCA decreased table game supervision in line with the introduction of risk technology, which was focused on fraudulent behaviour rather than ML/TF risk.

h. Supervision of table games and EGMs included reliance on Pit Cams, which were reviewed on an ad-hoc basis and when there were recorded customer complaints or disputes.

Particulars

SCA's AML risk assessment in relation to the introduction of the Pit Cams was not conducted in accordance with an appropriate ML/TF risk methodology.

See paragraphs 80 to 90.

i. Tickets from ETGs and EGMs could be issued in high values.

i. From 7 December 2016 the value of tickets that could be collected by a customer from an EGM or ETG without human intervention was:

A. $5,000 on the main gaming floor, and

B. $9,999 in premium gaming areas.

j. Money including cash could be inserted into ETGs and EGMs, and tickets could be collected with minimal or no play up to the threshold pleaded at paragraph 24.

k. There were no limits to buy-ins to EGMs or ETGs using cash or TITO tickets in premium gaming areas.

l. In table games that permit even-money wagering (such as roulette and baccarat), two customers could cover both sides of an even bet to give the appearance of legitimate gaming activity while minimising net losses.

m. Further, table games such as baccarat involve a low 'house edge'. Each hand can be high in value and is played within seconds. Money can therefore be turned-over very quickly, with minimal net loss and in collusion with other players.

n. The risks of even-money wagering are higher with ATGs.

Particulars

SCA's AML risk assessment of ETGs assessed that even betting was a likely inherent risk of gaming with this technology.

o. EGMs and ETGs were vulnerable to refining because they process large volumes of smaller amounts quickly.

p. EGMs and ETGs were vulnerable to structuring and structured funds could be redeemed at non-face-to-face CRTs in the following amounts:

i. From 7 December 2016, $2,000 per transaction and from August 2019, $2,500 per transaction;

ii. From 7 December 2016 to February 2018, $9,999 per transaction for the CRTs in the SCA Black Room.

Particulars

See particulars at paragraph 348.

q. Poker permitted peer-to-peer gaming, which posed risks of collusion.

r. Poker, particularly poker tournaments, could be used as a vehicle to legitimate the transfer of large amounts of funds between players.

s. By reason of a. to r., play on table games and EGMs could be used to layer funds, as part of a more complex transaction chain of designated services, making it difficult to understand the purpose of transactions, the beneficial owner of funds or the ultimate beneficiary of the value moved.

Particulars

See paragraph 24.

354. At no time did SCA identify and assess the different ML/TF risks of different tables games and EGMs in accordance with an appropriate ML/TF risk methodology.

Particulars

See paragraphs 97 to 113.

355. At no time did the Standard Part A Programs include appropriate systems and controls to identify, mitigate and manage the ML/TF risks of designated services provided under items 6 and 9, table 3, s 6 through each of the different table games and EGMs:

a. The Standard Part A Programs did not have appropriate regard to the different ML/TF risk profiles of different table games and EGMs when determining and putting in place risk-based systems and controls for items 6 and 9, table 3, s 6 designated services.

b. The Standard Part A Programs did not include appropriate preventative controls, such as appropriate transaction or daily limits, with respect to buy-ins and cash-outs.

c. The Standard Part A Programs did not include appropriate risk-based procedures to understand source of wealth or funds with respect to items 6 and 9, table 3, s 6 designated services (especially with respect to uncarded play as defined in paragraph 466).

d. The data recorded in Bally CMP for manual table games consisted of estimates and averages and was not accurate, and was only recorded against a customer where the customer presented their loyalty card.

Particulars

See paragraphs 431 to 495.

e. Detective controls were otherwise largely reliant on staff observation and surveillance, including Pit Cams, which were inadequate for the following reasons:

i. the ML/TF risks of EGMs and ETGs could not be adequately monitored by manual and observation methods;

ii. the Pit Cam system was reviewed on an ad hoc basis and the reviews that were conducted were focused on recorded customer complaints or disputes;

iii. manual and observational controls were not capable of consistently detecting the use of table games and EGMs to layer funds, as part of a more complex transaction chain of designated services; and

iv. the Part A detective controls did not allow the Cage visibility over any unusual patterns of activity on table games and EGMs at the point in time when the Cage exchanged chips, TITO tickets or other CVIs for money.

EzyPlay Guest Cards

356. At all times from 7 December 2016, SCA provided customers with table 3, s 6 designated services through EZYPlay Guest Cards.

Particulars

EZYPlay Guest Cards were a channel through which SCA provided items 6, 7, 8 and 9 table 3, s 6 designated services.

357. EZYPlay Guest Cards were used by SCA customers to undertake cashless gaming at SCA.

Particulars

In 2018, SCA issued 17,017 EZYPlay Guest Cards, of which 13,156 were used.

358. SCA did not issue EZYPlay Guest Cards in the name of a customer.

359. SCA did not take any steps to identify or verify the identity of a customer when they were issued an EZYPlay Guest Card.

360. At all times, funds could be added to or withdrawn from an EZYPlay Guest card in the following ways:

a. a customer could deposit funds (including cash) onto an EZYPlay Guest Card at a CRT or the SCA Cage;

b. a customer could download credits from an EGM or EGT to an EZYPlay Guest Card (table 3, item 9 designated service);

c. a customer could download funds from an EZYPlay Guest Card to an EGM (table 3, item 6 designated service); and

d. a customer could withdraw funds (in the form of cash or a TITO) from an EZYPlay Guest Card at a CRT or at the Cage (table 3, item 8 designated services).

361. The provision of designated services via EZYPlay Guest Cards was subject to higher ML/TF risks for the following reasons:

a. As EZYPlay Guest Cards were not issued in the name of a customer, the card was highly transferable and facilitated transactions where the source of funds could not be known.

b. EZYPlay Guest Cards could be used to conduct non-face-to-face transactions;

Particulars

At all times, a customer could deposit funds onto an EZYPlay Guest Card at a CRT, EGM or ETG (including cash).

At all times, a customer could download credits from an EGM to an EZYPlay Guest Card (table 3, item 9 designated service).

At all times, a customer could download funds on an EZYPlay Guest Card to an EGM (table 3, item 6 designated service).

At all times, a customer could withdraw funds (in the form of cash or a TITO) from an EZYPlay Guest Card at a CRT (table 3, item 8 designated services).

c. There were no daily limits on total transfers from an EGM or ETG to an EZYPlay Guest Card.

d. Cash could be deposited and withdrawn using EZYPlay Guest Cards through the Cage and CRTs.

Particulars to subparagraphs c. to d.

Prior to August 2019, there was an ongoing card balance limit of $1,000. This did not apply to customers in premium gaming areas.

From August 2019, there was an ongoing card balance limit of $5,000. This did not apply to premium gaming areas. However, from August 2019, cash deposits to and withdrawals from the EZYPlay Guest Card, which exceeded $2,500 could not be made in a single transaction.

362. The Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by SCA with respect to designated services provided through EZYPlay Guest Cards, for the reasons identified at paragraphs 363 to 367 below.

363. SCA did not conduct an assessment of the ML/TF risks of providing table 3, s 6 designated services through EZYPlay Guest Cards.

Particulars

At no time were EZYPlay Guest Cards subject to their own risk assessment.

EZYPlay Guest Cards were also known as Green Cards. Green Cards are mentioned in the 2022 Risk Assessments. However, SCA's Standard Part A Program was not aligned to the 2022 Risk Assessments: see paragraph 112.

364. At no time did SCA have appropriate processes or controls in place to understand who was being provided with designated services through EZYPlay Guest Cards:

a. Customers could obtain EZYPlay Guest Cards without identification, and were not subject to KYC processes unless they transacted above prescribed thresholds.

Particulars

Customers using EZYPlay Guest Cards for cash transactions over $10,000 were required to provide KYC Information.

b. SCA did not have any controls in place to prevent customers sharing EZYPlay Guest Cards, or giving their EZYPlay Guest Card to another patron.

c. SCA did not have any processes or controls to ensure that the person the EZYPlay Guest Card was issued to was the same person receiving designated services through the use of that EZYPlay Guest Card.

d. SCA provided designated services to customers through EZYPlay Guest Card other than face-to-face.

365. From 7 December 2016 to August 2019, in premium gaming areas or for premium customers, SCA did not impose:

a. any limits on the value of funds that could be stored on an EZYPlay Guest Card;

b. any daily limits on the funds that could be deposited into an EZYPlay Guest Card; and

c. any daily limits on the funds that could be withdrawn from an EZYPlay Guest Card.

Particulars

See the particulars to paragraph 218.b.

366. At no time did SCA's transaction monitoring program include appropriate risk-based systems and controls to monitor the transactions of customers receiving designated services through the use of EZYPlay Guest Cards.

Particulars

See paragraphs 488 and 489.

367. At no time did SCA impose appropriate processes or controls to limit the number of EZYPlay Guest Cards that could be obtained by a customer.

Particulars

As EZYPlay Guest Cards were issued without identification and did not require a customer to provide identification, SCA was unable to consistently ascertain or control whether a customer had obtained multiple EZYPlay Guest Cards.

For example, on 8 June 2018, SCA staff observed an anonymous customer using four separate EZYPlay Guest Cards, in transactions indicative of refining: SMR dated 12 June 2018. See particulars to paragraph 489.c.

Foreign currency exchange – item 14, table 3, s 6 designated services

368. From 7 December 2016 to on or around 17 November 2022, the Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by SCA with respect to item 14, table 3, s 6 designated services for the reasons pleaded at paragraphs 369 to 375 below.

369. At all times, SCA provided foreign currency exchange services to customers within the meaning of item 14, table 3, s 6 of the Act.

370. The SCA Cage accepted physical currency, foreign drafts and travellers' cheques for the purposes of currency exchange.

Particulars

From July 2022, SCA no longer accepted travellers' cheques.

During the period 7 December 2016 to on or about 17 November 2022, SCA accepted foreign drafts as the personal cheque provided in relation to a CCF: see paragraph 327.

371. Customers could also deposit funds into the SCEG Customer accounts held in foreign currencies. The International Business Patron accounts team would convert the funds to Australian dollars and SCA would then make them available to the customer in their FMA.

372. Currency exchange was also facilitated for customers who were repaying CCFs, including when SCA accepted repayment through the SCEG Customer accounts or by foreign draft.

Particulars

See paragraph 327.

373. At no time did SCA carry out ML/TF risk assessments with respect to designated services provided through the SCEG Customer accounts held in foreign currencies, including currency exchange services.

Particulars

See paragraphs 103.b and 145.c.

374. At no time did SCA carry out ML/TF risk assessments with respect to foreign drafts.

Particulars

The May 2022 SkyCity Cage risk assessment acknowledged the acceptance of cheques but did not acknowledge or assess the risks specifically associated with foreign drafts.

The October 2021 and November 2022 Standard Part A Programs were not aligned to the May 2022 SkyCity Cage risk assessment: see paragraph 112.

375. The Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by SCA with respect to item 14, table 3, s 6 designated services.

a. The FATF/APG Casino Typologies Report, Chapter 2, identifies indicators of money laundering using currency exchange, including:

i. multiple currency exchanges;

ii. dramatic or rapid increases in size and frequency of currency exchange transactions for regulator account holders;

iii. currency exchange for no reasonable purpose;

iv. currency exchanges with low denomination bills for high denomination bills;

v. currency exchanges carried out by third parties;

vi. large, one-off, or frequent currency exchanges for customers not known to the casino;

vii. currency exchanges with little or no gambling activity; and

viii. structured currency exchanges.

b. The Standard Part A Programs did not include appropriate controls for monitoring transactions indicative of the above typologies.

Particulars

The Standard Part A Programs provided for system-generated reports and transaction monitoring rules for certain scenarios related to foreign currency. However, they were not supported by appropriate criteria to review those transactions against all the typologies at paragraph a.

c. The Standard Part A Programs did not include controls for monitoring transactions that did not involve the physical exchange of currency, such as transactions on FMAs involving currency exchange, or the repayment of CCFs in foreign currency.

Designated services provided in cash

376. From 7 December 2016 to about 17 November 2022, the Standard Part A Programs did not include appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by SCA with respect to designated services involving cash for the reasons pleaded at paragraphs 377 to 381 below.

377. SCA is a cash intensive business that is vulnerable to the ML/TF risks and typologies pleaded at paragraphs 17 and 24.

378. Controls on large cash deposits and payouts at the SCA Cage were not adequate from 7 December 2016 to about 17 November 2022:

a. Prior to 23 December 2019, there was no requirement for a customer to provide source of funds information in order to make a large cash deposit at the Cage.

b. It was not until 23 December 2019 that SCA required a source of funds declaration form to be completed by international business customers presenting $100,000 or more in cash. There was no requirement for customers to provide supporting information with this form.

c. On 17 December 2020, SCA introduced updated requirements for a source of funds declaration form and supporting documentation to be provided by:

    i. International Business customers presenting $250,000 or more in cash; and

    ii. domestic customers presenting $150,000 or more in cash.

d. On 19 July 2021, SCA introduced further updated requirements for collecting source of funds information for large cash deposits:

    i. any customer presenting between $50,000 to $100,000 in cash had to complete a source of funds declaration form; and

    ii. any customer presenting $100,000 or more in cash had to complete a source of funds declaration form and provide supporting documentation.

e. If, in the circumstances identified at subparagraphs b. to d., a customer refused to complete a source of funds declaration form or provide supporting documentation (as applicable), SCA would not proceed with the transaction.

f. However, at no time was there appropriate written review criteria against which the SCA staff member reviewing the source of funds declaration form and supporting documentation was to determine whether to proceed with the transaction or whether to refer the customer to senior management to determine whether the transaction should be approved, having regard to ML/TF risk.

Particulars

See paragraphs 516 and 517.

g. There were no daily or transaction limits relating to cash deposits and payouts at the Cage.

h. The Standard Part A Programs did not include appropriate risk-based procedures requiring the ML/TF risks of large cash transactions to be considered and approved before the transactions could be processed.

i. The Standard Part A Programs did not include appropriate risk-based procedures for SCA to determine whether it would accept cash that was presented in an unusual or suspicious condition or in unusual or suspicious packaging.

Particulars

On 4 October 2018, the SCA Cage permitted Customer 39 to conduct a buy-in of $9,000 in $50 notes that were in poor condition and were covered in dirt as if they had been buried: SMR dated 9 October 2018.

On 18 January 2021, an associate of Customer 30 presented notes at the SCA Cage that were soiled and sticky, with a strong aroma of dirt.

The SCA Cage exchanged those dirty notes for cash chips: SMR dated 21 January 2021.

On 20 March 2021, the SCA Cage processed a cash buy-in transaction of $35,000 for Customer 29. The cash presented by Customer 29 had a strong aroma of dirt: SMR dated 7 April 2021.

379. At all times:

a. no limits were imposed with respect to cash deposits or withdrawals on FMAs.

Particulars

See paragraph 216.d.

b. there were no documented controls or procedures to identify or limit cash deposits into SCA Customer accounts.

Particulars

See paragraphs 221, 222.d and 224.

c. prior to late 2021, there were no controls or procedures to identify or limit cash deposits into SCEG Customer accounts.

Particulars

See paragraphs 221, 222.c and 223.

d. there were no documented processes detailing how a cash deposit received into an SCA or SCEG Customer account was to be returned to the depositor, in circumstances where that deposit was not permitted by SCA or SCEG.

Particulars

See paragraph 225.

380. At all times, controls on cash in private gaming rooms were inadequate:

a. There were no limits on the amount of cash that could be taken into a private gaming room.

b. There were no limits or caps on cash transactions conducted in private gaming rooms.

c. There were no appropriate controls on who could bring cash into private gaming rooms.

d. Controls with respect to cash transactions that could be conducted in private gaming rooms by junket operators, junket representatives or junket players were inadequate.

Particulars

For example, on 15 July 2018, Customer 2 withdrew $50,000 in cash and a $10,000 CPV from their FMA. A VIP Host collected the cash on Customer 2's behalf, placed it in a large envelope and delivered it to Customer 2 at a gaming table. Customer 2 then hid the envelope under the table and passed it to Person 5, who was sitting next to them. Shortly after, Person 5 took the envelope to the Grange Cage and deposited the $50,000 in cash into their account.

See *Customer 2's risk profile*, below.

e. SCA was aware of unusual activity involving large amounts of cash in private gaming rooms.

Particulars

Between October 2020 and March 2021, SCA identified several incidents involving Customer 29 covertly exchanging cash with other customers in private gaming rooms. See also Customer 37 and Customer 30.

Between June 2018 and May 2019, Customer 2, Customer 31 and Person 7 (Customer 31's spouse) exchanged approximately $700,000 in cash in private gaming rooms, including by passing cash in plastic bags and hiding cash in the toilets and under gambling tables.

On 30 June 2017, Customer 21 deposited $180,000 in cash into their SCA FMA. SCA issued two CPVs of $90,000 each to Customer 21. Customer 21 then attended two different gaming tables in the Grange Room and exchanged one CPV for cash at each table. Customer 21 then covertly passed the $180,000 in cash to Customer 27.

See *Customer 21's risk profile*, below.

On 12 July 2018, Person 5 lost approximately $675,000 playing baccarat. To continue playing, Person 5 produced two plastic bags of cash totalling $101,300 to the Grange Cashier. Customer 27 had given Person 5 the cash. Later that evening, Customer 28 passed a further $20,000 to Person 5 under the table at which Person 5 was playing: SMR dated 13 July 2018.

See *Customer 27's risk profile and Customer 28's risk profile*, below.

381. At all times, the controls on cash transactions under $10,000 for uncarded players were not adequate or appropriate.

Particulars

SCA relied on staff observation to identify potential structuring at table games by uncarded players: see particulars to paragraph 469.

SCA did not consistently keep records of cash transactions below $10,000 at table games: see paragraph 462.

Designated services provided through junket channels

What is a junket?

382. A junket is an arrangement between a casino and a **junket operator** to facilitate a period of gambling (**junket programs**) by one or more high wealth players (**junket players**) at the casino.

Particulars

SCA sometimes referred to junket operators as Group Commission Operators and junket players as Group Commission Players.

383. Junket operators were at times represented by **junket representatives**.

Particulars

SCA sometimes referred to junket representatives as Group Commission Representatives. Junket operators were not necessarily present during a junket program.

384. From 7 December 2016 to 12 April 2021, prior to the commencement of a junket program, SCA and the junket operator entered into a Group Commission Program Agreement (**GCPA**).

Particulars

SCA sometimes referred to these agreements as Revenue Share Programs.

385. The GCPA set out the terms and conditions of each junket program, including the benefits payable under the program.

386. In return for bringing junket players to the casino, SCA paid junket operators rebates or commissions.

a. GCPAs set out the rebates or commissions available to the junket operator under each junket program.

b. Rebates were calculated based on the junket's gross win/loss recorded by SCA at the time of settlement by SCA.

c. Junkets would agree to bear a percentage of the gross win by SCA (or loss by SCA) of each junket program play by receiving from SCA (or paying SCA) a rebate.

d. A rebate effectively operated as a 'hedge' to reduce the variability of wins/losses by the junket and SCA.

e. Commissions were calculated based on the total turnover of the junket program.

f. A commission would be payable by SCA and calculated in accordance with a pre-determined commission rate multiplied by the total turnover recorded at the time of settlement.

g. The calculations for commissions or rebates would be recorded at the end of the junket program on a junket settlement sheet.

h. Where the front money was drawn down from a CCF or line of credit, the rebate or commission payable to the junket operator was first applied to the relevant facility. This was also recorded on the junket settlement sheet.

SCA's junket business

387. From 7 December 2016 to 12 April 2021, SCA entered into GCPAs with junket operators.

a. Prior to and from 7 December 2016, SCA sought to attract business from international VIP customers to Australia.

b. On and from 7 December 2016 to 12 April 2021, SCA facilitated junkets operated by many different junket operators and governed by GCPAs.

c. Some junket operators were represented by multiple junket representatives.

d. Some junket operators ran multiple junkets at the same time.

e. Some junket programs had only one junket player.

f. On 12 April 2021, the SCEG Board decided permanently to cease dealing with junket operators. SCEG and SCA ceased doing business with all junkets at that time.

Designated services provided through junket channels

388. SCA provided items 6, 7, 31 and 32, table 1, s 6 designated services to customers through junket channels in Australian dollars.

Particulars

Customers who received designated services through junket channels included junket operators, junket representatives and junket players.

See *Loans – items 6 and 7, table 1, s 6 designated services* and *Remittance services – items 31 and 32, table 1, s 6 designated services* above.

389. SCA provided table 3 designated services to customers through junket channels in both Australian dollars and HKD.

Particulars

Customers who received designated services through junket channels included junket operators, junket representatives and junket players.

Junket revenue

390. From 1 January 2017 to December 2020, SCA generated revenue from junket programs, including from designated services provided through junket channels.

Particulars

Between 1 January 2017 and December 2020, SCA made over $23,000,000 in junket revenue.

391. From 7 December 2016 to 12 April 2021, SCA recorded significant turnover associated with table 3, s 6 designated services provided through junket channels.

Particulars

For example:

a. between FY17 and FY18, Customer 3's junket recorded turnover exceeding $432,000,000; and

b. between FY18 and FY20, the Suncity junket recorded turnover exceeding $120,000,000.

The ML/TF risks of junkets

392. The provision of designated services by SCA through junket channels involved higher ML/TF risks pleaded as follows:

a. Junket operators and representatives facilitated the provision by SCA of both gambling and financial services to junket players, often in high values.

b. Junket programs involved the movement of large amounts of money across borders.

Particulars

For example, on 11 June 2019, SCA transferred $2,091,482 from its account to a SCEG New Zealand casino's account on behalf of Customer 8. The SCEG New Zealand casino then transferred the funds to Customer 8's bank account overseas.

See Customer 8's risk profile.

c. Junket programs often used multiple bank accounts, including accounts held by third parties and companies, which could obscure the identities of the persons conducting the transactions through junket programs and the source and ownership of funds of customers receiving designated services through junket channels.

Particulars

For example, on 22 January 2019 a foreign company connected to Suncity used the SCEG Customer account channel to deposit HKD$4,876,545 into a SCEG customer account. A SCEG New Zealand casino then used the SkyCity New Zealand channel to transfer the funds from Customer 1's FMA held at the SCEG New Zealand casino to Customer 1's SCA FMA. The funds were made available to Customer 1 in the amount of AUD$873,917, and were used to repay an outstanding line of credit for the Suncity junket.

See *Customer 1's risk profile.*

d. Junket players generally relied on the junket operators to make their funds available at the casinos, including through CCFs.

e. Junket operators provided cash to junket players, in circumstances where SCA was unaware of the source of funds and the purpose for which the cash was used.

f. There was a level of anonymity and lack of transparency created by the pooling of all players' funds and transactions under the name of the junket operator.

g. The financial arrangements between the junket operators and junket players were not disclosed to SCA.

h. SCA offered significant amounts of credit in the form of CCFs and lines of credit to junket operators on request.

i. SCA recorded gambling activity on junket programs for the limited purpose of calculating rebates or commissions payable to junket operators.

Particulars

See paragraphs 399 to 405.

j. On a per-transaction and per-customer basis, the junket tour operations sector is exposed to the risks associated with high-value cash activity.

k. Junket operators used formal or informal systems to remit money.

l. Junkets used the SCEG Customer account channel and the SkyCity New Zealand channel to repay lines of credit or CCFs.

Particulars

See paragraphs 239 to 262 and paragraphs 292 to 306.

m. Junkets programs are vulnerable to cuckoo smurfing and structuring.

n. Money deposited into a junket operator's account at casinos and then withdrawn with minimal gambling activity can give the funds the appearance of legitimacy.

o. Offsetting arrangements (as explained in paragraph 24f) used by junket operators to facilitate the provision of funds for junkets:

   i. creates risk of exploitation by criminal entities;

   ii. can circumvent international funds transfer reporting requirements; and

   iii. can facilitate the laundering of domestically-generated proceeds of crime.

p. Gambling accounts used by junkets at casinos are highly vulnerable to the storage and movement of potentially illicit funds. The parking of illicit money in such accounts puts distance between the act or acts that generated the illicit funds and the ultimate recipients of those funds, making it harder to trace the flow of money.

q. Exposure to some higher ML/TF risk jurisdictions is inherent in the junket operations sector.

   i. There is a particular vulnerability associated with jurisdictions with currency flight and gambling restrictions in place as these measures create demand for covert money remittances which can be exploited by criminal groups.

   ii. Having a customer base composed of predominantly foreign residents can increase the junket sector's attractiveness and exposure to transnational serious and organised crime, simply due to its geographical reach.

   iii. Such a customer base can mean that the source and destination of funds, and information about customers' criminal and financial activity, are difficult to identify as they are located in foreign jurisdictions.

   iv. Some junket operators and junket players at SCA were foreign PEPs.

Particulars

For example:

a. junket operators such as Customer 1 were foreign PEPs; and

b. junket players such as Customer 11 were foreign PEPs.

Customer 11 was an immediate family member of a person holding a prominent public position in a foreign government body. Customer 11 played on junket programs operated by Customer 3 and Customer 9.

See *Customer 11's risk profile.*

   v. SCA provided designated services to customers through junket channels in both Australian dollars and foreign currencies.

   vi. As the volume of gambling transactions during junkets is very high, there is also a higher risk that junkets will be exploited for money laundering.

Particulars

FATF/APG Casino Typologies Report.

AUSTRAC Junket Assessment.

FATF RBA Guidance.

ML/TF risk assessments and controls

393. SCA did not carry out an appropriate risk assessment of the higher ML/TF risks of providing designated services through the junket channel in the period from 7 December 2016 to 12 April 2021.

Particulars

See paragraphs 92 to 110.

394. Consequently, from 7 December 2016 to 12 April 2021, the Standard Part A Programs did not include appropriate risk-based controls to identify, mitigate and manage the ML/TF risks of designated services provided through the junket channel for the reasons pleaded at paragraph 117.

395. Despite the known higher ML/TF risks as pleaded at paragraph 392, the controls in the Standard Part A Programs that applied to the provision of designated services through junket channels were generally no different to the controls that applied to other customers.

Customer risk

396. At no time prior to 12 April 2021 did the Standard Part A Programs include appropriate systems and controls to identify, mitigate and manage the ML/TF risks of customers receiving designated services through junket channels:

a. The customers receiving designated services through junket channels included junket operators, junket representatives and junket players.

b. The ML/TF risks posed by customers receiving designated services through junket channels include those pleaded at paragraph 392 above.

c. It was not until February 2021, that SCA classified junket operators as high risk for the purpose of the Act and Rules.

Particulars

Prior to February 2021, SCA assigned a default risk rating of 'moderate' to junket operators.

In the 2015 Standard Part A Program, junket operators visiting SCA on more than three occasions in a year were rated as 'high' risk.

d. Between 7 February 2017 and 15 February 2019, there was no default risk rating for junket representatives and junket players. At all other times, junket representatives and junket players were assigned a default risk rating of 'moderate'.

Particulars

Section 13 of the 2015 Standard Part A Program.

Section 3, paragraph 32 of the 2017-2019 Standard Part A Programs.

In the 2015 Standard Part A Program, junket players visiting the SCA casino on more than three occasions in a year were rated as 'high' risk.

Section 3 and Schedule 1 of the February 2021 Standard Part A Program.

e. At no time did SCA have adequate escalation procedures to determine whether the customers receiving designated services through junket programs should have been rated higher risk, having regard to the customer's specific ML/TF risks, including for the reasons pleaded at paragraph 392.

f. At no time did SCA adequately assess the jurisdictional risks associated with customers receiving designated services provided through the junket channel (see paragraph 392).

g. The Standard Part A Programs did not include appropriate risk-based controls to obtain and analyse source of wealth and source of funds information with respect to junket operators, representatives and players.

Particulars

See paragraph 138.

It was not until 16 February 2021 that the Standard Part A Programs included a requirement for junket operators to complete a source of wealth declaration form, with supporting documentation, as part of a junket operator's application for approval to SCEG: section 14, paragraph 14 of the February 2021 Standard Part A Program.

As pleaded at paragraph 397 below, the approvals provided to junket operators by SCEG New Zealand, were not supported or supplemented by SCA processes for due diligence, having regard to SCA's ML/TF risk appetite, including with respect to reviewing, updating or verifying source of wealth information provided by junket operators.

h. The Standard Part A Programs did not include appropriate risk-based controls to collect and verify appropriate KYC information with respect to junket operators and other customers receiving designated services through junket channels, such as the beneficial ownership of funds or the beneficiaries of transactions being facilitated by SCA on behalf of junkets operators, including the destination of funds.

Particulars

Rules 8.1.5, 15.2 and 15.3 and paragraphs (l) and (m) of the definition of *KYC information* in r 1.2.1 of the Rules.

i. SCA provided designated services to junket players in circumstances where it did not have a direct relationship with the customer, but relied upon the junket operator as an intermediary or agent. As a consequence, SCA did not always know who it was providing designated services to through junket channels.

Particulars

Junket operators and junket representatives pooled front money for use by, and winnings for distribution to, junket players. This limited the transparency of the source of funds used by junket players on

junket programs and obscured the beneficiaries of remittances arising from winnings on junket programs.

SCA provided table 3, s 6 designated services to junket players. SCA did not appropriately collect, verify, review, update and analyse KYC information for junket players, in circumstances where they had limited insight into the source and destination of funds.

Rules 1.2.1, 15.2, 15.10(1), (2) and (3) of the Rules.

j. At no time did SCA appropriately identify, mitigate and manage the ML/TF risks of providing designated services to junket players through junket operators and representatives as agents.

Particulars

SCA permitted junket operators to pay out winnings to junket players, without first assessing the ML/TF risks associated of such transactions.

SCA permitted junket operators to exchange cash for chips or vice versa for junket players, without first assessing the ML/TF risks of such transactions.

Junket due diligence

397. At no time did the due diligence conducted with respect to junket operators appropriately identify, mitigate and manage ML/TF risks with respect to designated services provided through the junket channel:

Particulars

All junket customers

At all times, junket operators, junket representatives and junket players were required to provide the same KYC information as other SCA customers: paragraph 553.

It was only in the February 2021 Standard Part A Program that junket operators were required to complete a source of wealth declaration form, with supporting documentation, as part of the junket operator's application for approval to SCEG: section 14, paragraph 14 of the February 2021 Standard Part A Program. This was added to the Standard Part A Program two months before SCA ceased operating junket programs on 12 April 2021.

At all times, the KYC information was screened against a global database to determine whether the junket operators, representatives and players were PEPs.

Sections 20-23 of the 2015 Standard Part B Program.

Section 19 of the 2017-2021 Standard Part B Programs.

Junket operators

Prior to 1 August 2019, aside from collecting ACIP information and conducting PEP screening, SCA did not conduct any due diligence in

relation to junket operators. SCA assigned junket operators a default risk rating of 'moderate' during this period. SCA did not have a reasonable basis for concluding that the ML/TF risks posed by junket operators were 'moderate'.

From 1 August 2019, there was no framework in place in the Standard Part A Programs to determine whether decisions with respect to the approval of junket operators were within SCA's ML/TF risk appetite. Rather, SCA required all junket operators to confirm that they had been approved by SCEG to conduct junket programs:

a. the SCEG approval process for junket operators required junket operators to complete an application form, which included identification documents, a police clearance (or a statutory declaration that such a certificate was not obtainable from the applicant's jurisdiction) and answers to questions about the applicant's personal history;

b. as part of the application process, SCEG would conduct a PEP search, iTrak search and open source Google search on the junket operator; and

c. successful applicants were required to apply for renewal every two years.

SCA relied on SCEG to conduct due diligence on prospective junket operators and consider whether they were suitable to conduct business with, which did not have regard to SCA's ML/TF risk appetite. Aside from collecting ACIP information and conducting PEP screens, SCA conducted no independent due diligence on prospective junket operators.

The approvals provided to junket operators by SCEG:

a. did not identify, mitigate and manage the risks with respect to the designated services that SCA provided through the junket channel, including items 31, 32, 6 and 7, table 1, s 6 designated services;

b. were not supported or supplemented by SCA processes for due diligence with respect to junket operators to appropriately identify, mitigate and manage the ML/TF risks with respect to designated services provided through the junket channel; and

c. There were no appropriate systems and controls for due diligence on junket operators to be guided by appropriate criteria relevant for ML/TF risks.

Complex transaction chains

398. SCA provided a range of table 1 and table 3, s 6 designated services to customers through junket channels, involving complex transaction chains, but at no time identified, mitigated or managed the associated ML/TF risks.

Particulars

Rule 8.1.3 of the Rules.

On multiple occasions following the settlement of junket programs, the junket settlement funds were paid out by:

a. a SCEG New Zealand casino transferring the settlement funds to the junket operator's personal bank account overseas on behalf of SCA using the SCEG Customer account channel; and

b. SCA then transferring the equivalent amount of funds to the SCEG casino to settle their debt.

See *Customer 1's risk profile* and *Customer 8's risk profile*.

On each occasion:

c. the funds were remitted out of SCA following play on a junket program, in circumstances where the source of funds was not clear;

d. the funds were remitted across international borders using one of the SCEG Customer accounts, obfuscating that the funds originated in Australia; and

e. the junket operators could then disburse the funds to third parties, including junket players, with no oversight from SCA.

Records of play on junket programs

399. The Standard Part A Programs did not require SCA to make and keep records of the designated services provided to individual junket players under a junket program.

400. At all times, the gambling activity of junket players was recorded by SCA collectively under the junket program, and not on an individual player basis.

Particulars

SCA did not record the gambling activity of individual junket players. Instead, SCA recorded the turnover and win/loss of the junket program collectively against the junket operator's FMA, for the purposes of paying commissions or rebates to the junket operator. This information was recorded in Bally.

401. At no time did SCA monitor the gambling activity of individual junket players.

Particulars

SCA did not monitor the transactions of individual junket players. Instead, SCA applied transaction monitoring processes to the junket program participants as a whole, by monitoring transactions recorded against the junket operator.

Because accurate records were not kept of the designated services provided to junket players, SCA did not have a complete picture of the customer's gambling activity which formed a part of their ML/TF risk profile.

402. Failure to monitor the gambling activity of each junket player individually meant that SCA had no visibility over how gaming chips were distributed amongst junket players. SCA could not appropriately monitor transactions through the junket channel, including whether a junket

player's level of gambling activity was commensurate with transactions conducted at the Cage.

Particulars

For example, Customer 13 attended SCA as a junket player on seven Suncity junkets between 16 December 2016 and 1 July 2019. Each of these junkets were funded by Customer 1. Three of these junkets were also operated by Customer 1. SCA recorded that the total cumulative turnover for these junkets exceeded $16,000,000. SCA kept no records of Customer 13's gambling activity or their individual turnover on these junkets.

See *Customer 13's risk profile*.

403. At all times, at the conclusion of junket programs, SCA paid winnings to a junket operator or representative by way of:

a. cash;

b. cheque;

c. transfer of funds to the junket operator's FMA (including to an account held at another SCEG casino); and/or

d. bank transfer.

404. At all times, the junket operator or representative paid winnings to the players of that junket program pursuant to agreements between them, to which SCA was not privy.

405. In the absence of appropriate records of the designated services SCA provided through junket program channels, SCA was unable to adopt and maintain appropriate risk-based AML/CTF controls.

Particulars

SCA recorded the provision of table 3, s 6 designated services to junket operators, junket representatives and junket players through junket programs for the primary purpose of calculating the commission or rebate payable to the junket operator for and on behalf of the junket players.

SCA did not collect and record the provision of table 3, s 6 designated services to junket operators, junket representatives and junket players through junket programs in order to adopt and maintain appropriate risk-based AML/CTF controls.

CCFs or lines of credit

406. At no time did the Standard Part A Programs appropriately identify, mitigate and manage the ML/TF risks of providing lines of credit or CCFs to junket operators or representatives (items 6 and 7, table 1, s 6):

a. When a customer applied for credit, SCA conducted a risk assessment which was largely focussed on credit risk and not ML/TF risk.

b. There was no framework in place in the Standard Part A Programs for SCA to determine whether decisions with respect to providing CCFs or lines of credit, including credit limit, for junket operators were within SCA's ML/TF risk appetite.

Particulars

See paragraphs 341343 and 418.

c. From 7 December 2016 until 12 April 2021, SCA provided junkets with CCFs or lines of credit.

Particulars

Between 2017 and 2020, the total value of CCFs approved for junket operators exceeded $1.2 billion.

d. SCA also provided ongoing CCFs with monthly limits for junket operators, which could be drawn down at multiple SCEG venues, including SCA.

e. A CCF or line of credit was opened in the name of the junket operator.

f. From 14 February 2017, CCFs or lines of credit could be operated by third parties.

Particulars

A junket operator could delegate authority to operate the facility to a junket representative, either up to the full amount of the facility or some lesser specified amount.

g. SCA permitted funds drawn on a CCF or line of credit to be accessed in cash.

h. Following the drawdown of a line of credit, a junket operator could transfer the credit to the FMA of a junket representative or junket player where written authorisation via a Funds Authorisation Form was in place.

i. SCA did not provide junket players with direct access to the approved junket lines of credit. However, following each drawdown of a line of credit by the junket operator or junket representative, the CPVs, gaming chips or cash equivalents issued by SCA – to be used for the relevant junket program – would be provided at the junket operator's or representative's discretion to the junket players.

j. At all times, SCA did not have any processes in place to identify how CPVs, gaming chips or cash equivalents purchased by junket operators or junket representatives, using the approved junket credit, were subsequently distributed among the junket players by the junket operator or representative.

k. SCA had no visibility as to how the junket operators funded junket players' front money or as to how junket players were paid their winnings.

l. Where a junket operator was involved in funding a junket player's front money, the junket operator also paid out winnings to the junket player.

m. SCA would apply commissions payable to junket operators to offset amounts outstanding under CCFs.

Particulars

See paragraph 386.h.

n. SCA did not appropriately identify and assess the ML/TF risks associated with junket operators redeeming or repaying credit, or the channels through which the credit was repaid.

Large cash transactions

407. Designated services provided through junket channels often involved large cash deposits and payouts.

408. At no time did SCA place any caps on cash transactions in private gaming rooms used by junkets.

Particulars

See paragraph 380.

409. At all times until April 2021, SCA required a Group Funds Disclosure Form to be completed for cash buy-ins made on behalf of a junket. This form identified the junket player(s) who contributed to the cash buy-in and the amount that each contributed.

Particulars

SCA had no documented process to analyse the Group Funds Disclosure Forms.

The Group Funds Disclosure Form was not an adequate control on its own to manage the ML/TF risks associated with large cash transactions through junkets, including risks associated with source of wealth and source of funds.

410. From 23 December 2019, SCA introduced Source of Funds Declaration forms to be completed by International Business customers for cash transactions over certain thresholds.

Particulars

See paragraphs 138.

411. The controls pleaded at paragraphs 408 to 410 did not appropriately mitigate and manage the ML/TF risks of large cash transactions through junket channels.

Remittance services

412. At no time did SCA identify, mitigate and manage the ML/TF risks of providing remittance services (items 31 and 32, table 1, s 6) through junket channels:

a. Until 12 April 2021, SCA permitted junket operators, junket representatives and junket players to transfer money between their FMAs with written authorisation.

Particulars

A Funds Authorisation Form was required to be completed authorising SCA to transfer funds from a customer's FMA to a third party's FMA.

Junket operators were permitted to transfer funds from their FMA to the FMA of a junket representative or junket player.

Junket players were permitted to transfer funds from their FMA to the FMA of a junket representative or junket operator.

Junket representatives were permitted to transfer funds from their FMA to the FMA of another junket representative, junket player, or junket operator.

b. From 14 February 2017 until 12 April 2021, SCA also permitted junket representatives to conduct transactions on the junket operator's behalf from the junket operator's FMA, if the junket operator provided written authorisation via a Funds Authorisation Form.

c. SCA permitted third party telegraphic transfers from FMAs held by junket operators, representatives and players.

Particulars

See paragraphs 216.f. and 228

There was no documented guidance or procedures to assess whether the relationship between that customer and the third party gave rise to any red flags that might indicate a money laundering risk.

d. Third party deposits, transferred via SCA Customer accounts or certain SCEG Customer accounts, could be credited to a junket operator's, representative's or player's FMA, including to repay CCFs.

Particulars

See paragraphs 220 to 231.

e. At no time did SCA identify and assess the ML/TF risks of transactions on FMAs held by junket operators or representatives.

f. The Standard Part A Programs did not include appropriate operational controls to limit or mitigate and manage the ML/TF risks of third party transfers and/or deposits at any time.

g. At no time did SCA assess the ML/TF risks of providing item 31 and 32, table 1, s 6 designated services to junket operators, representatives or players through non-transparent channels including the SCEG Customer account channel.

Particulars

See paragraphs 232, 239 to 268.

Oversight frameworks for junket customers and international VIP customers

413. The International Business department was a division of SCEG that was responsible for facilitating trips for international and interstate VIP customers visiting SCEG casinos in New Zealand and SCA for gambling and entertainment purposes.

414. The International Business department's role included the following:

a. reviewing credit applications and facilitating their consideration by those with the necessary delegated approval;

b. facilitating the movement of funds held in the SCEG Customer accounts to customers' FMAs; and

Particulars

See paragraphs 239 to 262.

c. facilitating applications from junket operators to determine their suitability to operate junket programs.

Particulars

See paragraph 397.

415. The International Business department was headed by senior SCEG personnel:

a. from 7 December 2016 until 25 February 2021, the International Business division reported directly to the Chief Financial Officer of SCEG; and

b. from 26 February 2021, the International Business department reported directly to the Chief Operating Officer Australia.

416. The International Business department had personnel located in multiple jurisdictions, including Adelaide.

417. SCA relied on the International Business department with respect to each of the functions outlined at paragraph 414.

418. The Standard Part A Programs did not include or incorporate a framework to determine whether decisions relating to:

a. SCA customers; or

b. designated services provided by SCA through junket channels, including the approval of lines of credit or CCFs for international customers and the credit limit that would apply to lines of credit or CCFs for international customers,

were within the ML/TF risk appetite of SCA.

Particulars

See paragraphs 313 to 343.

Designated services provided through individual commission programs

419. From 7 December 2016, SCA entered into arrangements with customers to play on Individual Commission Programs (**ICPs**), including on table games and EGMs.

Particulars

ICPs were arrangements between SCA and an individual to provide benefits to ICP customers, including commission on turnover, complimentary value based on a percentage of turnover which could be used on individual expenses and other benefits including accommodation, airfares, food and beverage, gaming chips and bonus points.

420. ICPs were only available to interstate or international players.

421. SCA continued to provide designated services to international VIPs via ICPs after ceasing its junket business in April 2021.

422. After junket operators at SCA ceased in April 2021, some customers who had previously been junket players were able to attend SCA as ICP customers.

Particulars

For example, in May 2022, Customer 19 recorded a turnover exceeding $93,000,000 at SCA on an international ICP.

Between 15 January 2016 and 29 April 2016, Customer 19 operated junkets at SCA. In 2019, Customer 19 operated one of SCEG's top six junkets based on turnover, with an estimated turnover exceeding $1,200,000,000.

Customer 19 played on an ICP in May 2022. During the ICP, SCA staff identified that Customer 19 engaged in cash and chip exchanges with their associates. SCA considered this was 'quasi-junket' type activity. These transactions had no apparent economic or visible lawful purpose.

See *Customer 19's risk profile*.

ICP customers sometimes attended SCA in groups. Players in those groups would often share funds and chips with each other.

ICP customers attending SCA in a group were observed by SCA staff to be:

a. transferring funds to each other's FMAs, which was permitted for ICP customers by SCA;

b. exchanging chips with one another often unrelated to gambling activity; and

c. funding other group members' buy-ins.

For example, in 2020, Customer 18 funded other guests' buy-ins on ICPs. SCA returned the funds to Customer 18 at the settlement of the ICPs.

In 2022, Customer 19 and their associates playing on ICPs were observed passing large amounts of cash and chips between one another in a series of covert exchanges.

Individual commission programs

423. For each ICP, SCA entered into **ICP agreements** with customers, including:

a. non-negotiable commission programs, which utilised non-negotiable chips;

Particulars

Non-negotiable chips were only available to international and interstate customers on commission programs and allowed SCA to track the turnover of customers playing on a non-negotiable ICP program.

b. turnover programs, which were only available on baccarat and roulette; and

c. EGM commission programs.

Particulars

A commission would be payable by SCA to the customer for each ICP. The commission was calculated by multiplying a customer's turnover by the agreed percentage as stipulated in the ICP agreement.

ML/TF risks of individual commission programs

424. The provision of table 3, s 6 designated services by SCA through ICPs involved the following higher ML/TF risks:

a. ICPs involved high volume and high turnover gambling.

Particulars

There was a minimum front money balance required for ICP customers.

The benefits available from ICPs were dependent both on the level of front money the customer presented and their subsequent turnover.

b. ICPs were only conducted in premium gaming areas of SCA.

c. ICPs exclusively used CVIs.

Particulars

See paragraphs 106.i and paragraphs 345 and 347.

ICPs could only use either cash chips, non-negotiable chips or commission chips, in order for SCA to track ICP customers turnover to determine the commission payable.

Commission chips were only available to international and interstate customers on commission programs. ICP players wagered at table games using non-negotiable chips, and were paid winnings in commission chips.

d. ICP customers were eligible to apply for CCFs and lines of credit for gambling purposes.

Particulars

See paragraphs 313 to 343.

e. SCA facilitated third party deposits for ICP customers.

Particulars

ICP customers could transfer funds from their FMA to another ICP customer's FMA.

Customer 18 provided funding to, and received funding from, other players to join individual commission programs at SCA. For example, on 10 October 2020, Customer 18 transferred $50,000 from their SCA FMA to Person 15's SCA FMA. On 11 October 2020, Customer 18 and Person 15 each conducted a $50,000 buy-in for an EGM commission program. Later that day, Customer 18 and Person 15

settled their commission programs. Customer 18 then received $54,940.20 into their SCA FMA from Person 15's SCA FMA.

See *Customer 18's risk profile*.

See paragraphs 220 to 227.

f. SCA facilitated ICP customers utilising foreign cheques.

Particulars

ICP customers who utilised foreign cheques were subject to cash out limits of no more than $25,000 or 5% of their initial front money, unless approved by SCA management for a higher amount.

See paragraphs 370 and 374.

g. The ability to conduct frequent full or partial settlement of ICPs could facilitate refining, converting or layering of illicit funds.

Particulars

Attachment 1 to Appendix B of the 2015 Standard Part A Program.

Frequent settlements increased the complexity for SCA in tracking ICP customers' transactions, making it harder to detect refining, converting or layering of illicit funds.

In May 2022, SCA conducted a post-visit review in respect of Customer 19. In a report highlighting the key ML/TF vulnerabilities identified in that review, SCA identified that recurrent large cash outs by ICP customers may facilitate ongoing cash buy-ins, which increases the complexity and burden in tracking cash. SCA identified inconsistencies between Customer 19's claims that their cash outs were their source of funds for their buy-ins. SCA's difficulties in monitoring Customer 19's transactional activity on the ICP were compounded by the use of a manual handwritten sheet to calculate turnover.

425. At no time did the Standard Part A Programs include appropriate risk-based controls to identify, mitigate and manage the ML/TF risks of the provision of designated services through ICPs for the reasons pleaded at paragraphs 419 to 424.

Record keeping on individual commission programs

426. For non-negotiable ICPs, at no time did SCA keep accurate records of the gambling activity of ICP customers, including amounts wagered, winning bets and losing bets.

Particulars

See paragraphs 399 to 405.

Under a non-negotiable program:

i. customers placed their wagers using non-negotiable chips;

ii. SCA paid out winning wagers in commission chips, with the customer retaining the non-negotiable chips used for the wager; and

iii. the commission was calculated in accordance with a pre-determined rate (a percentage value) and multiplied by the total non-negotiable turnover recorded at the time of settlement. Non-negotiable turnover means the total value of non-negotiable chips purchased by the customer, plus the value of any non-negotiable chips that had been issued in exchange for commission chips, less the total value of any non-negotiable chips returned to the cage.

427. For non-negotiable ICPs, SCA did not accurately record the gambling activity of customers because:

a. SCA only recorded estimates of the gambling activity of ICP customers for the primary purpose of calculating the commission payable to the ICP customer.

Particulars

For non-negotiable ICPs, turnover was calculated pursuant to a non-negotiable turnover methodology that facilitated calculation of rebates on turnover only and was manually inputted into Bally CMP by SCA staff based on estimates arising from observations.

Prior to July 2018, each chip exchange was recorded manually in a document by an SCA staff member at the relevant gaming table. The document recording the exchanges was then provided to Cage staff to enter the non-negotiable turnover amount into the customer's account in Bally CMP.

From July 2018, chip exchange transactions were entered directly into the Bally CMP by table games staff.

b. wins or losses of a customer were only calculated based on the value of any non-negotiable chips that a customer brought to the table, less the value of any non-negotiable chips taken by the customer when they left the table (non-negotiable win/loss) and were manually inputted into Bally by SCA staff based on estimates arising from observations; and

Particulars

See paragraph 426.

c. non-negotiable win/loss could not be accurately interpreted in the context where SCA did not record a customer's turnover on a bet by bet basis but only recorded non-negotiable turnover.

428. In the absence of appropriate records of each ICP customer's gambling activity for non-negotiable ICPs, including their turnover, wins or losses, SCA was unable to appropriately monitor the ML/TF risks associated with the provision of designated services to ICP customers.

Particulars

See paragraph 426.

429. For the reasons pleaded above at paragraphs 426 to 428 SCA did not have systems and controls in place to keep appropriate records of the provision of designated services to customers through ICPs.

430. In the absence of appropriate records of the provision of designated services to customers through ICPs, SCA was unable to adopt and maintain appropriate risk-based ML/TF controls.

The Standard Part A Programs - Transaction monitoring program

431. At all times from 7 December 2016, SCA was required by the Act and Rules to include a transaction monitoring program in its Standard Part A Program that:

a. included appropriate risk-based systems and controls to monitor the transactions of customers;

b. had the purpose of identifying, having regard to ML/TF risk, any transaction that appears to be suspicious within the terms of s 41 of the Act; and

c. had regard to unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

Particulars

Section 84(2)(c) of the Act, rr 8.1.3, 8.1.4 and rr 15.4 to 15.7 of the Rules.

432. At all times, the Standard Part A Programs included a transaction monitoring program.

a. Section 12, including table 2, of the of the 2015 Standard Part A Program set out the transaction monitoring program.

b. Section 13, including schedules 4 and 5, of the 2017-2021 Standard Part A Programs set out the transaction monitoring program.

c. The transaction monitoring programs included or incorporated in the Standard Part A Programs comprised of:

i. the manual review by the AML team or various non-AML team roles of system-generated reports specified in table 2 of the 2015 Standard Part A Program and schedule 4 of the 2017-2021 Standard Part A Programs;

ii. observations of frontline staff and observation reports submitted by front line staff to the AML team;

iii. from February 2017, the manual review of Jade transaction monitoring rule alerts by delegates of the AMLCO; and

iv. the reporting of the results of the manual review of system-generated reports or Jade transaction monitoring rule alerts to the AML/CTF Senior Management Group.

Particulars

Section 12 of the 2015 Standard Part A Program.

Section 13, paragraph 13 of the 2017-2021 Standard Part A Programs.

(the **transaction monitoring programs**)

433. From 7 December 2016 to about 17 November 2022, the transaction monitoring programs did not comply with the requirements of rr 8.1.3, 8.1.4, 15.4 to 15.7 of the Rules, by reason of the matters pleaded in paragraphs 435 to 495.

434. By reason of the matters pleaded in paragraph 433, the transaction monitoring programs did not comply with s 84(2)(c) of the Act during the period from 7 December 2016 to about 17 November 2022.

The transaction monitoring programs were not aligned to an appropriate ML/TF risk assessment

435. From 7 December 2016 to about 17 November 2022, the transaction monitoring programs were not aligned and proportionate to the ML/TF risks reasonably faced by SCA with respect to designated services, having regard to the nature, size and complexity of its business and the ML/TF risks reasonably faced.

Particulars

SCA did not appropriately identify and assess the inherent ML/TF risks of its designated services.

Rules 8.1.3 and 8.1.4 of the Rules.

436. By reason of the matters pleaded at paragraph 435, the transaction monitoring programs did not include appropriate risk-based systems and controls to monitor the transactions of customers.

Particulars

Section 84(2)(c) of the Act and r 15.5 of the Rules.

The transaction monitoring programs did not include appropriate risk-based procedures to monitor for ML/TF typologies and vulnerabilities

437. The ML/TF typologies and vulnerabilities pleaded at paragraph 24 include some indicia of transactions relating to designated services provided by SCA that may have appeared to:

a. be suspicious for the purposes of s 41 of the Act; and/or

b. involve unusual patterns of transactions, which had no apparent economic or visible lawful purpose.

438. In the absence of an appropriate assessment of its ML/TF risks, SCA was unable to design transaction monitoring systems to appropriately detect transactions that may have been indicative of the ML/TF typologies and vulnerabilities pleaded at paragraph 24.

439. SCA's transaction monitoring programs did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions, indicative of ML/TF typologies and vulnerabilities.

440. At no time did the transaction monitoring programs include appropriate risk-based procedures to consistently monitor for transactions of customers indicative of the following ML/TF typologies and vulnerabilities across all channels:

a. structuring on FMAs, including via the SCEG Customer account channel, the SCA Customer account channel and the SkyCity New Zealand channel;

b. cuckoo smurfing on FMAs, including via the SCEG Customer account channel, the SCA Customer account channel and the SkyCity New Zealand channel;

c. smurfing through third party deposits on FMAs, including via the SCEG Customer account channel, the SCA Customer account channel and the SkyCity New Zealand channel;

d. offsetting on FMAs, including through the provision of credit;

e. other transactions on FMAs involving third parties who are not the account holder;

f. transaction patterns showing deposits and withdrawals within a short timeframe;

g. even money betting and chip dumping;

h. chip or CVI cashing with minimal or no gaming activity;

i. gaming by a customer over time involving high turnover or high losses;

j. bill stuffing within minimal gaming;

k. chip walking/unknown source of chips;

l. jackpot purchases; and

m. loan sharking.

441. By reason of the matters pleaded at paragraphs 437 to 440, the transaction monitoring programs did not include appropriate risk-based procedures to monitor the transactions of customers:

a. for the purpose of identifying, having regard to ML/TF risk, any transaction that appeared to be suspicious within the terms of s 41 of the Act; and

b. that had regard to unusual patterns of transactions, which had no apparent economic or visible lawful purpose.

Particulars

Section 84(2)(c) and rr 15.6 and 15.7 of the Rules.

Transactions indicating higher customer risks

442. The Standard Part A Programs specified classes of customers who would not be considered low risk if they engaged in transactional activity that met certain criteria.

443. The transaction monitoring programs did not include or incorporate appropriate risk-based procedures to identify, for all specified classes, transactions that met the transactional criteria requiring the customer to be risk-rated above low.

Particulars

See paragraph 137.d.

There were no transaction monitoring processes to consistently identify transactional criteria that required SCA customers to be rated moderate risk by reason of:

i. a customer purchasing CVIs such as chips, gaming machine credits or gaming machine tickets and then cashing those out with little or no gaming;

ii. transactions inconsistent with customer's known background; or

iii. sudden changes in transaction patterns.

Nor were there any transaction monitoring processes to consistently identify transactional criteria that required SCA customers to be rated high risk by reason of:

i. a customer's gaming patterns not being supported by their occupation; or

ii. wagering patterns which point to balanced betting.

Nor were there any transaction monitoring processes to consistently identify transactional criteria that required SCA customers to be rated significant risk by reason of:

i. any customer who was from a high-risk jurisdiction or, from 2019, whose primary residence was in a high risk jurisdiction, and who presents front monies in excess of $100,000.

444. The system-generated reports and transaction monitoring rules in SCA's transaction monitoring program that purported to identify transactions that met the transactional criteria requiring the customer to be risk-rated above low were not supported by appropriate risk-based procedures to consistently identify customers required to be risk-rated above low.

Particulars

See paragraphs 451 and 452.

445. By reason of the matters pleaded at paragraphs 443 and 444, the transaction monitoring programs did not include appropriate risk-based systems and controls to monitor the transactions of customers who were not low risk.

Particulars

Section 84(2)(c) of the Act and r 15.5 of the Rules.

The transaction monitoring programs were largely manual and not supported by appropriate risk-based procedures

446. From 7 December 2016 the transaction monitoring programs were reliant on systems and controls based on:

a. the review by either the AML team or various non-AML team roles of system-generated reports specified in table 2 of the 2015 Standard Part A Program and schedule 4 of the 2017-2021 Standard Part A Programs;

b. from February 2017, the review of Jade transaction monitoring rule alerts by delegates of the AMLCO;

c. observations of frontline staff and observation reports submitted by front line staff to the AML team; and

d. the reporting of the results of the review of system-generated reports or Jade transaction monitoring rule alerts to the AML/CTF Senior Management Group.

Particulars

Section 12 of the 2015 Standard Part A Program.

Section 13, paragraph 13 of the 2017-2021 Standard Part A Programs.

447. At no time did the transaction monitoring programs include or incorporate appropriate risk-based automated monitoring.

Particulars

See paragraphs 448 to 452.

448. The processes pleaded at paragraph 446 were not capable of detecting suspicious or unusual patterns of transactions or behaviours across complex transaction chains involving multiple designated services.

Particulars

See paragraphs 18 and 19.

The August 2021 external review observed that SCA appeared to have a relatively low number of transaction monitoring rules within Jade that did not appear to offer much value in identifying complex, unusual large transactions and unusual patterns of transactions.

See paragraphs 179 and 180.

449. The transaction monitoring programs did not include or incorporate appropriate risk-based systems and controls to monitor transactions on EGMs, ETGs and ATGs.

Particulars

SCA's Jade transaction monitoring did not capture any EGM or ETG transactional activity.

Bally did not record EGM and ETG transactional activity where customers were playing uncarded.

The transaction monitoring programs did not include any documented processes or procedures requiring consideration of turnover and win/loss information for customers using EGMs and ETGs with their loyalty card.

450. The systems-generated reports and Jade transaction monitoring rule alerts were not appropriately risk-based and were not capable of consistently and fully identifying across all designated services:

a. transactions that may have had indicia of ML/TF typologies and vulnerabilities (as identified at paragraph 24 above);

b. transactions that may be suspicious for the purposes of s 41 of the Act; and

c. unusually large or unusual patterns of transactions, which had no apparent economic or visible lawful purpose.

Particulars

Rules 15.6 and 15.7 of the Rules.

For example:

i. One of the two transaction monitoring rule alerts directed towards identifying structuring was run monthly and could not have identified all transactions below the reporting threshold because Bally did not

contain a full record of all transactions by SCA with respect to designated services: see paragraphs 461 and 462.

ii. The other transaction monitoring rule alert directed towards structuring was designed to identify customers who conducted five or more cash transactions in one day. However, it was not capable of identifying cash deposits into the SCA Customer accounts or the SCEG Customer accounts because there were no controls to identify cash deposits in those accounts.

iii. From February 2017, SCA had a system-generated report to identify FMAs with balances of $10,000 or more. However, SCA did not have any processes, procedures or controls to manage any accounts that were identified in those reports as being dormant.

iv. The 'report identifying changes in betting habits' was compiled and reviewed monthly. The report was based on a customer's turnover relative to their buy-in on a three month basis, relative to a three-month average. The criteria for this report did not appropriately detect the ML/TF risks reasonably faced by SCA that might be reflected in changes in gaming habits relating to turnover. For example, the report did not detect escalating turnover over periods of time greater than 3 months. Further, SCA did not accurately record individual turnover for junket customers' play on junkets. Neither did it accurately record turnover for ICP players on non-negotiable programs. Consequently, the 'report identifying changes in betting habits' could not accurately reflect whether a junket player or ICP player's gambling activity had changed over time.

In relation to system-generated reports see also paragraph 451.

In relation to Jade transactions monitoring alerts see also paragraph 452.

451. The system-generated reports were not appropriately risk-based and were not supported by risk-based procedures, including because:

a. each of the reports was required to be generated manually;

b. there were no documented appropriate review criteria for persons responsible for manually reviewing the reports;

c. the persons responsible for reviewing the system-generated reports included roles outside of the AML team who did not receive any training in relation to reviewing those reports, or receive adequate ML/TF risk awareness training appropriate to their role;

Particulars

The roles outside of the AML team were the Cage Manager, Surveillance Operations Manager, Table Games Shift Managers and Gaming Machine Shift Managers / Supervisors.

SCA employees did not receive adequate ML/TF risk awareness training because as SCA did not carry out appropriate ML/TF risks assessments, their risk awareness training was not capable of

covering the ML/TF risks reasonably faced with respect to all designated services: Part 8.2 of the Rules.

In the absence of appropriate training for persons tasked with the responsibility of reviewing reports, it was not possible to consistently identify unusual patterns of transactions.

For example, there was no guidance provided to SCA staff regarding how to interpret the 'report identifying changes in betting habits'. Consequently, SCA staff were unable to consistently and appropriately analyse the report for the purpose of identifying ML/TF risks. In particular, no guidance was given to SCA staff regarding how the relationship between turnover and buy-in might be indicative of ML/TF risks, and what type of transactional behaviour they should look for in the report.

d. most of the reports were only reviewed monthly; and

e. there was no appropriate procedure relating to the reporting of the results of the review to the AMLCO.

452. The Jade transaction monitoring rules were not appropriately risk-based and were not supported by risk-based procedures, including because:

a. most of the reports or alerts were required to be manually generated;

b. there was no documented process identifying the frequency with which each rule would be run or the circumstances in which each rule should be run. This was left to the discretion of the AML Analyst;

Particulars

From 6 November 2017, an AML Analyst role procedure document (as amended) identified when certain rules should be run.

c. there was no documented process identifying the frequency with which each report or alert would be reviewed;

d. Jade relied on data entered from Bally, which was subject to limitations;

Particulars

See paragraphs 461, 462, 470, 540.d and 541.d.

In July 2022, SCA conducted a review of Jade's transaction monitoring capabilities, and found that the Jade system did not ingest all data from SCA's Bally system and additional source systems, which affected the transaction monitoring rules that could be implemented in the Jade system.

e. Jade also required some information to be manually entered, which was labour-intensive and required data gaps to be filled by the AML team;

f. there were no appropriate processes or procedures in place to review or update transaction monitoring rules to respond to new or emerging ML/TF risks;

g. the transaction monitoring rules were not capable of consistently identifying transactions consistent with the ML/TF typologies pleaded at paragraph 24;

Particulars

See, for example, particulars at paragraph 450 in relation to the structuring rules.

As part of SCA's AML Enhancement Programme, in July 2022 SCA conducted a review of Jade's transaction monitoring capabilities, and found that the existing transaction monitoring rules were not optimally configured to generate meaningful alerts.

h. there were inadequate criteria to guide the review of Jade reports or alerts; and

i. there were no documented processes or procedures requiring the AMLCO to monitor the reviews of Jade reports or alerts performed by delegates.

Particulars

The September 2021 external review in September 2021 identified that there was no information in the Standard Part A Programs setting out how the AMLCO monitors the reviews performed by its delegates to ensure a correct and complete assessment of alerts or reports.

The report also identified that the Jade system appeared not to be functionally conducive to working efficiently, created multiple processing issues and inefficiencies, and resulted in no tangible or actionable outputs.

See particulars at paragraph 453 with respect to SCA's AML Enhancement Programme.

453. The resourcing of the AML team did not support the consistent generation, review and actioning of system-generated reports or transaction monitoring rule alerts as required by the transaction monitoring programs.

Particulars

As part of SCA's AML Enhancement Programme, by November 2021 three new full-time roles were added to SCA's AML team.

By May 2022, as part of the AML Enhancement Programme, SCA approved a new target operating model for the Financial Crime team. This re-structure proposed to significantly expand the AML team (now known as the Financial Crime team) to include 17 roles.

As part of SCA's AML Enhancement Programme, in July 2022 SCA conducted a review of Jade's transaction monitoring capabilities. The workflow capabilities arising after a transaction monitoring alert was generated introduced some inefficiency within the AML team and placed some constraints on the way SCA managed performance and reporting.

See paragraph 61.

454. Transaction monitoring reliant on largely manual processes was not appropriate for a business of the size, nature and complexity of SCA.

Particulars

Rule 8.1.3 of the Rules.

The 2018 external review observed that observation reports typically act as the trigger for investigations of suspicious activity, and identified an over-reliance on front line employees to identify potentially suspicious activity.

The September 2021 external review identified that the overwhelming majority of SMRs originated from observation reports, and very few if any SMRs originated from the transaction monitoring process. The review observed that no SMRs were submitted as a result of the alerts generated by Jade.

455. For the reasons pleaded at paragraphs 447 to 454, the systems and controls pleaded at paragraph 446 were not appropriate risk-based systems and controls that were capable of consistently identifying transactions that may have:

a. appeared to be suspicious for the purposes of s 41 of the Act; or

b. involved unusual patterns of transactions, which had no apparent economic or visible lawful purpose.

Particulars

Rules 8.1.3, 8.1.4, 8.2, 15.5, 15.6 and 15.7 of the Rules.

The 2016 external review found that SCA was unable to demonstrate that its transaction monitoring program was operating effectively. It observed that the transaction monitoring program required ten reports to be manually prepared and reviewed monthly, and found that transactions included within the monthly reporting are up to a month old by the time they are reviewed. The report also found that there had been no suspicious matters raised by the existing transaction monitoring program, that the underlying reports used in the transaction monitoring program did not demonstrate analysis of transactions, and that there were no processes and/or controls to assess or challenge the effectiveness of the transaction monitoring. AUSTRAC's November 2016 compliance assessment of SCA observed that SCA had not addressed these findings, and recommended that SCA immediately address the findings identified in the 2016 external review.

The 2018 external review identified that SCA was not fully utilising Jade's transaction monitoring capability to full effect due to insufficient resourcing.

The effect of this finding was that transaction monitoring activities may not be effective in identifying suspicious matters and investigating in a timely manner and an over-reliance on front line employees to identify potential suspicious activity and the compliance analyst to investigate suspicious activity using other methods.

The August 2021 external review identified that SCA appeared to have a relatively low number of transaction monitoring rules within

Jade that did not appear to offer much value in identifying complex, unusual large transactions and unusual patterns of transactions.

The September 2021 external review identified, among other issues with SCA's transaction monitoring program, that the Jade system did not appear to be optimised to monitor all customers across a comprehensive rule, the current approach was manual, time-consuming and had not had a material impact on identifying SMRs.

The September 2021 external review also identified that there were very few if any SMRs originating from the transaction monitoring process and none as a result of the alerts generated by Jade.

As part of SCA's AML Enhancement Programme, in July 2022 SCA conducted a review of Jade's transaction monitoring capabilities. The uplift of transaction monitoring capabilities is ongoing.

The transaction monitoring programs were not supported by appropriate information systems

456. At all times, the transaction monitoring capabilities of Jade were limited by reason of the matters pleaded at paragraph 452.

457. At all times, transaction monitoring by SCA through system-generated reports and transaction monitoring alerts was reliant upon data entered into Bally.

458. At all times, Bally did not contain a full record of all transactions provided by SCA with respect to designated services, including as pleaded at paragraphs 461, 462 and 541.d.

Transactions on table games

459. Until December 2018, the Table Games Supervisor was responsible for entering data in relation to items 6 and 9, table 3 designated services into Bally.

460. From December 2018, the Table Games Area Manager and the dealers at tables were responsible for entering data in relation to items 6 and 9, table 3 designated services.

461. Table games staff members did not capture all transactions at table games relating to the provision of these designated services.

Particulars

Not all transactions were recorded against a player's rating because the ratings process was based on estimates rather than actual transactions and relied on the observations of staff members.

Transactions under $10,000

462. At all times, Bally contained limited records of transactions under $10,000 conducted by SCA unless the customer elected to play carded (that is, with their loyalty card):

a. exchanging cash or cheques for gaming chips or CVIs up to $10,000 were not recorded in Bally;

b. currency exchanges up to $1,000 were not recorded in Bally;

c. payment of winnings in relation to EGMs and ATGs under $10,000 were not recorded in Bally; and

d. EGM jackpot wins of more than $5,000 were only recorded in surveillance logs against the customer's name on the main gaming room floor.

463. While the Standard Part A Programs included or incorporated some transaction monitoring rules designed to identify transactions under $10,000, the effectiveness of such rules was compromised by Bally's incomplete records.

464. By reason of the matters pleaded at paragraphs 462-463 and 469-470 the transaction monitoring rules did not appropriately cover transactions under $10,000.

465. By reason of the matter pleaded at paragraph 464, the transaction monitoring program was unable to appropriately monitor for transactions that were structured to avoid reporting of cash transactions of $10,000 or above.

Uncarded transactions or unrated play

466. Customers of SCA could elect to play **uncarded**. That is, a customer could elect to buy-into or enter into a table game, EGM or ETG within the meaning of item 6, table 3, s 6 without using their loyalty card.

467. SCA recorded carded or rated play differently to uncarded or unrated play:

a. where customers played carded (that is, using their loyalty card), they were subjected to 'rated play'; and

Particulars

Customers were able to have their play 'rated' when they inserted their loyalty card into an EGM or ETG. The customer's session of play would cease to be 'rated' once the customer had removed their loyalty card.

Customers were also able to have their play rated at manual table games when they presented their loyalty card (subject to the limitations identified at 355.d).

b. the details of a customer's rated play were tracked, recorded and stored in the customer's individual Bally profile.

468. In circumstances where customers elected to play uncarded, and had engaged in a threshold transaction that was required to be reported, SCA created an uncarded account with an identification number.

469. SCA did not track, record and store play that was 'unrated' where a customer played uncarded (subject to the matter pleaded at paragraph 468).

Particulars

Gaming activity on EGMs and ETGs was not recorded in uncarded accounts.

SCA relied on the observations of frontline staff and surveillance to monitor the transactions of customers in circumstances where their play was unrated.

470. At all times, Bally contained limited records of transactions of customers playing uncarded, unless they were threshold transactions not conducted on EGMs and ETGs.

471. By reason of the matters pleaded at paragraphs 466 to 470, the transaction monitoring programs were unable to consistently attribute transactions to individual customers.

472. A reporting entity cannot consistently identify transactions that may be:

a. suspicious for the purposes of s 41 of the Act; or

b. unusually large or involve unusual patterns with no apparent economic or visible lawful purpose

in the absence of appropriate KYC information relating to the customer conducting the transaction.

473. By reason of the matters pleaded at paragraphs 456 to 472, from 7 December 2016 to about 17 November 2022 the transaction monitoring programs were not aligned to the nature, size and complexity of SCA's business, having regard to the ML/TF risks it reasonably faced.

Particulars

Rule 8.1.3 of the Rules.

474. By reason of the matters pleaded at paragraphs 456 to 473, from 7 December 2016 to about 17 November 2022, the transaction monitoring programs did not include appropriate risk-based systems and controls to monitor the transactions of customers.

Particulars

Rules 8.1.3, 8.1.4, 15.5, 15.6 and 15.7 of the Rules.

The transaction monitoring programs were not capable of appropriately monitoring financial services or gaming account transactions

475. From 7 December 2016 to about 17 November 2022, the transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers in relation to:

a. items 6 and 7, table 1, s 6 designated services with respect to loans or credit;

b. items 13, table 3, s 6 designated services with respect to gaming accounts; and

c. items 31 and 32, table 1, s 6 designated services with respect to remittance,

by reason of the matters pleaded at paragraphs 476 to 487.

Particulars

Rules 8.1.3, 15.5, 15.6 and 15.7 of the Rules.

Loans or credit

476. From 7 December 2016 to about 17 November 2022, the transaction monitoring programs did not include any risk-based systems and controls to monitor transactions of customers with respect to items 6 and 7, of table 1, s 6 designated services.

Particulars

The system-generated reports and the transaction monitoring rules did not expressly apply to items 6 and 7, s 6 designated services.

The transaction monitoring programs did not include or incorporate any processes that were capable of monitoring items 6 and 7, table 1,

s 6 designated services, having regard to the ML/TF risks pleaded at paragraph 342.

See also paragraphs 343.a to 343.b, and the particulars to paragraphs 134.b and 493.

FMAs, including transactions facilitated through the SCEG and SCA Customer account channels and the SkyCity New Zealand channel

477. From 7 December 2016, the transaction monitoring programs did not include appropriate risk-based systems and controls to monitor the transactions of customers with respect to items 13, table 3, s 6 designated services, by reason of the matters pleaded at paragraphs 478 to 484 below.

Particulars

Item 13, table 3, s 6 designated services were provided with respect to FMAs.

See paragraphs 435 to 474.

478. The transaction monitoring programs did not include appropriate risk-based systems and controls to consistently monitor the provision of item 13, table 3, s 6, designated services to customers for the purposes of identifying any transactions that may be suspicious or unusual, having regard to the ML/TF risks pleaded at paragraph 216 with respect to FMAs.

479. At no time did the transaction monitoring programs include appropriate risk-based systems and controls to monitor FMA transactions of customers in relation to item 13, table 3, s 6 designated services through the SCEG Customer account channel, the SCA Customer account channel or the SkyCity New Zealand channel, including by reason of the matters pleaded at paragraphs 480 to 484.

SCEG Customer account channel

480. SCA did not monitor transaction activity on the SCEG Customer accounts for the purpose of s 36 of the Act, but instead relied on the transactions applied to the customer's FMA.

481. The process pleaded at paragraph 480 was not appropriately risk-based, including because:

a. The SCEG International Business Patron Accounts team or a SCEG New Zealand casino Cage staff member would reconcile transaction receipts from the bank as evidence of deposits and then communicate those details to SCA to facilitate the crediting of the customer's FMA as pleaded at paragraph 249.

b. Until 1 July 2017, the International Business Patron Accounts team had a practice of creating a spreadsheet to record telegraphic transfers that displayed indicators of potentially unusual activity, including for SCA customers. The SCA AML team did not have access to the spreadsheets.

c. SCA staff would credit a customer's FMA by creating a manual entry in Bally, which included the name of the customer, the amount in Australian dollars (including the applicable exchange rate, if any) and the form of deposit (if this was known).

i. The name of the person who deposited the funds would not be included.

ii. Accordingly, SCA was unable to identify and monitor for third party deposits into FMAs through the SCEG Customer account channel.

d. Prior to September 2021, the International Business Patron Accounts team would only be able to identify a cash deposit into SCEG Customer accounts if the bank teller who processed the transaction labelled it as such for SCEG Customer accounts that accepted cash deposits.

e. Prior to 26 October 2020, SCA had a practice of aggregating multiple deposits made by a customer into a SCEG Customer account and recording those transactions as a single transaction or sum in the customer's FMA in Bally:

i. multiple deposits could be indicative of structuring (if cash under $10,000) or cuckoo smurfing or both;

ii. the transaction monitoring of FMAs relied on the Bally records;

iii. SCA's policies and procedures did not provide for any transaction monitoring based on underlying transaction records, such as SCEG Customer account bank statements;

Particulars

SCEG staff did not undertake any transaction monitoring processes in relation to SCA customers.

SCA Cage staff would receive details to facilitate the crediting of the customer's FMA. SCA's main cage operations were set out in the Cash Handling Operations Procedures, which did not contain any processes for Cage staff to review underlying transaction records for the purposes of identifying structuring.

iv. the aggregation of deposits in Bally meant that the system-generated reports and Jade transaction monitoring rule alerts were unable to identify patterns of transactions that may have been indicative of money laundering; and

v. the practice of aggregation meant that unusual and suspicious activity could not be consistently identified by SCA.

f. In circumstances where a deposit was made by an overseas remitter for or on behalf of an SCA customer the information would not be recorded in Bally.

Particulars

The International Business Patron Accounts team would record this on a finance tracker sheet in New Zealand.

Until October 2018, the evidence of transfer by the overseas remitter (such as the receipt) would be emailed to relevant SCA Cage staff and a hard copy would be stored in an individual packet relating to a customer's specific trip. After October 2018, the packets were also scanned into network drives.

SCA Customer account channel

482. SCA did not monitor transaction activity on the SCA Customer accounts, but instead relied on the transactions applied to the customer's FMA.

483. The process pleaded at paragraph 482 was not appropriately risk-based, including because:

a. the system-generated reports relevant to monitoring transactions on FMAs were not supported by documented review criteria for persons responsible for manually reviewing the reports;

b. the Jade transaction monitoring rule alerts for FMAs were not supported by adequate review criteria for persons responsible for manually reviewing the reports;

c. the system-generated reports and Jade transaction monitoring rule alerts relevant to monitoring transactions on FMAs relied on data recorded in Bally, which was subject to limitations;

Particulars

See paragraphs 461, 462, and 541.d.

d. SCA did not have any controls to identify cash deposits into the SCA Customer accounts;

e. SCA did not have appropriate policies and procedures in place to identify third party transactions; and

Particulars

See paragraphs 224 to 227.

f. prior to 26 October 2020, SCA had a practice of aggregating multiple deposits made by a customer into an SCA Customer account and recording those transactions as a single transaction or sum in the customer's FMA in Bally:

i. multiple deposits could be indicative of structuring (if cash under $10,000) or cuckoo smurfing or both;

ii. the transaction monitoring of FMAs relied on the Bally records;

iii. SCA's policies and procedures did not provide for any transaction monitoring based on underlying transaction records, such as SCA Customer account bank statements;

Particulars

See paragraph 482.

SCA's main cage operations were set out in the Cash Handling Operations Procedures, which did not contain any processes for Cage staff to review underlying transaction records for the purposes of identifying structuring.

iv. the aggregation of deposits in Bally meant that the systems-generated reports and Jade transaction monitoring rule alerts were unable to identify patterns of transactions that may have been indicative of money laundering; and

v. the practice of aggregation meant that unusual and suspicious activity was not consistently identified by SCA.

SkyCity New Zealand channel

484. SCA's monitoring of transactions into FMAs via the SkyCity New Zealand channel was not appropriately risk based and was not capable of consistently identifying transactions that may have been suspicious or unusual, including because:

a. in crediting a customer's FMA in accordance with the process described at paragraphs 295 to 298, SCA Cage staff would not have been able to consistently identify transactions that may have been suspicious or unusual for the purpose of observation reports;

Particulars

The information provided by the International Business team or the SCEG Cage team to the SCA Cage team did not include details regarding the deposit of funds into the SkyCity New Zealand FMA (for example, whether this occurred through SCEG customer accounts, whether the deposit was in cash or not and the identity of the depositor).

b. the system-generated reports relevant to monitoring transactions on FMAs were not supported by documented review criteria for persons responsible for manually reviewing the reports;

c. the Jade transaction monitoring rule alerts relevant to monitoring transactions on FMAs were not supported by adequate review criteria for persons responsible for manually reviewing the reports; and

d. the systems-generated reports and Jade transaction monitoring rule alerts relevant to monitoring transactions on FMAs relied on data recorded in Bally, which was subject to limitations.

Particulars

See paragraphs 461, 462, and 541.d.

Items 31 and 32, table 1, s 6 designated services

485. The transaction monitoring programs did not include appropriate risk-based systems and controls to monitor the transactions of customers with respect to items 31 and 32 table 1, s 6 of the Act designated services, by reasons of the matters pleaded at paragraphs 480 to 484.

486. The transaction monitoring programs did not include appropriate risk-based systems and controls to consistently monitor the provision of items 31 and 32, table 1, s 6 designated services to customers for the purposes of identifying any transactions that may be suspicious or unusual, having regard to the ML/TF risks pleaded at paragraphs 255, 267, 283, 289 and 302.

487. For the reasons pleaded at paragraphs 485 to 486, remittance transactions (being items 31 and 32, table 1, s 6 designated services) that were facilitated through the SCEG Customer account channel, the SCA Customer account channel and the SkyCity New Zealand channel were not subject to appropriate risk-based monitoring under the transaction monitoring programs.

EzyPlay Guest Cards

488. The transaction monitoring programs did not include appropriate risk-based systems and controls to monitor the transactions of customers receiving designated services through the use of EZYPlay Guest Cards for the reasons pleaded at paragraph 489.

489. At no time did the Standard Part A Programs include appropriate risk-based systems and controls to monitor the transactions of customers through EZYPlay Guest Cards for ML/TF typologies and vulnerabilities.

a. SCA relied on frontline staff observation, and the review of three separate daily reports, to identify suspicious activity relating to transactions conducted through the use of EZYPlay Guest Cards.

Particulars

The daily transaction monitoring reports included:

i. a 'Cashless Out above $5k' report, which provided SCA with an overview of cashless transactions equal to or above a $5,000 threshold, including those that were conducted via EZYPlay Guest Cards (if any);

ii. a 'CRT Report', which provided SCA with an overview of all transactions conducted on each CRT (including those conducted via an EZYPlay Guest Card); and

iii. a 'Jackpot list' report of all jackpot payments sent by EGMs, which highlighted jackpots paid to all customers (including customers who attempted to transfer credits from an EGM to an EZYPlay Guest Card).

b. The controls identified at subparagraph 489a. were inadequate to identify the various indicators of ML/TF activities, typologies and vulnerabilities that EZYPlay Guest Cards were susceptible to, or indicators of ML/TF activities, including:

i. structuring;

ii. parked funds;

iii. loading and unloading funds onto the card, in circumstances where the source of funds was unknown;

iv. loading and unloading large volumes onto the card, in a manner inconsistent with the customer's profile or claimed source of funds;

v. obtaining multiple cards;

vi. refining;

vii. funds deposited and then withdrawn with minimal or no gaming activity; and

viii. transactions involving third parties.

c. As EZYPlay Guest Cards were issued without identification, the daily reports identified at subparagraph a. were unable to link behaviours indicative of ML/TF typologies to a specific customer.

Particulars

On 8 June 2018, SCA staff observed suspicious behaviour indicative of refining involving the use of four EZYPlay Guest Cards by an unidentified customer. The customer had brought a bag full of $50 notes. After the SCA Cage refused to exchange the $50 notes for $100 notes, the customer used multiple CRTs to insert the $50 notes and credit the funds to their EZYPlay Guest Cards. The same morning, the customer used a CRT to cash out approximately $2,000 from the four EZYPlay Guest Cards. The customer then added an

additional $900 cash to one of the EZYPlay Guest Cards at the same CRT, and immediately cashed this same amount out. Around two minutes later, the customer went to another CRT and performed further cash outs using multiple EZYPlay Guest Cards. In an SMR submitted to the AUSTRAC CEO, SCA staff observed that it suspected the customer was using the four EZYPlay Guest Cards to refine cash, disguise the purpose of the transactions, and distance themselves from the origin of the funds. When submitting the SMR, SCA was unable to identify the customer: SMR dated 12 June 2018.

Transactions facilitated through junkets

490. From 7 December 2016 to 12 April 2021, the transaction monitoring programs did not include appropriate risk-based systems and controls to monitor the transactions of customers receiving designated services through junket channels, for the reasons pleaded at paragraphs 491 to 494.

Particulars

Rules 8.1.3, 15.5, 15.6 and 15.7 of the Rules.

491. The transaction monitoring programs were not able to appropriately monitor the designated services provided through junket channels because:

a. SCA did not make or keep records of transactions conducted by individual junket players.

Particulars

The Standard Part A Programs did not require SCA to make and keep records of the designated services provided to individual junket players under a junket program.

At all times, the gaming activity of junket players was recorded by SCA collectively under the junket program, and not on an individual player basis.

SCA did not record the gaming activity of individual junket players. Instead, SCA recorded the turnover and win/loss of the junket program collectively against the junket operator's FMA.

See paragraphs 399 to 401.

b. Therefore, at no time did SCA appropriately monitor the gaming activity of individual junket players.

c. Instead, SCA applied transaction monitoring processes to the junket program participants as a whole, by monitoring transactions recorded against the junket operator.

492. The failure to appropriately monitor the gaming activity of each junket player individually meant that SCA could not identify suspicious transactions, where, for example, a junket player's level of play was not commensurate with their source of wealth or funds.

493. The transaction monitoring programs did not include appropriate risk-based systems and controls to monitor transactions relating to table 1, s 6 designated services (loans and remittance) provided through junket channels.

Particulars

When a junket operator or junket representative applied for credit, SCA conducted a risk assessment that was largely focussed on credit risk not ML/TF risk.

At no time did SCA have any processes in place to identify how, for example, the gaming chips issued by SCA, based on the approved junket credit, were subsequently distributed among the junket players by the junket operator or representative.

See paragraph 406.

494. The transaction monitoring programs did not include appropriate risk-based systems and controls to monitor deposits to FMAs through the SCEG Customer account channel, SCA Customer account channel or the Sky New Zealand channel on behalf of junket operators or players.

Particulars

See paragraphs 480 to 487.

Assurance processes with respect to the transaction monitoring programs

495. The transaction monitoring programs did not include or incorporate appropriate risk-based systems and controls for assurance.

a. There were no quality assurance processes at the operational level, such as a 'four eye check' or peer review, to confirm that processes in the transaction monitoring programs (such as review of manual reports) were being applied correctly, including by the AMLCO.

b. There were no controls for reviewing whether transaction monitoring criteria or reporting were capturing behaviours of concern, including new or changed behaviours.

Particulars

The September 2021 external review identified that there was no further information in the Standard Part A Programs explaining when or how the rules will be subject to review, such as periodic review or review as a result of emerging typologies.

c. There were no appropriate controls to ensure that updates to ML/TF risk assessments or material changes to ML/TF risk profiles were recognised in the transaction monitoring programs.

d. There was no periodic review of the overall transaction monitoring framework to ensure that escalation and decision-making processes were effective and being consistently applied, and that the transaction monitoring programs were properly aligned to other AML/CTF systems and controls.

Particulars

Between August 2016 and August 2021, SCA commissioned three external reviews of its Standard Part A Programs, which incorporated the transaction monitoring programs (the 2016, 2018 and August 2021 external reviews). Each review identified areas of concern with

respect to SCA's transaction monitoring program: see particulars at paragraph 455.

Sections 84(2)(a) and (c) and rr 8.1.3 and 15.5 of the Rules.

The Standard Part A Programs – Enhanced customer due diligence program

496. At all times from 7 December 2016, SCA was required by the Act and Rules to:

a. include an enhanced customer due diligence (**ECDD**) program in its Part A Program that complies with the requirements of the Rules;

b. apply the ECDD program when:

i. SCA determines under its risk-based systems and controls that the ML/TF risk is high;

ii. a designated service is being provided to a customer who is or who has a beneficial owner who is, a foreign PEP; or

iii. a suspicion has arisen for the purposes of s 41 of the Act.

(the **ECDD triggers**).

c. include appropriate risk-based systems and controls in their ECDD program so that, in cases where one or more of the circumstances identified in paragraph 496.b above arises, SCA was required to undertake measures appropriate to the circumstances, including the range of measures in rule 15.10 of the Rules (**ECDD measures**), including but not limited to:

i. clarify or update KYC information already collected from the customer;

ii. clarify or update beneficial owner information already collected from the customer;

iii. obtain any further KYC information or beneficial owner information, including, where appropriate, taking reasonable measures to identify the customer's source of wealth and funds and the beneficial owner's source of wealth and funds;

iv. undertake a more detailed analysis of the customer's source of wealth and funds and the beneficial owner's source of wealth and funds;

v. undertake a more detailed analysis and monitoring of the customer's transactions;

vi. seek senior management approval for continuing a business relationship with the customer and whether a designated service should continue to be provided to a customer; and

vii. consider whether a transaction or particular transactions should be processed.

Particulars

Section 84(2)(c) of the Act and rr 1.2.1 (definition of KYC information), 8.1.3 and 8.1.4, 15.8 to 15.11 of the Rules.

497. An ECDD program must include appropriate systems and controls to apply ECDD measures to customers falling within r15.9(1) and (2) from time to time, on a risk-basis.

Particulars

Sections 36, 84(2)(a) and (c) of the Act; and rr 8.1.3, 8.1.4, 8.1.5, 15.9 and 15.10 of the Rules.

498. At all times, the Standard Part A Programs included an enhanced customer due diligence program (the **ECDD Programs**).

a. Section 17 of the 2015 Standard Part A Program set out the ECDD Program;

b. Section 14 of the 2017- 2021 Standard Part A Programs set out the ECDD Program; and

c. from around May 2018, the ECDD template SOP, which was a form to centralise ECDD information located in multiple systems.

499. By reason of the matters pleaded in paragraph 501 to 528 below, the ECDD Programs in the Standard Part A Programs did not comply with rr 15.8 to 15.11 of the Rules from 7 December 2016 to about 17 November 2022.

500. By reason of the matters pleaded in paragraph 499, the Standard Part A Programs did not comply with s 84(2)(c) of the Act.

Systems and controls to determine when a customer should be referred for ECDD

501. From 7 December 2016, the ECDD Programs did not include appropriate systems, controls and procedures for SCA to apply ECDD to customers, as and when required on a risk-basis, who were:

a. determined to pose high ML/TF risk;

b. foreign PEPs or had a beneficial owner who was a foreign PEP; or

c. subject of a suspicion that had arisen for the purpose of s 41 of the Act

for the reasons set out at paragraphs 502 to 506 below.

Identifying and escalating high or significant risk customers for the purposes of ECDD

502. The Part A Programs required ECDD to be completed on customers with a high or significant risk rating.

Particulars

Section 17 of the 2015 Standard Part A Program.

Section 14, paragraph 6 of the 2017-2021 Standard Part A Programs.

503. As SCA was unable consistently to determine when a customer should be rated high or significant risk under its Standard Part A Programs, for the reasons pleaded in paragraph 504 below, it was unable consistently to apply its ECDD Programs to these customers.

504. The ECDD Programs did not include appropriate systems, controls and procedures to identify customers who were required under the Standard Part A Programs to be categorised high or significant risk, or who presented high risks, and to escalate them for ECDD as and when appropriate on a risk basis, for the following reasons.

a. The processes for identifying and escalating customers who were not low risk by default were inadequate, for the reasons pleaded at paragraphs 133 to 137.

b. The screening procedures to identify foreign and international organisation PEPs and to identify whether a customer was on a terrorism or sanctions list or was otherwise

subject to adverse media were inadequate by reason of the matters pleaded at paragraphs 135 to 136.

c. The Standard Part A Programs did not include or incorporate a process to consistently identify customers from high risk jurisdictions and apply an automatic high risk rating.

Particulars

See *The risk assessments* above.

d. Prior to 12 May 2020, there was no written procedure in place for SCA to appropriately consider whether information received from law enforcement in relation to a customer required a customer's risk rating to be higher than moderate.

e. The transaction monitoring programs were not capable of consistently identifying and escalating customers engaging in unusual or suspicious transactions, in particular:

vi. The transaction monitoring programs were not capable of identifying and escalating customers who moved money through complex transaction chains involving both table 1 (financial) and table 3 (gambling) s 6 designated services.

vii. The transaction monitoring programs were not capable of consistently identifying and escalating customers whose transactions involved third parties or agents.

viii. The transaction monitoring programs had limited application to customers who were transacting under $10,000, who were uncarded (see paragraph 466) and who had not been the subject of ACIP. It had limited capacity to identify customers engaging in structuring.

ix. There were no procedures in the transaction monitoring program requiring escalation of customers where transactions indicating high risk had been detected.

f. For the reasons set out in paragraphs 431 to 495 and 504.e above, SCA's transaction monitoring program was unable to consistently identify customers who should be high or significant risk in accordance with the Standard Part A Programs.

g. There were no documented processes in place for the International Business team or SCA Cage team to refer customers to the AMLCO or delegate for ECDD when, during the course of a credit risk assessment, matters relevant to ML/TF risk, such as a customer's PEP status, were identified.

h. There were no processes to consistently identify when customers would be referred to senior management for approval with respect to the ongoing business relationship or the processing of transactions, in circumstances where the customer had not been rated significant risk, or high risk with respect to PEPs in the 2017-2021 Standard Part A Programs.

Particulars

Section 18 of the 2015 Standard Part A Program.

Section 14, paragraphs 10 and 11 of the 2017-2021 Standard Part A Programs.

i. The Standard Part A Programs did not include any requirement for customers who had been rated high or significant risk to undergo regular ECDD after initial ECDD was completed when the customer was first rated high or significant risk.

Particulars

The SCA Standard Part A Programs contained a requirement for PEP screening to be completed on customers rated high and significant risk once per year: section 19 of the 2017-2021 Standard Part A Programs, and Appendix B, paragraph 69 of the 2015 Standard Part A Program.

Foreign PEPs

505. From 7 December 2016 to about 17 November 2022, the ECDD Programs did not include appropriate systems, controls and procedures for SCA to consistently identify customers who were foreign PEPs for ECDD as and when required on a risk basis.

Particulars

See paragraphs 135, 136 and 504.b.

Customers in respect of whom a s 41 suspicion has arisen

506. From 7 December 2016 to September 2019, the ECDD Programs did not include appropriate systems, controls and procedures for SCA to escalate customers for appropriate ECDD when a s 41 suspicion arose.

a. Prior to September 2019, there were no clear procedures to ensure that the ECDD Programs were applied when a s 41 suspicion arose.

b. From September 2019, SCA had a SOP that provided for customers the subject of an SMR to have their risk rating elevated and to be the subject of ECDD checks.

Particulars

Rule 15.9(3) of the Rules.

High & Significant Risk Customer Elevations SOP (16 September 2019).

Systems and controls to determine what ECDD measures would be undertaken

507. From 7 December 2016 to about 17 November 2022, the ECDD Programs did not include systems and controls to carry out appropriate risk-based ECDD measures once a customer had been referred for ECDD, for the reasons pleaded at paragraphs 508 to 528.

Resources and accountabilities

508. Under the Standard Part A Programs, the AMLCO was responsible for applying the ECDD Programs.

Particulars

Section 17 of the 2015 Standard Part A Program.

Section 14 of the 2017-2021 Standard Part A Programs.

509. There were other roles that were responsible or accountable for the ECDD Programs, including:

a. the AML Analyst;

b. until July 2017, the Compliance Manager;

c. from 5 April 2021, the AML Compliance Manager;

d. from 19 July 2021, the Cash Handling Shift Manager; and

e. from 19 July 2021, the Senior Casino Manager (a role within the Table Games department).

Particulars to subparagraphs d. and e.

The AML Analyst was primarily responsible for carrying out ECDD with respect to customers.

The Cash Handling Shift Manager and Senior Casino Manager were required to review the source of funds declaration form: see further paragraph 138.

510. The roles and responsibilities established by the Standard Part A Programs did not provide for appropriate resourcing for the consistent conduct of ECDD, having regard to the nature, size and complexity of SCA and the ML/TF risks it reasonably faced.

Particulars

The September 2021 external review stated that although one example of ECDD undertaken provided by the AML/CTF team highlighted a capability to do detailed and comprehensive due diligence of a particular customer, the application of the ECDD process was unstructured and not replicated to the same standard in every instance and in a consistent manner. It also observed that carrying out appropriately extensive ECDD on other high risk customers similar to the case reviewed would be challenging given current AML/CTF team resourcing and capacity constraints.

See paragraphs 185 to 189 and 453 above.

No appropriate procedures or guidance addressing the suite of ECDD measures specified by the Rules

511. From 7 December 2016 to about 17 November 2022, the ECDD Program did not include or incorporate appropriate procedures or guidance on the suite of risk-based ECDD measures to be applied by the AMLCO or delegate for the following reasons pleaded at paragraphs 512 to 515.

512. The ECDD Programs listed some ECDD measures, but did not include appropriate processes or guidance as to:

a. which steps to apply in response to the specific ML/TF risks posted by the customer;

b. how those measures addressed the ML/TF risks posed by customer activity;

c. how to analyse and assess a customer's transactional activity; and

d. the customer risks that were acceptable and those that were not.

Particulars

Rule 15.10 of the Rules.

Section 17 of the 2015 Standard Part A Program.

Section 14, paragraph 7 of the 2017-2021 Standard Part A Programs

In around September or October 2019, SCA introduced the following SOPs relevant to the ECDD Programs:

a) High & Significant Risk Customer Elevations SOP (16 September 2019).

b) SMR reporting SOP (1 October 2019).

c) High Risk Jurisdiction SOP (17 September 2019).

d) PEP screening SOP (17 September 2019).

However, these standard operating procedures did not contain appropriate processes or guidance to determine which ECDD measures should be taken in a certain situation, or how to analyse and assess the ECDD information obtained.

For example, in October 2021, the SCEG International Gaming General Manager and the SCEG General Counsel determined to continue doing business with Customer 24, notwithstanding that they were advised that Customer 24 had attempted to use over $1,000,000 in cash for gaming, was the subject of a warrant served on SCA by a law enforcement agency, and was suspected of assisting other SCA customers to structure their transactions. In reaching this decision, SCEG International Gaming General Manager and the SCEG General Counsel recorded that SCEG was not aware of any adverse information in respect of Customer 24 and SCA had no reason to suggest Customer 24 had done anything to warrant a banning order.

In March 2021, an SCA AML Analyst conducted a compliance investigation and concluded that Customer 21's gaming and transactional history appeared to be relatively harmless. The AML Analyst reached this conclusion despite the fact that, by this date, SCA had:

a. given the AUSTRAC CEO seven SMRs in respect of Customer 21 reporting large and suspicious cash transactions with a value of more than $554,700; and

b. observed on at least four occasions that Customer 21 was engaged in loan sharking with large amounts of cash in concert with other high risk customers including Customer 2 and Customer 27.

513. By reason of the matters pleaded at paragraphs 514 and 515, the Standard Part A Programs did not provide for a consistent approach to ECDD and the ECDD measures were not capable of being consistently applied.

Particulars

The September 2021 external review observed that the application of the ECDD process was unstructured and not replicated to the same standard in every instance and in a consistent manner. The ECDD

process appeared to be ad-hoc and discretionary, with no formal process or procedure setting out the relevant measures to be undertaken when completing ECDD based on the level of ML/TF risk faced.

514. The ECDD Programs did not set out appropriate ECDD measures that were aligned to the nature, size and complexity of SCA's business and the ML/TF risk posed by customers.

515. The ECDD Programs did not include appropriate procedures that were capable of being consistently applied to the ML/TF risk posed by customers, including to ensure:

a. analysis of the full suite of designated services received by customers across multiple transaction chains and channels, including designated services provided under table 1, s 6;

b. analysis of third party transactions; and

c. that source of wealth and source of funds would be appropriately assessed (see paragraphs 516 and 517 below).

Particulars

Rule 15.10 of the Rules.

Source of wealth and source of funds

516. At no time did the ECDD Programs include appropriate systems and controls for SCA to obtain, analyse, verify and record source of wealth or source of funds information with respect to customers for the purposes of carrying out ECDD for the following reasons:

a. The ECDD Programs required the AMLCO or delegate to take reasonable measures to identify the sources of wealth and funds for PEPs who were rated at least high risk.

b. The reasonable measures were at the discretion of the AMLCO or delegate, and were not subject to appropriate guidance.

Particulars

Section 15 and 17 of the 2015 Standard Part A Program; section 14, paragraph 11 of the 2017-2021 Standard Part A Programs.

c. The Standard Part A Programs required source of wealth or source of funds information to be obtained in limited circumstances.

Particulars

See paragraph 138 above.

For example, prior to 19 July 2021, SCA did not require customers transferring funds to SCA by electronic transfer to provide source of wealth information with supporting documentation.

On and from 19 July 2021, SCA required a source of wealth declaration form, with supporting information, to be completed by domestic customers who made an inward ETF transfer of $300,000 or more, and international customers who made an inward ETF transfer of $1,000,000 or more.

In July 2021, SCA initiated a process of collecting source of wealth information from all of its current top tier (Black) loyalty program members.

d. At no time were there appropriate processes or controls for SCA to identify customers whose transactions or gaming activity did not align with their stated occupation, for the purposes of ECDD.

Particulars

Any customer whose gaming patterns were not supported by their occupation and there was no other reasonable explanation to support their level of turnover was a trigger for elevation to high risk: section 13 of the 2015 Standard Part A Program and section 3 of the 2017-2021 Standard Part A Programs.

However, SCA was unable to consistently identify customers whose gaming activity was inconsistent with their source of wealth or stated occupation.

For example, between 7 December 2016 and 8 August 2021, Customer 32 recorded a turnover at SCA exceeding $44,000,000. At all times, SCA understood Customer 32 to be a truck driver. At no time was Customer 32's source of wealth or stated occupation consistent with their gaming activity. It was not until 9 August 2021 that SCA issued a ban in respect of Customer 32.

See *Customer 32's risk profile,* below.

e. There were no processes to ensure that source of wealth information obtained by International Business for the purpose of credit risk assessments was referred, on a risk basis, to the AMLCO at SCA for the purposes of ECDD.

f. There were no documented systems or processes in place to ensure that the results of any source of funds or source of wealth enquiries or analyses conducted by SCEG were recorded against the customer's profile in Bally or other information system accessible by SCA employees responsible for ECDD.

g. The ECDD Programs did not include or incorporate any guidance or criteria for the analysis of source of wealth information, having regard to ML/TF risks or any ML/TF risk appetite to be accepted with respect to customers.

h. The Standard Part A Programs did not include appropriate risk-based controls to identify customers whose source of wealth was unexplained or possibly illegitimate, and in such cases, to determine whether:

   i. specific transactions should be processed; or

   ii. an ongoing relationship with the customer was within ML/TF risk appetite.

517. In the absence of appropriate information and guidance about source of wealth and source of funds, SCA was unable to carry out appropriate risk-based ECDD measures.

Particulars

Rules 15.10(1)(c), (2) and (5) of the Rules.

For example, SCA was not in a position to understand the purpose of customer transactions, or the ML/TF risks they posed. Nor were they in a position to determine the ML/TF risk posed by the customer and the ongoing business relationship.

Senior management approval

518. From 7 December 2016 to about 17 November 2022, the ECDD Program did not include appropriate systems and controls to seek senior management approval:

a. for continuing business relationships with customers, having regard to the ML/TF risks reasonably faced;

b. on whether a designated service should be provided to a customer;

c. on whether a transaction or particular transactions should be processed

for the reasons pleaded at paragraphs 519 to 523 below.

Particulars

Rules 15.10(6), (7) and 15.11 of the Rules.

519. The Standard Part A Programs did not set out appropriate criteria for the ML/TF risks that would and would not be accepted by SCA with respect to customers (**ML/TF risk appetite for customers**).

520. In the absence of a ML/TF risk appetite for customers, there was no criteria or guidance in the Standard Part A Programs against which senior management could appropriately and consistently determine whether to approve:

a. a continued business relationship with a customer;

b. the provision of a designated service (such as a loan or remittance service) to a customer;

c. a transaction or particular transactions.

Particulars

Rules 15.10(6), (7) and r 15.11 of the Rules.

For example, see paragraphs 262.h and 378.i.

521. At all times, the Standard Part A Programs provided that:

a. All customers accorded a significant risk rating would be referred to the General Manager for a decision whether to continue the business relationship, and the General Manager would liaise with the Group General Counsel before making such a decision.

b. For Foreign PEPs, or international organisation PEPs and domestic PEPs who had been accorded a high or significant risk, the AMLCO would seek the General Manager's approval for continuing a business relationship with that customer and continuing to provide a designated service to that customer.

Particulars

Sections 15 and 17 of the 2015 Standard Part A Program.

Section 14, paragraphs 10-12 of the 2017- 2021 Standard Part A Programs.

Section 3, paragraph 32 of the 2017- February 2021 Standard Part A Programs.

Section 3, paragraph 31 of the June 2021 and October 2021 Standard Part A Programs.

Section 19, paragraphs 12-14 of the 2017- 2021 Standard Part A Programs.

522. As the SCEG and SCA Boards did not set the ML/TF risk appetite for customers, there was no criteria against which senior management could appropriately determine whether to approve:

a. continuing the business relationship with a customer;

b. the provision of a designated service (such as a loan or remittance service) to a customer;

c. a transaction or particular transactions.

Particulars

Rules 15.10(6), (7) and r 15.11 of the Rules.

There was otherwise no appropriate and consistent guidance with which management could appropriately consider approving the matters pleaded at paragraph 522 having regard to ML/TF risks.

For example, on 8 August 2019, at a meeting between the SCEG General Counsel/Company Secretary, the Group General Manager Regulatory Affairs and AML, and the SCEG Chief Financial Officer, senior management agreed that Customer 11 would not be offered any designated services at SCEG pending confirmation of their source of wealth and repayment of a NZD$2,500,000 debt to a SCEG New Zealand casino. By November 2019, SCA did not have any source of wealth or source of funds information in respect of Customer 11. Despite this, SCEG continued its business relationship with Customer 11 until at least June 2020 without having obtained any source of wealth or source of funds information from Customer 11.

See *Customer 11's risk profile*, below.

523. The process for senior management to approve some loans or credit limits (items 6 and 7, table 1, s 6 designated services) did not have appropriate regard to ML/TF risk.

Particulars

See paragraph 343.

Records of ECDD

524. From 7 December 2021, the ECDD Programs were not supported by appropriate information management and record keeping.

525. By reason of the deficiencies in information and record keeping pleaded at paragraphs 456 to 474 above:

a. SCA did not have a full view of customers' transactions for ECDD purposes; and

b. the procedures in the ECDD Programs were not capable by design of operating as intended.

526. At no time did SCA keep adequate or appropriate records of ECDD carried out with respect to a customer, such as records of the ECDD measures taken or conclusions formed following ECDD.

Particulars

In or around May 2018, SCA introduced an ECDD template SOP form to centralise ECDD information located in multiple systems.

In relation to the period prior to May 2018, due to the various documents and systems used to record the ECDD undertaken by SCA, SCA remains unable to produce basic information in relation to the extent of ECDD conducted during that period.

There was no documented guidance in place about how the ECDD template SOP should be used.

The August 2021 external review tested a sample of 20 customers deemed as high risk by SCA, in relation to the application of SCA's ECDD Program. For 19 of the 20 customers reviewed, the reviewer was unable to determine what reasonable measures had been taken to verify a customer's source of funds or source of wealth.

527. This lack of records meant that SCA did not have a full view of a customer's history and risk profile when conducting ECDD on a customer that had previously been subject to ECDD.

528. At no time did the Standard Part A Programs include or incorporate appropriate systems and processes requiring all relevant or potentially adverse information relating to SCA customers to be escalated and recorded as part of the consideration of an SCA's customer's ML/TF risk profile.

Particulars

For some customers, adverse information was held by SCEG staff in relation to SCA customers, including International Business. However, there was no appropriately documented process or procedure for that information to be escalated or recorded as part of the consideration of SCA customer's risk profile. In the absence of this process, it was not clear whether the SCA AML team considered this information for the purposes of the ECDD Programs.

For example, SCEG held a copy of a third party report relating to Customer 1 dated 30 May 2016. The report identified a number of ML/TF risks posed by Customer 1, including that they were a foreign PEP, and that they were associated with overseas casinos which would have necessitated associations with overseas organised crime syndicates. It is unclear whether SCEG provided a copy of the report to SCA or recorded it as part of the consideration of Customer 1's

ML/TF risk profile. It SCEG did do so, it is not clear when this occurred. At no time did SCA identify Customer 1 as a foreign PEP: see *Customer 1's risk profile* below.

The Standard Part A Programs – Appropriate systems and controls to ensure SMR, TTR and IFTI reporting

529. At all times, Part A of an AML/CTF program was required to include systems and controls designed to ensure compliance with the obligations to report:

a. suspicious matter reports, or **SMRs**, under s 41 of the Act;

b. threshold transaction reports, or **TTRs**, under s 43 of the Act;

c. international funds transfer instructions, or **IFTIs**, under s 45 of the Act.

Particulars

Rule 8.9.1(2) of the Rules, made for the purposes of section 84(2)(c) of the Act.

SMR reporting

530. From 7 December 2016 to about 17 November 2022, the Standard Part A Programs did not include appropriate systems and controls designed to ensure compliance with the obligation to report SMRs under s 41 of the Act, for the reasons pleaded at paragraphs 531 to 539 below.

531. The SCA staff members who were responsible for SCA's SMR reporting, did not receive appropriate guidance or training on SMR reporting:

a. At all times from 7 December 2016 the AMLCO was responsible for submitting SMRs to AUSTRAC, and delegated this role to the AML Analyst.

b. SCA did not provide the AMLCO or AML Analyst with appropriate written guidance on what matters required an SMR to be given to the AUSTRAC CEO, or how this was to be determined.

Particulars

At no time did SCA have formal SMR investigation guidelines for the AML Analyst or Financial Crime team to refer to, or formal SMR guidance detailing what would constitute reasonable grounds for forming a suspicion for the purposes of s 41 of the Act. While SCA did have a SOP in place relating to SMRs from 2019, this SOP only included a checklist for creating and saving an SMR after a suspicion had been formed, rather than providing guidance as to what matters required an SMR to be given to the AUSTRAC CEO.

c. SCA did not give the AMLCO or their delegate any formal training relating to the investigation and submission of SMRs to AUSTRAC.

Particulars

At no time did SCA have a formal, documented training in relation to the investigation and reporting of suspicious matters for the purposes of s 41 of the Act.

532. The deficiencies in the transaction monitoring program, as pleaded at paragraphs 435 to 495, meant that SCA was unable to consistently identify suspicious activity within the meaning of s 41 of the Act, having regard to unusual patterns of transactions, which had no apparent economic or visible lawful purpose.

Particulars

Rules 15.4 to 15.8 of the Rules.

The September 2021 external review found that very few, if any, SMRs were the result of SCA's transaction monitoring process and none were the result of alerts generated by Jade.

A key component of SCA's transaction monitoring program was staff observation, by way of frontline staff reporting suspicious or unusual activity through observation reports. SCA staff provided feedback that they were unsure of common casino typology indicators that should result in the submission of an observation report.

533. From 7 December 2016 to about 17 November 2022, escalation processes for unusual or suspicious activity were inadequate:

a. Workflows were manual and relied on frontline staff on the casino floor or the Cage raising 'observation reports' to the AMLCO.

b. As frontline staff did not receive adequate AML/CTF risk awareness training, they were unable to consistently identify suspicious matters requiring escalation to the AML Analyst or Financial Crime team.

Particulars

See paragraphs 184, 189 and 451.c.

At risk assessment workshops conducted by SCA, staff provided feedback that they were unsure of common casino typology indicators that should result in the submission of an observation report.

This feedback was noted in SCA's August 2022 end-to end review of SMR reporting, and as a result SCA determined it would:

i. introduce a new Observation Report Form containing a list of red flag indicators;

ii. review the existing AML/CTF risk awareness training; and

iii. send broadcast emails to relevant business units reminding them to submit Observation Reports via the online form.

534. SCA did not have appropriate policies or procedures to ensure that it identified and reported suspicious matters relating to designated services provided by SCA to customers through the SCEG Customer account channel:

a. The Standard Part A Programs did not include oversight of transactions made by SCA customers into the SCEG Customer accounts, as transfers through these accounts were managed centrally through a SCEG New Zealand casino.

Particulars

Transactions into the SCEG Customer accounts were managed by the International Business Patron Accounts team and a SCEG New Zealand Cage.

See paragraphs 159, 478, 480 and 481.

b. SCEG staff did not monitor transactions through the SCEG Customer accounts for the purpose of enabling SCA to comply with the requirements of s 41 of the Act.

Particulars

See paragraphs 478, 480 and 481.

c. There were no policies or procedures in place between SCA and the SCEG New Zealand casino to ensure that SCA was discharging its SMR reporting obligations under s 41 of the Act with respect to transactions through the SCEG Customer accounts.

d. There were no policies or procedures in place between SCA and the SCEG New Zealand casino requiring SCEG staff to notify SCA of suspicious transactions through the SCEG Customer accounts that related to a customer of SCA.

Particulars

While SCEG kept records of potential unusual activity occurring through the SCEG customer accounts, SCA did not have access to these records. In addition, the Observation Reports submitted by the International Business Patron staff to the New Zealand AML team in relation to these potentially unusual or suspicious transactions were not submitted to SCA and SCA staff were not able to access them.

535. The provision of designated services via EZYPlay Guest Cards, including in circumstances where multiple cards were issued to a single customer, impacted SCA's ability to include accurate customer information in SMRs.

Particulars

See paragraphs 488 and 489.

536. Cash handling staff, who were responsible for identifying SCA's IFTIs for reporting, were not given appropriate AML/CTF training to enable them to identify potential suspicious activity relating to international transfers to or from the SCA Customer accounts.

Particulars

The Cage Manager or Cash Handling Shift Manager were responsible for reviewing and identifying IFTIs. These staff were not given appropriate training to enable them to identify potential suspicious activity relating to international transfers.

537. There was no documented process or procedure detailing the level of assurance and oversight to be applied to the SMR reporting process.

Particulars

The SMR reporting function was delegated from the AMLCO to the AML Analyst. Neither the Standard Part A Programs, nor any of

SCA's policies and procedures relating to SMRs, adequately described the assurance and oversight to be applied to the SMR process by the AMLCO.

538. On or about 30 August 2022, SCA completed an end-to-end review of the SMR reporting process as part of its AML Enhancement Programme.

539. As a result of this review, SCA determined to make several changes to address the deficiencies in its SMR processes, including:

a. implementing a written SMR Guidance document detailing what constitutes reasonable grounds for forming a suspicion; and

b. implementing a written SMR Investigation Guidelines document.

Particulars

These changes have not yet been implemented.

TTR reporting

540. From 7 December 2016 to about 17 November 2022, the Standard Part A Programs did not include appropriate systems and controls designed to ensure compliance with the obligation to report TTRs under s 43 of the Act.

a. The processes for TTR reporting were not subject to appropriate assurance.

Particulars

There was no process in place for the AMLCO to check that cash handling staff were correctly identifying all TTRs for reporting, and no second level review to confirm that the manual processes in the TTR reporting process had been completed correctly.

b. TTRs relating to transactions conducted through junket programs were likely to be reported under the junket operator's name rather than under the name of the junket representative or the player who conducted the transaction.

Particulars

Transactions conducted in relation to a junket program were recorded against the junket operator's FMA, rather than the FMA of the junket player or junket representative.

c. This made it difficult for AUSTRAC and its law enforcement partners to understand the role of different parties involved in the threshold transaction, including what transactions took place, the owner of the funds, who instructed the movement of funds, the recipient of the funds and further details of the transaction.

d. Not all transaction types were exported from Bally to Jade for TTR reporting.

e. The TTR process relied on data sourced from Bally, which was inaccurate and required significant manual review.

Particulars

From 7 December 2016 to 9 August 2021, all transactions entered in Bally were recorded as cash.

This required significant manual review to ensure that non-cash transactions were excluded for the purposes of TTR reporting.

A 2022 external review identified that manual review by the Cage Manager and Financial Crime team was required to identify threshold transactions that may be recorded as multiple transactions within Bally Cage, as separate transactions could not be identified as potential TTRs by the automated reporting screen and Jade.

The same 2022 external review identified that not all transaction types were exported from Bally to Jade, requiring manual checks to identify missed threshold transactions.

IFTI reporting

541. From 7 December 2016 to about 17 November 2022, the Standard Part A Programs did not include appropriate systems and controls designed to ensure compliance with the obligation to report IFTIs under s 45 of the Act.

a. Processes at SCA were manual and not subject to appropriate assurance.

Particulars

A 2022 external review observed that the process performed by the SCA Cage to identify IFTIs was labour-intensive and based on a review of executed transactions by transaction code in Bally Cage along with bank deposit slips, bank remittance confirmations and banks statements.

The same 2022 external review identified that there was no assurance control in place to verify if all reportable transactions had been communicated to AUSTRAC, and no second level of review to confirm that the manual processes in the IFTI reporting process had been done correctly.

b. Up until February 2021, there was limited oversight of the IFTI reporting process by the AMLCO.

Particulars

Up until January 2021, the Cage Manager and their delegates (the Cash Handling Shift Manager and Acting Cash Handling Shift Manager) were responsible for preparing and submitting IFTIs to AUSTRAC.

By August 2016, the 2016 external review had identified errors in SCA's IFTI reporting and recommended that risk based periodic checks be conducted by the AMLCO prior to submitting reports to AUSTRAC, to make sure that SCA met its IFTI reporting requirements under the Act on an ongoing basis.

The 2017, 2018 and 2019 Standard Part A Programs contained a requirement for the AMLCO to review a random selection of IFTIs each month: section 11, paragraph 23 of the 2017-2019 Standard Part A Programs.

From January 2021, the AMLCO delegated the preparation and submission of IFTIs to the AML Analyst.

From February 2021 onwards, the Standard Part A Programs required the AMLCO to regularly review IFTI reports each month to ensure that all the required information had been accurately recorded and reports submitted within required timeframes: section 11, paragraph 23 of the February 2021 and June 2021 Standard Part A Programs, and section 11, paragraph 22 of the October 2021 Standard Part A Program.

In the absence of appropriate assurance, this monthly review process was not effective.

c. There was no documented process for SCEG to communicate IFTI information to SCA, in circumstances where SCA customers had transferred funds through the SCEG Customer accounts.

d. Until 26 October 2020, SCA and SCEG's practice of aggregating customer deposits meant that SCA may have incorrectly reported IFTI transactions to AUSTRAC.

Particulars

Until 26 October 2020, some SCEG and SCA staff would aggregate multiple customer transfers into the SCA Customer accounts and SCEG Customer accounts and record these as a single transaction to a customer's FMA. This may have resulted in SCA reporting multiple IFTIs as one larger transaction.

e. SCA's practice of transferring funds to a SCEG New Zealand casino by way of inter-company journal entry, with the funds then transferred to a final destination overseas, and reporting these IFTIs as transfers to New Zealand, obscured the actual destination of the funds.

Particulars

See paragraphs 295 to 303.

f. The practice described in sub-paragraph e. made it difficult for AUSTRAC and its law enforcement partners to understand the role of different parties to the IFTI, including the source of the funds, who instructed the movement of funds, the intended final destination of the funds and further details of the transaction.

542. By reason of the matters pleaded in:

a. Paragraphs 530 to 541, the Standard Part A Programs did not comply with r 8.9.1(2) of the Rules from 7 December 2016 to about 17 November 2022.

b. Paragraph 542.a, the Standard Part A Programs did not comply with s 84(2)(c) of the Act from 7 December 2016 to about 17 November 2022.

PART B

543. From 7 December 2016, SCA's Standard AML/CTF Program included a Part B Program (the **Standard Part B Programs**), set out in:

a. Sections 20 to 25 of 2015 Standard Part B Program.

b. Sections 16 to 20 of the 2017-2021 Standard Part B Programs.

c. Section 17 of the November 2022 Standard Part B Program, including pages 39-49 (noting that the sections after section 17 are unnumbered).

Particulars

Chapters 4 and 10 and r 14.4 of the Rules

544. From 7 December 2016, the Standard Part B Programs were not programs:

a. the sole or primary purpose of which was to set out the applicable customer identification procedures (**ACIPs**) for the purposes of the application of the Act to customers of the reporting entity; and

b. that complied with the requirements of the Rules.

Particulars

Section 84(3)(a) and (b) of the Act and Chapter 4 of the Rules.

Also see Chapter 10 and r 14.4 of the Rules, made under s 39 of the Act, which provide for certain exceptions to the application of Part 2 with respect to some designated services provided by SCA.

Also see r 8.1.6 of the Rules.

545. From 7 December 2016, the Standard Part B Programs did not include appropriate risk-based systems and controls that were designed to enable SCA to be reasonably satisfied, where the customer was an individual, that the customer was the individual he or she claimed to be, for the reasons pleaded at paragraphs 546 to 555.

Particulars

Rule 4.2.2 of the Rules.

546. The Standard Part B Programs did not include appropriate risk-based systems and controls to consistently identify customers who were not low risk at the time the ACIP was being carried out:

a. Customers were considered low risk by default, with limited exceptions.

Particulars

Section 13 of the 2015 Standard Part A Program and section 3, paragraph 31 of the 2017-2021 Standard Part A Programs.

See paragraphs 122 to 132.

b. There were no systems, controls or procedures to identify customers who were not low risk prior to carrying out ACIP.

c. There were no appropriate procedures in the Standard Part B Programs to consistently trigger a review of the default risk rating at the time ACIP was being carried out, and

customers who were not low risk were unlikely to be consistently identified at the time ACIP was being conducted.

Particulars

The Standard Part B Programs' screening processes were inadequate by reason of the matters pleaded at paragraphs 97 to 113.

d. The Standard Part B Programs were accordingly not risk based.

Particulars

Rules 4.2.2 and 4.1.3 of the Rules.

547. The Standard Part B Programs did not appropriately consider the ML/TF risk posed by a customer's sources of wealth and funds.

a. While from 23 December 2019 some requirements were introduced requiring the collection of source of funds or source of wealth information under the Standard Part A Programs, at no time were there appropriate risk-based procedures to collect and analyse information with respect to source of wealth or source of funds.

Particulars

See paragraph 138.

b. While the Standard Part B Programs provided that in some circumstances enquiries would be made to determine a customer's source of wealth or source of funds, these procedures were discretionary and not appropriately risk-based.

Particulars

Rules 4.2.2 and 4.1.3(2) of the Rules.

The complexity and volume of designated services provided to customers, combined with inadequate source of funds and source of wealth information, significantly limited SCA's ability to fully understand who they were dealing with as a customer.

The failure to obtain adequate source of wealth or funds information at the time of the ACIP, on a risk-basis, affected the operation of processes in the Standard Part A Programs. For example, this failure impacted SCA's ability to identify unusual or suspicious transactions, such as unusually high turnover or losses.

c. The Standard Part B Programs provided that domestic PEPs rated high or significant risk and International Organisation and Foreign PEPs 'shall be the subject of enquiries to determine the PEPs source of wealth/source of funds', but there was no appropriate guidance regarding the nature of the enquiries to be undertaken.

Particulars

Only where public records were unhelpful in these enquiries would customers be 'invited' to complete documentation relating to source of funds or source of wealth. However, there was no risk-based requirement requiring source of wealth or source of funds information to be collected or verified.

The Standard Part B Programs did not otherwise include appropriate guidance regarding establishing a PEP's source of wealth and source of funds.

Section 19, paragraph 11 of the 2017-2021 Part B Programs, and November 2022 Part B Program.

d. The Standard Part B Programs stated that customers undertaking certain designated services would be asked to provide details of their occupations, but provision of this information by the customer was optional.

Particulars

Verification of any occupation details provided by customers was not required.

Section 20 of the 2015 Standard Part B Program, section 16, paragraph 15 of the 2017-2021 Standard Part B Programs, and section 17, paragraph 15 of the November 2022 Standard Part B Program.

Section 22 of the 2015 Standard Part B Program, section 16, paragraph 23 of the 2017-2021 Standard Part B Programs, and section 17, paragraph 23 of the November 2022 Standard Part B Program.

548. At no time did the Standard Part B Programs appropriately consider the ML/TF risk posed by the nature and purpose of SCA's business relationships with its customers, including as appropriate, the collection of information relevant to that consideration.

a. The Standard Part B Programs did not appropriately consider the nature and purpose of the business relationship with customers who were junket operators, junket representatives and junket players or ICP Customers.

Particulars

Rules 4.2.2 and 4.1.3(3) of the Rules

At all times, the Standard Part B Programs stated that 'the nature and purpose of the business relationship with each of SCA's customers is the same for all concerned, (recreational gambling) and is not in itself a factor which dictates ML/TF Risk'.

This assumption did not involve any appropriate consideration of customers' risk profiles.

549. The Standard Part B Programs did not consider the ML/TF risk posed by the types of designated services SCA provided, together with the methods or channels by which designated services were delivered.

a. At no time did the Standard Part B Programs appropriately consider the ML/TF risks of designated services provided under table 1, s 6 (such as items 6 and 7, table 1, s 6 loans and overseas/domestic remittance services under items 31 and 32, table 1, s 6).

b. At no time did the Standard Part B Programs appropriately consider the ML/TF risks involved in providing table 1, s 6 designated services (remittance services) and item

13, table 3, s 6 (FMAs) designated services through non-face-to-face channels, including through the SCA Customer account and SCEG Customer account channels.

c. The Standard Part B Programs did not appropriately consider the ML/TF risks of providing table 1 and table 3, s 6 designated services to customers through junket or other rebate channels.

Particulars

Rules 4.2.2, 4.1.3(5) and (6) of the Rules.

550. At no time did the Standard Part B Programs consider the ML/TF risk posed by the foreign jurisdictions with which SCA dealt.

a. There were no risk-based procedures within the Standard Part B Programs to identify customers from higher risk jurisdictions at the time SCA was conducting the applicable ACIP.

b. While the Standard Part A Programs linked some automatic risk ratings to whether a customer resided in a high-risk jurisdiction, a customer risk rating review was not triggered by conducting ACIP and there were no processes even within the Standard Part A Programs to consistently identify customers from high-risk jurisdictions.

Particulars

Rules 4.2.2 and 4.1.3(7) of the Rules.

See paragraphs 137.a and 146.

551. At no time did the Standard Part B Programs include appropriate risk-based systems and controls for SCA to determine whether additional KYC information would be collected about a customer and/or verified:

a. Some limited procedures to collect or verify additional KYC information about a customer were included in the Standard Part A Programs, but not included in Standard Part B Programs as part of the ACIP.

b. Aside from when foreign or international organisation PEPs were identified in the 2017-2021 Standard Part B Programs, the procedures under the Standard Part A Programs were not otherwise triggered at the time ACIP was conducted.

c. Aside from procedures to conduct checks on sources of wealth and funds for certain categories of PEPs in the 2017-2021 Standard Part B Programs, the Standard Part B Programs did not otherwise include any procedures to collect or verify additional KYC information about a customer.

d. There were no risk-based procedures in the Standard Part B Programs to determine whether to collect or verify additional KYC information relating to the beneficial ownership of funds used by the customer with respect to designated services or the beneficiaries of transactions being facilitated by the reporting entity on behalf of the customer including the destination of funds.

e. The Standard Part B Programs applied the same ‘safe-harbour’ ACIP to all customers regardless of risk.

Particulars

Rules 4.2.2, 4.2.5 and 4.2.8 of the Rules; and the definition of KYC information in r 1.2.1 of the Rules.

552. At no time did the Standard Part B Programs include ACIPs to be applied to all customers who SCA was required to identify for the purposes of Part 2 of the Act.

a. There were no procedures in the Standard Part B Programs to determine whether the exemptions in rr 10.1.3 and 10.1.4 of the Rules did not apply to a customer or prospective customer by reason of r 10.1.5 of the Rules.

b. There were no procedures in the Standard Part B Programs that required identification of customers who exchanged foreign currency by way of foreign drafts or travellers' cheques below $1,000 – noting that the exemption in r 14.4(2)(b) of the Rules applies to physical currency only.

c. There were no procedures in the Standard Part B Programs to determine whether the exemption in r 14.4(b) of the Rules did not apply to a customer or prospective customers.

Particulars

Rule 14.5 of the Rules.

d. There were no appropriate risk-based procedures in the Standard Part B Programs to apply ACIPs to prospective customers who were receiving items 6, 7, 31 or 32, table 1, s 6 designated services.

Particulars

Section 84(3)(a) of the Act.

See also sections 32 and 39 of the Act; and Chapter 10 and r 14.4 of the Rules.

There were no additional procedures to take account of the particular risks relating to remittance services, including that they were not provided face-to-face.

553. At no time did the Standard Part B Programs include appropriate procedures to collect information and documents about an agent of a customer (who was an individual) or to determine whether to verify (and to what extent) the identity of the agent.

a. In particular, the Standard Part B Programs did not contain appropriate ACIPs for identifying junket operators or junket representatives acting as agents for junket players.

Particulars

The same ACIPs as applied to all other customers subject to ACIP also applied to junket operators, junket representatives and junket participants.

Part 4.11 of the Rules.

See paragraph 398.

554. At no time did the Standard Part B Program include appropriate risk-management systems that would enable SCA consistently to determine whether a customer was a PEP, either before the provision of a designated service to the customer or as soon as practical after the designated service was provided:

a. The Standard Part A and B Programs included screening procedures that were intended to identify PEPs. As pleaded at paragraphs 135 to 136, the processes in the Standard Part A and Standard Part B Programs for screening for PEPs were inadequate for consistently identifying PEPs.

Particulars

Part 4.13 of the Rules.

Section 20 of the 2015 Standard Part B Program and section 15 and Appendix B, paragraph 90 of the 2015 Standard Part A Program.

Section 19 of the 2017-2021 Standard Part B Programs and Part B of the November 2022 Program.

555. At no time did the Standard Part B Programs include or incorporate appropriate risk-management procedures and guidance regarding PEPs, including relating to:

a. obtaining senior management approval before establishing or continuing a business relationship with the customer;

b. taking reasonable measures to establish a customer's source of wealth and source of funds; or

c. complying with Chapter 15 of the Rules, including r 15.11 with respect to a foreign PEP.

Particulars

Rules 4.13.2 and 4.13.3 of the Rules

The September 2021 external review identified that the Standard Part B Program did not describe risk-management systems and controls in relation to rule 4.13 of the AML/CTF Rules.

556. By reason of the matters pleaded in paragraphs 543 to 555, the Standard Part B Programs did not:

a. set out the ACIPs for the purposes of the application of the Act to all customers of SCA; and

b. comply with Chapter 4 of the Rules from 7 December 2016.

557. By reason of the matters pleaded in paragraph 556, the Standard Part B Programs did not comply with s 84(3)(a) and (b) of the Act from 7 December 2016.

THE NOVEMBER 2022 STANDARD PART A PROGRAM

558. On or about 17 November 2022, the SCA Board approved:

a. a Standard Part A Program (the **November 2022 Standard Part A Program**); and

b. a Standard Part B Program (the **November 2022 Part B Program**).

Particulars

The November 2022 Standard Part B Program does not include any amendment to the October 2021 Standard Part B Program.

559. The risk-based controls under the November 2022 Standard Part A Program that are intended to identify, mitigate and manage the ML/TF risks SCA reasonably faced with respect to the provision of designated services are to be set out in Standards (the **Part A Standards**).

Particulars

Under the November 2022 Standard Part A Program, a Standard is defined as a core policy document that supports the Program by prescribing the requirements SCA employees must follow in order to implement and operationalise the Program and providing additional content about the relevant process, system and/or control that SCA has put in place to comply with its obligations under the Act and Rules.

Sections 84(2)(a) and (c) of the Act.

560. The Part A Standards are yet to be developed, approved, adopted or maintained.

Particulars

Section 81 of the Act.

SCA intends to develop and adopt standards in relation to the following for the purposes of its Part A program:

i. ML/TF Risk Assessment;

ii. Customer Risk Rating;

iii. Threshold Transaction Monitoring;

iv. International Funds Transfer Instruction Reporting;

v. Suspicious Matter Reporting;

vi. Transaction Monitoring;

vii. AML/CTF Risk Awareness Training;

viii. Employee Due Diligence; and

ix. Enhanced Customer Due Diligence.

561. In the absence of Standards to operationalise and maintain the November 2022 Standard Part A Program, it is not a Part A Program that meets the requirements of the Act and Rules.

Particulars

SCA's enterprise wide AML/CTF risk assessment dated May 2022 identified that AML/CTF Control Operational Effectiveness was either sub-optimal or not assessed. The AML Enhancement Programme roadmap identified a number of delivery workstreams to operationalise the November 2022 Part A Program that would be continuing until May 2023, with a post implementation review scheduled to commence in August 2023.

The May 2022 assessment reported that the framework for Board and senior management approval and oversight was adequately designed. However, the oversight framework is yet to be supported by each of the matters pleaded at paragraph 170.

Pending finalisation and implementation of the Standards, the Part A controls are not aligned to an appropriate ML/TF risk assessment.

Sections 81 and 84(2)(a) and (c) of the Act and Chapters 8 and 15 of the Rules.

562. By reason of the matters pleaded at paragraphs 559 and 561, the November 2022 Standard Part A Program did not comply with s 84(2)(a) and (c) of the Act from 17 November 2022.

563. By reason of the matters pleaded at paragraphs 543 to 557, the November 2022 Part B Program did not comply with ss 84(3)(a) and (b) of the Act from 17 November 2022.

ONGOING CUSTOMER DUE DILIGENCE – SECTION 36 OF THE ACT

564. At all times from 7 December 2016, SCA was required by s 36(1) of the Act to:

a. monitor its customers in relation to the provision of designated services at or through a permanent establishment of SCA in Australia, with a view to identifying, mitigating and managing the risk that SCA may reasonably face that the provision of a designated service at or through a permanent establishment in Australia might (whether inadvertently or otherwise) involve or facilitate money laundering; and

b. do so in accordance with the Rules.

(**ongoing customer due diligence**)

565. At all times from 7 December 2016, SCA was required by the Rules made under s 36(1)(b), among other things, to:

a. have regard to the nature, size and complexity of its business and the type of ML/TF risk it might reasonably face, including the risk posed by customer types;

b. include appropriate risk-based systems and controls in its Part A Program to enable SCA to determine in what circumstances further KYC information should be collected or verified to enable the review and update of KYC information for ongoing customer due diligence purposes;

c. include a transaction monitoring program in its Part A program that, among other things:

   i. includes appropriate risk-based systems and controls to monitor the transactions of customers;

   ii. has the purpose of identifying, having regard to ML/TF risk (as defined in the Rules), any transaction that appears to be suspicious within the terms of s 41 of the Act;

   iii. has regard to unusual patterns of transactions, which have no apparent economic or visible lawful purpose;

d. include an enhanced customer due diligence program in its Part A program that complies with the requirements of the Rules; and

e. apply the enhanced customer due diligence program when:

   i. SCA determines under its risk-based systems and controls that the ML/TF risk (as defined in the Rules) is high;

   ii. a designated service is being provided to a customer who is or who has a beneficial owner who is, a foreign PEP; or

   iii. a suspicion has arisen for the purposes of s 41 of the Act.

f. undertake the measures specified in rr 15.10(2) and 15.10(6) in the case of a customer who is a foreign PEP.

Particulars

Section 36(1) of the Act and rr 8.1.3, 8.1.4 and 15.2 to 15.11 of the Rules.

See paragraphs 118, 121, 123, 134, 227, 231, 396 and 431 to 528.

Customer 1

566. Customer 1 was a customer of SCA during the relevant period. Between 2017 and 2020, SCA recorded turnover exceeding $120,000,000 for junkets operated by Customer 1.

Particulars

Customer 1 was a customer of SCA from at least 14 June 2016.

On 22 March 2022, SCA issued a ban in respect of Customer 1 following investigations by the SCA AML team and significant adverse open source media in respect of Customer 1.

567. SCA provided Customer 1 with designated services within the meaning of table 1 and table 3, s 6 of the Act during the relevant period including services connected to Customer 1's role as a junket operator.

Particulars

On 14 June 2016, SCA opened an FMA for Customer 1, which was closed on 22 March 2022 (item 11, table 3, s 6 of the Act).

Between June 2016 and March 2019, SCA provided lines of credit for Customer 1 on 28 occasions with a limit ranging from $300,000 to $8,100,000 (item 6, table 1, s 6 of the Act).

Between September 2017 and August 2019, Customer 1 also had access to monthly lines of credit with a limit ranging from NZD$5,000,000 to NZD$25,000,000 (item 6, table 1, s 6 of the Act).

See *Customer 1's risk profile* below.

568. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 1.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 1's risk profile

569. On and from 7 December 2016, Customer 1, and the provision of designated services to Customer 1 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 1's risk profile prior to the relevant period

a. by 7 December 2016, Customer 1 had the following risk history:

   i. SCEG possessed a report dated 30 May 2016 in relation to Customer 1 which was prepared by a third party. The report identified a number of ML/TF risks in respect of Customer 1, including that they were a foreign PEP;

Particulars

The third party report identified that:

a. Customer 1 was a foreign PEP, and had been since at least 2013;

b. during the 1990s Customer 1 had a number of roles with foreign overseas casinos, which would have necessitated associations with overseas organised crime syndicates;

c. during this period, Customer 1 was detained on a number of occasions by a foreign law enforcement agency but released without charge on each occasion and did not have a criminal record;

d. Customer 1 was a director of at least 31 companies, including Suncity, a company that was a licenced gaming promotor and operated at a number of overseas casinos;

e. Suncity had allegedly made illegal campaign contributions to a candidate for a foreign political office; and

f. funds stolen from an overseas central bank were deposited into accounts held by Suncity at an overseas casino.

On 14 June 2016, the Group General Manager – Corporate Asset Protection emailed the third party report to the SCEG General Manager Regulatory Affairs and AML and the SCEG AML Compliance and Intelligence Manager, and copied in the SCEG General Counsel and Company Secretary.

It is not known whether SCEG provided this report to SCA: see paragraph 528 above.

ii. SCA had provided Customer 1 with significant amounts of credit upon request, up to limits of $3,000,000. These lines of credit were used to fund Suncity junkets operated by other junket operators;

Particulars

See paragraphs 321 to 323, and 342 above.

Between June 2016 and October 2016, SCA provided Customer 1 with lines of credit totalling at least $5,300,000, ranging between $300,000 and $3,000,000, on four occasions.

Each of these lines of credit was used for Suncity junkets operated by other junket operators, including Person 1.

On each occasion that this occurred, Customer 1 signed a Funds Authorisation Letter, allowing the funds from their approved line of credit to be transferred from their SCA FMA to Person 1's SCA FMA. At the settlement of the junket program, any remaining funds were then transferred back to Customer 1's SCA FMA.

For example, on 18 October 2016 Customer 1 authorised the release of a line of credit to Person 1. On 21 October 2016, after the settlement of the Suncity junket operated by Person 1, Customer 1 received $3,333,334 into their SCA FMA from Person 1's SCA FMA.

iii. media reports named Customer 1 as a person linked to overseas organised crime syndicates; and

Particulars

From 30 April 2013, international media articles reported on the connection between Customer 1's junket operations and overseas organised crime syndicates. One of these articles also reported that Customer 1 was a member of a foreign political body.

On 15 September 2014, an Australian broadcast program reported that another Australian casino had dealt with Customer 1, who had links to overseas organised crime syndicates.

On 14 March 2016, Customer 1 allegedly made millions of dollars in illegal campaign donations to a candidate for political office in a foreign country.

Some of the information contained in the media reports was also contained in the third party report dated 30 May 2016 that had been received by SCEG senior management by 7 December 2016. SCA's due diligence records relating to Customer 1 did not contain contemporaneous records of the media reports: see paragraph 569.a.i above.

See paragraph 528 above.

iv. senior management was aware of media articles which reported that Customer 1 was linked to funds stolen overseas;

Particulars

By April 2016, media articles alleged that Customer 1's account at an overseas casino was used to receive funds that were allegedly stolen from a central bank in another foreign country. The theft was being investigated by a foreign government body, which indicated that it would commence civil forfeiture proceedings against the casinos and junket operators implicated in the theft, including Customer 1.

Despite these media articles being referred to in the third party report dated 30 May 2016 (see paragraph 569.a.i above), it was not until October 2016 that members of SCEG's senior management (other than those who directly received the report dated 30 May 2016) and an SCA Director became aware of these media reports.

These articles were brought to senior management's attention during consideration of Customer 1's credit application in October 2016, at which time Customer 1 was provided with credit for both SCA and another SCEG casino.

It appears that the SCA AML team did not become aware of these media articles until 13 January 2017: see particulars to paragraph 569.m below.

Customer 1's risk profile during the relevant period

b. Customer 1 was a foreign PEP;

Particulars

See paragraphs 123, 505 and 528 above.

Between 2013 and 2018, Customer 1 was a member of a foreign political body.

By at least 14 June 2016, SCEG possessed a report prepared by a third party dated 30 May 2016 that identified Customer 1 as a PEP. There are no records to suggest that this report was shared with SCA.

At no time did SCA identify Customer 1 as a foreign PEP.

c. Customer 1 was a junket operator who facilitated the provision of high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA;

i. between December 2017 and March 2020, Customer 1 operated and funded 12 junkets at SCA;

Particulars

Between 9 December 2017 and 21 March 2020, Customer 1 operated 12 Suncity junkets at SCA.

Eleven of these junkets were commission based programs, and the other junket was subject to a 50/50 revenue sharing program.

ii. between 2017 and 2020, SCA recorded that the total cumulative turnover of junkets operated by Customer 1 in the relevant period was $120,077,430 with wins of at least $4,796,190;

Particulars

See paragraphs 399 to 401 above.

In the 2018 financial year, SCA recorded that junkets operated by Customer 1 had buy-in of at least $41,471,100, turnover of $78,723,288 with wins of at least $2,161,795.

In the 2019 financial year, SCA recorded that junkets operated by Customer 1 had buy-in of at least $10,155,000, turnover of $33,885,898 with wins of at least $2,047,935.

In the 2020 financial year, despite closures related to the COVID-19 pandemic, SCA recorded that junkets operated by Customer 1 had buy-in of at least $500,000, turnover of $7,468,244 with wins of at least $586,460.

iii. between 2017 and 2020, total benefits of at least $764,983 were payable by SCA to Customer 1 in their capacity as a junket operator, which included a commission on the turnover of their junket programs;

Particulars

In 2017, total benefits of at least $109,808 were payable by SCA to Customer 1 in their capacity as a junket operator which included a commission on junket turnover.

In 2018, total benefits of at least $467,977 were payable by SCA to Customer 1 in their capacity as a junket operator which included a commission on junket turnover.

In 2019, total benefits of at least $187,198 were payable by SCA to Customer 1 in their capacity as a junket operator which included a commission on junket turnover.

iv. between 7 December 2016 and March 2020, SCA provided Customer 1 and their junket programs with significant amounts of credit upon request, up to limits of $8,100,000;

Particulars

See paragraphs 321 to 323, and 342 above.

Between 16 December 2016 and 15 March 2020, SCA provided Customer 1 with lines of credit ranging between $300,000 and $8,100,000 on 24 occasions.

A number of these lines of credit were used for Suncity junkets operated at SCA by other junket operators, including Person 1.

Between September 2017 and August 2019, Customer 1 also had access to monthly lines of credit, ranging between NZD$5,000,000 and NZD$25,000,000.

v. Customer 1 operated Suncity junkets in private gaming rooms at SCA;

Particulars

See paragraph 145(e) above.

Customer 1 operated Suncity junkets in private gaming rooms at SCA, including the Barossa Room, the Horizon Room and the Grange Room.

vi. Customer 1 had 10 junket representatives at SCA including Customer 13 and Person 2; and

vii. Customer 1 and their junket representatives facilitated the provision of high value designated services to 25 junket players at SCA including players who posed higher ML/TF risks such as Customer 2, Customer 13, Customer 14 and Person 2;

Particulars

See paragraphs 388 and 389 above.

Between 9 December 2017 and 13 July 2019, Customer 13 was a junket player on three Suncity junket programs that Customer 1 operated at SCA.

Between 15 April 2018 and 16 October 2018, Customer 2 was a junket player on two Suncity junket programs that Customer 1 operated at SCA.

Between 24 November 2019 and 25 November 2019, Person 2 was a junket player on a Suncity junket program that Customer 1 operated at SCA.

Between 16 December 2019 and 19 December 2019, Customer 14 was a main junket player on a Suncity junket program that Customer 1 operated at SCA.

d. designated services provided to Customer 1 lacked transparency as the services were provided through the channel of junket programs at SCA;

Particulars

See paragraph 392 above.

e. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 1 by remitting large amounts of money into, out of and within the casino environment via their accounts, including through high risk remittance channels:

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCEG customer account channel

SCA accepted instructions to transfer funds from Customer 1's accounts for the following transactions.

On 19 December 2017, a SCEG New Zealand casino transferred $1,679,451 from its Cage account to Customer 1's personal bank account overseas on behalf of SCA, following the settlement of Customer 1's junket program. SCA then transferred $1,679,451 from its account to the SCEG New Zealand casino;

On 23 January 2018, a SCEG New Zealand casino transferred $802,349 from its Cage account to Customer 1's personal bank account overseas on behalf of SCA, following the settlement of Customer 1's junket program. SCA then transferred $802,349 from its account to the SCEG New Zealand casino;

On 4 May 2018, a SCEG New Zealand casino transferred $481,245 from its account to Customer 1's personal bank account overseas on behalf of SCA, following the settlement of Customer 1's junket program. SCA then transferred $481,245 from its account to the SCEG New Zealand casino;

On 13 March 2019, SCA attempted to transfer $480,886 in junket winnings from Customer 1's SCA account to Customer 1's personal bank account overseas. SCA was unable to successfully send the funds, so SCA subsequently transferred the funds to a SCEG New Zealand casino. The SCEG New Zealand casino then transferred the funds to Customer 1's personal bank account overseas.

The above transfers were made by SCA to repay the SCEG New Zealand casino, after the SCEG casino transferred Customer 1's funds to Customer 1's personal bank account overseas via the SCEG Customer Account channel on behalf of SCA. This was done because SCA had issues with transferring funds to Customer 1's bank, as that bank would not accept Australian dollars. These transactions reflect a complex transaction chain involving the remittance of money, and carried a number of ML/TF risks: see paragraphs 382 to 418 above.

SCA made money available to Customer 1 in the following transactions.

On 10 September 2019, $90,552 was deposited into an account held by SCEG with an Australian bank. This amount was made available to Customer 1 by SCA and was used to repay a line of credit.

Remittances through both the SCEG customer account channel and SkyCity New Zealand channel

On 22 January 2019, a foreign company connected to Suncity used the SCEG Customer Account channel to deposit HKD$4,876,545 into a SCEG customer account. A SCEG New Zealand casino then used the SkyCity New Zealand channel to transfer the funds from Customer 1's FMA held at the SCEG New Zealand casino to Customer 1's SCA FMA. The funds were made available to Customer 1 in the amount of AUD$873,917, and were used to repay an outstanding line of credit for a Suncity junket.

Remittances through the SCA customer account channel

SCA made money available to Customer 1 in the following transactions.

On 27 March 2018, Customer 1 transferred $698,287 from their personal bank account overseas to SCA's bank account to buy back an outstanding cheque.

On 13 July 2019, Customer 1 received $2,101,860 into their SCA FMA from an unknown account.

SCA accepted instructions to transfer funds from Customer 1's accounts for the following transactions.

On 24 April 2018, Customer 1 transferred $245,322 from their SCA account to their personal bank account overseas.

Remittances through the SkyCity New Zealand channel

SCA made money available to Customer 1 in the following transactions.

Between 31 October 2018 and 29 January 2019, SCA credited $969,804 to Customer 1's SCA FMA with these funds originating from Customer 1's FMA held at a SCEG New Zealand casino. These funds were used to redeem a line of credit and a held cheque.

Remittances within the casino environment

Customer 1 transferred funds to the FMAs of Suncity junket representatives and junket players at SCA. For example:

a. on 14 December 2017, Customer 1 transferred $12,000 from their SCA FMA to a junket player's (Customer 13) SCA FMA;

b. on 16 December 2018, Customer 1 transferred $700,000 from their SCA FMA to a junket player's (Customer 14) SCA FMA; and

c. also on 16 December 2018, Customer 1 transferred $800,000 from their SCA FMA to a second junket player's SCA FMA.

f. Customer 1 was connected to other customers at SCA, including junket operators, junket representatives and junket players, and players who posed higher ML/TF risks such as Customer 2, Customer 13, Customer 14 and Person 2;

Particulars

See particulars to subparagraphs 569.c above.

Person 2 was a junket player on Customer 1's junket.

Customer 14 was previously excluded from SCEG casinos due to behavioural issues at other Australian casinos. By 7 December 2016, there had been law enforcement interest in Customer 14 for suspected money laundering, which was publicly reported by the media in July 2019. In February 2020, Customer 14 was arrested and extradited to a foreign country for suspected money laundering and corruption.

See *Customer 2's risk profile, Customer 14's risk profile* and *Customer 14's risk profile below.*

g. Customer 1, and persons associated with the Suncity junkets operated by Customer 1, transacted using large amounts of cash and chips at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 22 December 2017 and 19 October 2020, SCA gave the AUSTRAC CEO 19 TTRs detailing incoming and outgoing payments made by Customer 1 totalling $6,748,280, which comprised:

a. three TTRs totalling $195,887 in account deposits;

b. 11 TTRs totalling $4,864,122 in account withdrawals;

c. two TTRs totalling $25,500 in chip and cash exchanges; and

d. three TTRs totalling $1,662,771 in marker redemptions.

Large cash and chip transactions

Between December 2017 and March 2020, SCA frequently recorded that Customer 1 and persons associated with the Suncity junket made significant buy-ins or cash outs at SCA. For example:

a. on 14 December 2017, Customer 1 deposited $12,000 in cash into Customer 13's SCA FMA;

b. on 24 February 2018, a junket representative and player on Customer 1's junket made a buy-in with a $300,000 CPV;

c. on 16 April 2018, a junket player on Customer 1's junket made a buy-in with a $500,000 CPV. Less than an hour later, $645,000 in chips was cashed out and deposited into Customer 1's FMA. Shortly after, another $1,101,000 in chips was cashed out and deposited into Customer 1's FMA;

d. on 29 April 2018, a junket player on Customer 1's junket made a buy-in with a $1,000,000 CPV. One minute later, $90,000 in cash was deposited into Customer 1's SCA FMA at the Grange Cage. Two hours later, $1,315,500 in non-negotiable chips was deposited into Customer 1's FMA, and $13,500 in cash was withdrawn. Ten minutes later, $10,000 in cash was deposited into Customer 1's SCA FMA;

e. on 16 October 2018, Customer 2, a junket player on Customer 1's junket, was issued with a $200,000 CPV from Customer 1's FMA. Customer 2 recorded a win of $162,000 playing baccarat. Later that day, $512,900 in non-negotiable chips was deposited into Customer 1's FMA;

f. on 10 August 2019, a junket representative and player on Customer 1's junket withdrew a $200,000 CPV from Customer 1's FMA and made a buy-in in that amount. On 11 August 2019, an SCA VIP Host deposited $100,200 in chips into Customer 1's FMA on behalf of the junket; and

g. on 22 March 2020, $24,000 in chips was deposited into Customer 1's FMA. On 23 March 2020, $11,180 in cash was withdrawn from Customer 1's SCA FMA.

h. Customer 1 made some of their credit available to another Suncity junket operator, Person 1, for the purpose of funding Suncity junket programs;

Particulars

Between 16 December 2016 and 15 March 2020, SCA provided Customer 1 with lines of credit. Customer 1 made several of these lines of credit available to Person 1, for the purposes of operating Suncity junket programs: see particulars to paragraph 569.c.iv above.

On each occasion that this occurred, Customer 1 signed a Funds Authorisation Letter, authorising the funds from their approved line of credit to be transferred from their SCA FMA to Person 1's SCA FMA, and stating that at the settlement of the junket program, any

remaining funds were to be transferred back to Customer 1's SCA FMA.

For example:

a. on 12 January 2017, $1,000,000 was deposited into Customer 1's SCA FMA. Customer 1 then transferred the funds from their SCA FMA to Person 1's SCA FMA. On 31 January 2017, following the settlement of Person 1's junket program, Person 1 transferred $727,003 from their SCA FMA back to Customer 1's SCA FMA; and

b. on 24 February 2017, $6,666,666 was deposited into Customer 1's SCA FMA. Customer 1 then transferred $2,000,000 from their SCA FMA to Person 1's SCA FMA. On 25 February 2017, Person 1 transferred $2,000,000 from their SCA FMA back to Customer 1's SCA FMA.

i. at various times, Customer 1 had significant parked or dormant funds in their FMA;

Particulars

See paragraph 216(k) above.

On or around 5 February 2020, SCA's 'Transaction Monitoring Overview' report recorded that Customer 1's FMA balance was $33,313. The report noted that these funds were from a commission program in November 2019.

On or around 13 August 2020, SCA's 'Transaction Monitoring Overview' report recorded that Customer 1's FMA balance was $42,906. The report noted that these funds were from the settlement of a commission program on 23 March 2020. The Report also stated that SCA had been closed from 23 March to 28 June 2020.

j. in 2017, Customer 1 was the subject of law enforcement enquiries on one occasion at SCA;

Particulars

On 26 July 2017, SCA received a request from a law enforcement agency in respect of an IFTI given by SCA to the AUSTRAC CEO totalling $272,997 where Customer 1 was named as the customer.

k. Customer 1 had access to private gaming rooms at SCA;

Particulars

See paragraph 145(e) above.

Customer 1 had access to private gaming rooms at SCA, including the Opal Room, Barossa Room, McLaren Room and Horizon Suites.

l. from 2017, media reports named Customer 1 and their company Suncity as having engaged in proxy betting, online gambling, and underground banking, with links to organised crime syndicates;

Particulars

On 8 May 2017, a media article reported that Customer 1's company, Suncity, was engaged in proxy betting, to the extent that 80% of its business came from proxy betting and only 20% of its business related to table games.

On 9 August 2019, a media article reported that in 2012 two individuals suspected of money laundering had deposited $403,000 in cash into an account at another Australian casino, which was transferred into Customer 1's account at that casino.

On 3 September 2020, a media article reported that another Australian casino had received due diligence reports suggesting that Customer 1 was involved in overseas organised crime syndicates.

On 20 October 2020, a media article reported that another Australian casino had received information to suggest that Customer 1 was a foreign PEP with a criminal history.

SCA's due diligence records relating to Customer 1 did not contain details of these reports.

m. by January 2017, SCA was aware of a number of media articles which reported that Customer 1 was linked to stolen funds overseas;

Particulars

By April 2016, media articles alleged that Customer 1's account at an overseas casino had been used to receive funds allegedly stolen from a central bank in another foreign country: see particulars to paragraph 569.a.iv above.

Despite SCEG senior management being in possession of the third party's report dated 30 May 2016 that referred to this adverse media, it was not until 13 January 2017 that the SCA AML team became aware of these media reports, following open source searches on Customer 1: see paragraph 528 above.

n. by July 2019, SCA was aware of a number of media articles which reported that Customer 1 was linked to overseas organised crime syndicates;

Particulars

On 9 July 2019, a media article reported that Customer 1 and their company, Suncity, provided an online gambling service and utilised underground banking to move capital. The reports were denied by Customer 1 in their capacity as Chief Executive of the Suncity Group. SCA became aware of this report in late August 2019.

On 27 July 2019, a media article reported that another Australian casino dealt with junket operators, including Customer 1, who were backed by overseas organised crime syndicates. The same day, the SCA General Manager circulated the article to members of the SCEG senior management team. On 28 July 2019, the SCEG Chief Financial Officer replied and noted that the article contained no new

information and that there was no substance to the allegations it reported. On 30 July 2019, the SCA General Manager forwarded the article to the SCA General Manager Legal, Compliance & Regulatory Affairs.

On 30 July 2019, the SCEG Chief Operating Officer circulated an Australian broadcast program to several members of the SCEG senior management team, and copied in the SCA General Manager. The program reported on the alleged links between Customer 1, and other Suncity associates, and overseas crime syndicates.

Between 1 August 2019 and 5 August 2019, media articles reported that Customer 1 had been banned from entering Australia, allegedly on the basis of their links to organised crime. It was not until October 2019 that SCA became aware of these reports.

Therefore, by at least July 2019, SCA was aware of the high ML/TF risks associated with Customer 1 and the Suncity junket, which had been the subject of media reports.

o. in February 2020, the Bergin ILGA Inquiry into another Australian casino commenced, and in February 2021 the Bergin Report was publicly released which made adverse findings regarding Customer 1 and the Suncity junket;

Particulars

In February 2020, publicly accessible media articles reported that the Bergin ILGA inquiry had heard evidence relating to Suncity and Customer 1's alleged links to overseas crime syndicates.

In September 2020, the Bergin ILGA Inquiry was referred to in a report presented to SCEG and SCA senior management: see particulars to paragraph 577.b below.

In February 2021, the Bergin ILGA Report was published. The report summarised the allegations against Customer 1 and the Suncity junket contained in media and due diligence reports, and found that:

a. there were links between Customer 1, the Suncity junket and overseas organised crime syndicates; and

b. the large amounts of suspicious cash transacted at the Suncity cash administration desk in a private gaming room in another Australian casino was more probable than not money that was to be laundered.

Shortly after the publication of the Bergin ILGA Report, the SCEG General Manager Risk prepared a paper summarising the Bergin Report, which was provided to the International Business and Premium Strategy Working Group.

p. despite SCA being aware of the above adverse information regarding Customer 1, it relied on decisions made by SCEG and did not ban Customer 1 until March 2022;

Particulars

In November 2019, Customer 1's junket agreement with a SCEG New Zealand casino expired and Customer 1 submitted a renewal application. At this time, SCA's policy was that it would only give approval to junkets to operate at SCA where the junkets were approved by the SCEG New Zealand casino: see paragraphs 382 to 418 above.

As part of the renewal application, the SCEG New Zealand casino conducted an open source search, a PEP search and an iTrak search with respect to Customer 1. The open source search revealed that there were a number of media articles which stated that:

a. Customer 1 had been banned from entering Australia due to ongoing investigations regarding Suncity's alleged links to organised crime;

b. Customer 1 and other Suncity associates were connected to an overseas organised crime syndicate; and

c. Australian law enforcement had informed a foreign institution, the Hong Kong Jockey Club, in May 2017 that it was concerned that Customer 1 was involved in large-scale money laundering activities.

On 13 November 2019, the SCEG Corporate Services Executive advised the SCEG General Manager Regulatory Affairs AML that:

a. they had processed the renewal applications for Customer 1 and their 13 junket representatives; and

b. as expected, their open source search of Customer 1 had returned several media articles in relation to investigations into junket activities.

The SCEG General Manager Regulatory Affairs AML determined that SCEG had no reason to consider that Suncity was unsuitable to continue a business relationship with, and confirmed that SCEG would continue its business relationship with Suncity.

On 19 November 2019, the SCEG New Zealand casino approved the renewal of Customer 1's junket agreement.

Following the approval by SCEG, on 24 November 2019, SCA and Customer 1 entered into a Group Commission Program Agreement for Customer 1 to operate a junket program at SCA. Customer 1 subsequently operated a junket program at SCA between 24 November 2019 and 25 November 2019.

On 14 March 2020, the Suncity junket arrived at SCA to run a junket program, operated by Customer 1. On 16 March 2020, an SCA AML Advisor emailed the SCA General Manager Legal, Compliance & Regulatory Affairs and asked whether SCA should be concerned about allowing Customer 1 to operate a junket program at SCA, in

light of media reports that Customer 1 was banned from entering Australia while investigations into the Suncity junket continued.

However, because SCEG made a decision in November 2019 to continue its business relationship with Customer 1 and Suncity, the SCA General Manager confirmed that SCA would continue its business relationship with Customer 1: see paragraphs 382 to 418 above.

On 16 March 2020, SCA and Customer 1 entered into a Group Commission Program Agreement for Customer 1 to operate a junket program at SCA. Customer 1 subsequently operated a junket program at SCA between 16 March 2020 and 21 March 2020.

Suncity therefore continued to operate junkets at SCA until March 2020, when COVID-19 restrictions forced junket operations to cease.

q. in November 2021, Customer 1 was arrested in a foreign country on several charges including money laundering and illegal gambling; and

Particulars

On 27 November 2021, a media article reported that a law enforcement agency in a foreign country had issued an arrest warrant for Customer 1. The foreign law enforcement agency accused Customer 1 of operating illegal gambling activities.

Between 28 November 2021 and 30 November 2021, a number of media articles reported that Customer 1 had been arrested on 28 November 2021 by another foreign law enforcement agency and remanded on charges of alleged criminal association, illegal gambling, money laundering and encouraging foreign citizens to engage in an illegal online gambling operation.

SCA's due diligence records did not contain details of these reports.

r. SCA did not have adequate reason to believe that Customer 1's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 1 by SCA.

Particulars

See paragraph 516 above.

By 7 December 2016, SCA was aware that Customer 1 was the founder and chairman of the Suncity Group and its subsidiaries.

It was not until 28 July 2020 that SCEG requested source of wealth information from Customer 1, on behalf of several SCEG casinos including SCA. By that time, junkets operated by Customer 1 at SCA had a recorded turnover of over $120,000,000.

On 4 August 2020, Suncity provided Customer 1's source of wealth information to SCEG. The Source of Wealth Declaration in respect of Customer 1 stated that:

a. Customer 1's source of wealth came from their shareholdings in a hotel and gaming business and their role as a junket operator; and

b. Customer 1's annual commission from their junket operations was NZD$2,060,966.

Suncity provided supporting documentation including the 2019 annual reports for the Suncity Group and the company Customer 1 had shareholdings in, a spreadsheet setting out Customer 1's commission from the various junket programs they had operated at different SCEG casinos in 2019 and other business information about the Suncity Group.

On 7 October 2020, the SCEG General Manager Regulatory Affairs AML advised the SCEG Commercial Manager and the SCEG General Manager International Gaming of the following concerns about Customer 1's source of wealth information:

a. the source of wealth checks highlighted wider issues around SCEG's junket arrangements and the persons it had contractual relationships with;

b. the benefit of seeking source of wealth information from Customer 1 was questionable in circumstances where the junket was operated by Suncity; and

c. while the information provided by Customer 1 confirmed that they were a legitimate shareholder in two large companies, in terms of income streams the only information Customer 1 provided was in relation to their commission from junket programs at SCEG casinos. Customer 1 had not provided any information in relation to their salary, dividends received or savings.

The SCEG Group Manager Regulatory Affairs AML considered that the source of wealth information provided did not satisfy SCEG's obligations. On 7 October 2020, the Compliance team for a SCEG New Zealand casino rejected Customer 1's source of wealth information for all SCEG casinos.

At no time did SCA take any steps to independently verify or consider Customer 1's source of wealth. SCA did not take appropriate steps to verify Customer 1's source of wealth or source of funds in circumstances where:

a. between 2017 and 2020, turnover on junkets operated by Customer 1 exceeded $120,000,000: see paragraph 569.c.ii above;

b. from 2017, publicly accessible media articles alleged that Customer 1 was connected to overseas organised crime syndicates and underground banking, and that their

companies had engaged in illegal proxy and online betting: see paragraphs 569.l and 569.n; and

c. by November 2021, Customer 1 had been arrested in a foreign country on charges of alleged criminal association, illegal gambling, money laundering and running an illegal online gambling operation: see paragraph 569.q above.

SCA's determination of the ML/TF risks posed by Customer 1

570. SCA was unable to identify or assess the ML/TF risks posed by Customer 1 appropriately because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 1.

a. On and from 7 December 2016, Customer 1 should have been recognised by SCA as a high risk customer for the purpose of the Act and Rules for the reasons pleaded above: see *Customer 1's risk profile* above.

Particulars

Sections 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

b. It was not until 13 January 2017 that Customer 1 was rated high risk by SCA for the purpose of the Act and Rules.

Monitoring of Customer 1's transactions

571. At no time did SCA apply appropriate transaction monitoring to Customer 1's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities;

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not make or keep appropriate records of designated services provided to junket operators; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

c. SCA did not carry out adequate due diligence on source of funds in respect of third party deposits received for the benefit of Customer 1 into its bank accounts; and

Particulars

See paragraph 227 above.

d. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 1 through:

i. the junket channel; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

ii. the SCEG customer account channel, the SCA Customer account channel and the SkyCity New Zealand channel, which were high risk remittance channels.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 1's KYC information

572. SCA did not review, update or verify Customer 1's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business relationship with Customer 1, including the nature, extent and purpose of Customer 1'stransactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update or verify Customer 1's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 1's risk profile* above, there were real risks that Customer 1's source of wealth and source of funds were not legitimate.

On 8 March 2017, SCA reviewed Customer 1's profile and determined that it did not need to request any KYC information. By this date, SCA had provided Customer 1 with lines of credit ranging between $300,000 and $3,000,000 on 10 occasions, which were used by other Suncity junket operators to run junket programs at SCA.

d. to the extent that SCA reviewed Customer 1's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 1.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

In December 2016 and January 2017, SCEG conducted ECDD screening in respect of Customer 1 as part of its assessment of their various credit applications. This screening included reviews of:

a. Customer 1's gaming and credit history;

b. previous lines of credit that had been issued to Customer 1, both at SCEG casinos and other casinos;

c. open source media searches in respect of Customer 1; and

d. "derogatory information" in respect of Customer 1.

On each occasion, SCEG rated Customer 1 as medium/moderate risk and determined to grant their applications for credit. However, SCEG's focus for this risk assessment, being for the purpose of credit applications, was credit risk rather than ML/TF risks.

There are no records demonstrating that SCA conducted its own due diligence for the purposes of considering whether it was within its own ML/TF risk appetite to provide designated services to Customer 1, including lines of credit.

On 13 January 2017, SCA conducted open source searches in respect of Customer 1. These open source searches revealed media reports which named Customer 1 as being involved in alleged stolen funds and money laundering.

Following this screening, Customer 1's risk rating was elevated to high.

However, SCA did not ban Customer 1 until 22 March 2022.

Failure to apply appropriate due diligence suited to the high ML/TF risks

573. Had SCA conducted ongoing customer due diligence on and from 7 December 2016 by:

a. appropriately identifying and assessing the ML/TF risks posed by Customer 1;

b. applying appropriate risk-based transaction monitoring to Customer 1; and

c. appropriately reviewing and updating Customer 1's KYC information, having regard to the high ML/TF risks;

SCA would have been required by the Act and Rules to apply the ECDD Program to Customer 1 at a time before the date of the ECDD triggers pleaded below: see *ECDD triggers in respect of Customer 1*.

ECDD triggers in respect of Customer 1

574. SCA was required to apply the ECDD program to Customer 1 following any ECDD triggers in respect of Customer 1.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1) and 15.10 of the Rules

575. Customer 1 was determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 1* above.

576. The matter pleaded at paragraph 575 above was an ECDD trigger.

Particulars

See paragraphs 496 and 504 above.

577. SCA did not conduct appropriate risk-based ECDD with respect to Customer 1 following an ECDD trigger because:

a. on each occasion prior to 22 March 2022 that SCA conducted ECDD in respect of Customer 1 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 1 and failed to appropriately consider whether the ML/TF risks posed by Customer 1 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501, 511 and 516 to 517 above.

Credit applications

Between April 2017 and July 2019, SCEG conducted ECDD screening in respect of Customer 1 as part of its assessment of their various credit applications. This screening included reviews of:

a. Customer 1's gaming and credit history;

b. previous lines of credit that had been issued to Customer 1, both at SCEG casinos and other casinos;

c. open source media searches in respect of Customer 1; and

d. "derogatory information" in respect of Customer 1.

On each occasion, SCEG rated Customer 1 as medium/moderate risk and determined to grant their applications for credit. However, SCEG's focus for this risk assessment, being for the purpose of credit applications, was credit risk rather than ML/TF risks.

There are no records demonstrating that SCA conducted its own due diligence for the purposes of considering whether it was within its

own ML/TF risk appetite to provide designated services to Customer 1, including lines of credit.

Junket approvals

In or around June 2017 and November 2019, SCEG conducted due diligence in respect of Customer 1 to determine whether it would allow Customer 1 to operate junket programs in New Zealand. As part of the junket agreement renewal process in November 2019, SCEG conducted an open source search which identified adverse information regarding Customer 1 and Suncity: see particulars to paragraph 569.p above.

There are no records demonstrating that SCA conducted its own due diligence for the purposes of determining whether it was within its own ML/TF risk appetite to approve Customer 1 to be a junket operator at SCA: see paragraphs 382 to 418 above.

ECDD screenings

On 8 March 2017, SCA reviewed Customer 1's profile and determined that it did not need to conduct any ECDD.

Between June 2019 and October 2019, ECDD screening in respect of Customer 1 identified that:

a. financial information about the Suncity Group was publicly available, and in April 2019 it had announced a large loss of NZD$317,000,000;

b. in May 2019, Customer 1's net worth was estimated to be in excess of $3 billion;

c. publicly available information regarding Customer 1 indicated that they were a committee member of a foreign political group. Despite this, SCA failed to identify Customer 1 as a PEP at this time;

d. there were allegations that Suncity and Customer 1 were being investigated by authorities in Australia and Customer 1 had been banned from entering Australia, although Suncity denied these allegations; and

e. a media article dated 13 July 2019 stated that Customer 1 had delivered a statement denying Suncity's involvement in online gaming.

On 7 July 2021, the ECDD screening in respect of Customer 1 identified that:

a. Customer 1 had several known and presumed associates at SCA;

b. further investigation into Customer 1 and their businesses revealed that there were multiple media articles alleging that

Customer 1 had links to an overseas organised crime syndicate;

c. another media article reported that a portion of stolen funds from an overseas bank heist in 2016 was transferred to overseas casinos and spread between two junkets, including Customer 1's Suncity junket; and

d. Customer 1 had many companies under their name and had a net worth of around $2 billion.

On 13 October 2021, the ECDD screening in respect of Customer 1 identified a media article dated 10 September 2020 that reported that Customer 1 had been banned from entering Australia in 2019 due to their suspected links to organised crime and money laundering.

However, it was not until 22 March 2022 that SCA issued a ban in respect of Customer 1 following investigations by the AML team and significant adverse open source media in respect of Customer 1.

The ECDD conducted by SCA did not have appropriate regard to Customer 1's higher ML/TF risks: see *Customer 1's risk profile above.*

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 1's source of funds or source of wealth.

By reason of the matters set out in *Customer 1's risk profile* above, there were real risks that Customer 1's source of wealth and source of funds were not legitimate.

b. on any occasion prior to 22 March 2022 that senior management considered the higher ML/TF risks posed by Customer 1 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 1 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

'Transaction Monitoring Overview' reports

Between February 2020 and August 2020, Customer 1 was mentioned in two 'Transaction Monitoring Overview' reports for the period 1 November 2019 to 1 August 2020, which were provided to SCA's AML/CTF Senior Management Group for discussion at its meeting. The reports noted the current balance of Customer 1's SCA FMA: see particulars to paragraph 569.i above.

Senior management consideration

Between August 2019 and November 2019, SCEG senior management considered SCEG's relationship with Customer 1. Despite a number of adverse media reports relating to Customer 1 and Suncity, SCEG determined to continue its business relationship

with Customer 1. Following SCEG's decision, SCA also continued its business relationship with Customer 1: see paragraph 569.p above.

There are no records demonstrating that SCA senior management conducted its own due diligence for the purposes of determining whether it was appropriate to continue a business relationship with Customer 1.

On 2 August 2019, the SCEG AML Compliance and Intelligence Manager prepared an internal memorandum following allegations made against another Australian casino. The memorandum was provided to the SCEG General Manager Regulatory Affairs and AML, and copied to the SCEG General Counsel and Company Secretary. The memorandum identified that:

a. another Australian casino had come under scrutiny for its relationship with Suncity, which regularly sent junket groups to SCEG casinos;

b. media articles alleged that the Suncity junket was connected to an organised crime syndicate which was alleged to be a key organisation in the drug trade in Australia;

c. in 2018, Suncity was reportedly 'black-banned' by the Hong Kong Jockey Club; and

d. whilst Suncity denied any wrongdoing, in light of the allegations against Suncity, SCEG considered that Suncity should be deemed high risk, and that Customer 1, as the Chief Executive Officer of Suncity, should be subject to ECDD.

On the same day, the memorandum was circulated to other members of SCEG senior management, as well as the SCA General Manager Legal, Compliance & Regulatory Affairs. The Group General Manager Regulatory Affairs and AML considered that SCEG's ongoing association with Customer 1 presented reputational, regulatory and AML risks, and that the Suncity relationship needed to be considered in the context of the allegations made against it.

On 5 August 2019, the SCEG General Manager Regulatory Affairs and AML sent a further email in which they recommended writing to Customer 1 to obtain further information in relation to the allegations and their source of wealth. The SCEG General Manager recommended that SCA cease conducting further business with Suncity and Customer 1 until they provided responses and those responses were assessed. However, the SCEG Chief Financial Officer suggested that no action be taken in respect of Suncity or Customer 1 until the SCEG Board had received a paper on the issue.

On 8 August 2019, a meeting was held between the SCEG General Manager Regulatory Affairs and AML, the SCEG General Counsel and Company Secretary and the SCEG Chief Financial Officer in

respect of Suncity and Customer 1. At this meeting, it was determined that:

a. the information concerning Suncity was speculative and historical;

b. despite this, in light of the allegations, it was considered prudent to elevate the risk associated with the Suncity junket and to meet with Suncity representatives to invite their response to the allegations as part of SCEG's ongoing customer due diligence; and

c. SCEG would continue doing business with Suncity and Customer 1.

Following this meeting, the SCEG General Manager Regulatory Affairs and AML confirmed that the risk profile of Customer 1 should be elevated as a result of the media allegations. Despite this decision, at no time was Customer 1's risk rating at SCA elevated.

On 20 August 2019 the SCEG General Manager Regulatory Affairs and AML emailed several members of SCEG's senior management, as well as the SCA General Manager Legal, Compliance & Regulatory Affairs, regarding next steps. The email stated that the ongoing due diligence with respect to Suncity and Customer 1 had no bearing on SCA's continued business relationship with either Suncity or Customer 1.

In late August 2019, the SCEG Commercial Manager, International Business met with Suncity personnel overseas to discuss the allegations against Suncity. On 29 August 2019, the Commercial Manager informed SCEG senior management and the SCA General Manager Legal, Compliance & Regulatory Affairs that Suncity had denied all allegations made against it, and that Suncity would provide further information regarding its organisational structure and group operation activities.

In late September 2019, the SCEG General Manager Regulatory Affairs and AML met with Suncity representatives overseas where they again denied all of the allegations made against Suncity.

On 13 November 2019, the SCEG General Manager Regulatory Affairs and AML prepared a memorandum recording the position agreed upon at the meeting on 8 August 2019, and emailed it to the SCEG General Counsel and the SCEG Chief Financial Officer. In the report, the SCEG General Manager confirmed that they were satisfied that there were no grounds to recommend terminating the business relationship with Suncity. On 14 November 2019, the memorandum was subsequently finalised, on instruction from the SCEG Chief Financial Officer.

On 18 November 2019, the SCEG General Manager Regulatory Affairs and AML emailed the SCEG Corporate Services Executive to confirm that SCEG was comfortable with continuing its business

relationship with Suncity and entering into a further junket agreement with it upon the expiry of Suncity's current agreement.

On 28 November 2019, an SCA AML Advisor recorded on Customer 1's SCA file in iTrak that SCEG had made a decision to maintain a business relationship with Customer 1.

There are no records demonstrating that SCA conducted its own due diligence for the purposes of determining whether it was appropriate to continue a relationship with Customer 1: see paragraphs 382 to 418 above.

AFRC meetings

The AFRC was responsible for monitoring SCA in relation to several matters, including SCA's compliance with AML/CTF legislation in Australia. At each meeting, the AFRC received a report in relation to the discharge of SCA's AML/CTF obligations. These meetings were attended by SCEG and SCA senior management: see paragraphs 160 and 181 above.

On 4 December 2019, the SCEG General Manager Regulatory Affairs and AML and SCEG General Counsel presented an AML Update report to the AFRC. The report acknowledged the media allegations against another Australian casino, but nonetheless set out the reasons why SCEG management had determined to continue its business relationship with Customer 1 and Suncity.

On 1 September 2020, the SCEG General Manager Regulatory Affairs and AML and SCEG General Counsel presented an AML Update report to the AFRC. The report noted that:

a. there was an ongoing inquiry into another Australian casino, the Bergin ILGA Inquiry;

b. media reports regarding the Bergin ILGA Inquiry focused on the Australian casino's ongoing relationship with Suncity and Customer 1, despite there being allegations that Customer 1 was involved in organised crime; and

c. SCEG remained of the view that there were no grounds to terminate its relationship with Suncity. However, the report noted that SCEG would continue to monitor the Bergin ILGA Inquiry and any associated findings relating to Suncity.

On 1 December 2020, the SCEG General Manager Regulatory Affairs and AML and SCEG General Counsel presented an AML Update report for the AFRC. The report, which was prepared by Bank 2, reported that it no longer considered Suncity or Customer 1 suitable, and would not facilitate transactions involving these parties.

Decision to ban Customer 1

On 22 March 2022, SCA issued a ban in respect of Customer 1. SCA banned Customer 1 following investigations by the AML team and significant adverse open source media in respect of Customer 1.

At all times on and from 7 December 2016, there was adverse media alleging that Customer 1 and Suncity were linked to overseas organised crime syndicates: see particulars to paragraph 569.a above. Material reviewed by SCA senior management on several occasions between July 2019 and October 2021 included adverse media reports identifying Customer 1's alleged links to overseas organised crime syndicates: see particulars to paragraphs 569.n, 569.o and 577.a above.

Monitoring of Customer 1 as a foreign PEP

578. At all times from 7 December 2016, Customer 1 was a foreign PEP: see *Customer 1's risk profile* above.

579. At all times, SCA was required to:

a. undertake detailed analysis of Customer 1's KYC information including taking reasonable measures to identify the source of Customer 1's wealth and the source of Customer 1's funds; and

b. seek senior management approval to continue a business relationship with Customer 1 and whether SCA should continue to provide designated services to Customer 1.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.10(2), 15.10(6) and 15.11 of the Rules.

580. At no time did SCA identify that Customer 1 was a foreign PEP. SCA therefore failed to monitor Customer 1 as a foreign PEP.

Particulars

See paragraph 577.b above.

It was not until August 2019 that SCA senior management considered its business relationship with Customer 1. The consideration did not have appropriate regard to the higher ML/TF risks posed by Customer 1 because senior management was not aware that Customer 1 was a foreign PEP.

If Customer 1 had been appropriately identified as a foreign PEP, the 2017-2021 Standard Part A Programs required:

a. that Customer 1 be automatically accorded a significant risk rating; and

b. that Customer 1 then be referred to the SCA General Manager, to determine whether it was appropriate to continue SCA's business relationship with Customer 1. The SCA

General Manager would liaise with the SCEG General Counsel before making such a decision.

Contravention of s 36 of the Act in respect of Customer 1

581. By reason of the matters pleaded at paragraphs 566 to 580 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 1 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

582. By reason of the matters pleaded at paragraph 581, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 22 March 2022 with respect to Customer 1.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 2

583. Customer 2 was a customer of SCA during the relevant period. Between 7 December 2016 and 9 August 2021, SCA recorded turnover exceeding $420,000,000 for Customer 2's individual rated gambling activity and junkets operated by Customer 2.

Particulars

Customer 2 was a customer of SCA from at least 3 July 2015.

On 9 August 2021, SCA issued a ban in respect of Customer 2 at the direction of the AML team.

On 24 March 2022, SCA issued another ban in respect of Customer 2.

584. SCA provided Customer 2 with designated services within the meaning of table 1 and table 3, s 6 of the Act during the relevant period including services connected to Customer 2's role as a junket operator, and as an individual commission player and junket player, facilitated through one junket operator, Customer 1.

Particulars

Prior to 7 December 2016, SCA opened an FMA for Customer 2 which remained open as at 28 October 2022 (item 11, table 3, s 6 of the Act).

While a customer of SCA, Customer 2 remitted funds to and from their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 2's risk profile* below.

585. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 2.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 2's risk profile

586. On and from 7 December 2016, Customer 2, and the provision of designated services to Customer 2 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 2's risk profile prior to the relevant period

a. by 7 December 2016, Customer 2 had the following risk history:

i. SCA had formed suspicions for the purposes of s 41 of the Act with respect to Customer 2;

Particulars

SCA gave the AUSTRAC CEO an SMR on 7 August 2016.

The SMR reported that on 5 August 2016, Customer 2 cashed out $5,000 at one Cashier and then immediately went to another Cashier and cashed out a further $5,000. SCA noted that Customer 2 was trying to avoid the threshold transaction amount: SMR dated 7 August 2016.

ii. Customer 2 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs or individual commission programs;

Particulars

In the 2016 financial year, Customer 2's recorded individual rated gambling activity for non-commission play at SCA was estimated as a buy-in of $1,068,750, turnover of $92,077,484 with wins of $987,700.

iii. Customer 2 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA from play on individual commission programs, and a commission of $822,134 was recorded as payable by SCA to Customer 2 on individual commission programs;

Particulars

Between 1 September 2015 and 3 August 2016, Customer 2 played on two individual commission programs at SCA.

In the 2016 financial year, Customer 2's recorded gambling activity on individual commission programs at SCA was estimated as a buy-in of $2,338,457, turnover of $137,022,300 with losses of $3,187,920. A commission of $822,134 was payable by SCA to Customer 2 from play on individual commission programs.

iv. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 2 by remitting large amounts of money into and within the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

SCA made money available to Customer 2 in the following transactions:

a. on or around 9 November 2015, Customer 2 engaged the services of Company 1, an Australian third party remittance company, to transfer $190,000 to SCA's bank account on their behalf; and

b. on or around 16 October 2015, Customer 2 engaged the services of another third party remittance company, to transfer $212,368 to SCA's bank account on their behalf.

Remittances within the casino environment

On or around 13 August 2016, Customer 2 received $50,000 into their SCA FMA from Person 3's SCA FMA. SCA made these funds available to Person 3.

v. SCA was aware that Customer 2 had engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

Particulars

On 29 May 2016, SCA recorded several chips exchanges between Customer 2 and Customer 17 over a 35-minute period.

Between July 2016 and October 2016, Customer 2 was mentioned in an internal report titled 'AML Unusual Changes in Betting' on three occasions.

vi. Customer 2 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 20 December 2013 and 7 November 2016, SCA gave the AUSTRAC CEO 246 TTRs detailing transactions made by Customer 2 totalling $8,102,259 which comprised:

a. 95 TTRs totalling $3,772,776 in account deposits;

b. six TTRs totalling $1,670,000 in account withdrawals;

c. 142 TTRs totalling $4,121,110 in chip and cash exchanges; and

d. three TTRs totalling $41,373 in foreign currency exchanges.

vii. SCA was aware that Customer 2 frequently engaged in large buy-ins and cash outs, including with cash, CVIs and cheques;

Particulars

Cash and chips

SCA frequently recorded that Customer 2 made significant buy-ins or cash outs at SCA. For example:

a. on 18 July 2015, Customer 2 made a cash buy-in for $10,000. A couple of hours later, Customer 2 cashed out $22,800 in chips for cash. Later that evening, Customer 2 exchanged $12,000 in chips for cash;

b. on 19 August 2015, Customer 2 made a cash buy-in for $170,000 and received a CPV. Later that day, Customer 2 cashed out $200,000. Customer 2 then made a cash buy-in with $180,000 in cash and received a CPV;

c. on 3 November 2015, Customer 2 made a cash buy-in with $30,000 and received a CPV. A few hours later, Customer 2 deposited $80,000 in cash chips into their FMA. Five minutes later, Customer 2 exchanged $56,500 in chips for cash; and

d. on 27 September 2016, Customer 2 cashed out $15,000 in CCF chips for cash. Later that day, Customer 2 cashed out $4,700. A few hours later, Customer 2 cashed out $30,700 in chips for cash. Customer 2 then deposited $30,000 in cash into their account and received a CPV. Customer 2 made a buy-in with the CPV.

viii. Customer 2 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including structuring; and

Particulars

See paragraph 24 above.

See particulars to paragraph 586.a.i above.

ix. Customer 2 had access to private gaming rooms at SCA;

Particulars

See paragraph 145(e) above.

Customer 2 had access to the Grange Room, which was a private gaming room at SCA.

Customer 2's risk profile during the relevant period

b. Customer 2 was a junket operator who facilitated the provision of high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA;

i. between 28 September 2017 and 20 October 2017, Customer 2 operated two junkets at SCA, one of which was partly funded by another customer;

Particulars

Customer 2 jointly funded the junket they operated at SCA between 15 October 2017 and 20 October 2017 with another SCA customer.

ii. between 28 September 2017 and 20 October 2017, SCA recorded that the total cumulative turnover of junkets operated by Customer 2 in the relevant period was $11,629,646 with losses of at least $1,566,335;

Particulars

See paragraphs 399 to 401 above.

In 2017, SCA recorded that junkets operated by Customer 2 had turnover of $11,629,646 with losses of at least $1,566,335.

iii. between 28 September 2017 and 20 October 2017, total benefits of at least $82,000 were payable to Customer 2 by SCA in their capacity as a junket operator;

Particulars

In 2017, total benefits of at least $82,000 were payable to Customer 2 in their capacity as a junket operator which included a commission on junket turnover.

iv. Customer 2 operated junkets in private gaming rooms; and

Particulars

See paragraph 145(e) above.

Customer 2 operated junkets in private gaming rooms, including Suite 88.

v. Customer 2 facilitated the provision of high value designated services to eight junket players at SCA, including foreign PEPs;

Particulars

See paragraphs 388 and 389 above.

On 23 June 2017, SCA identified that the main player on one of Customer 2's junkets was a foreign PEP.

c. Customer 2 was a junket player who received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA through junket programs;

i. between 28 September 2017 and 16 October 2018, Customer 2 was a player on four junkets at SCA, two of which were operated and funded by Customer 1 and two of which Customer 2 operated and funded themselves;

ii. at no time did SCA record Customer 2's individual gambling activity on the two junket programs that Customer 1 operated and Customer 2 attended only as a junket player; and

iii. SCA recorded all of the turnover for the junkets operated by Customer 2 (including those on which they also played) against Customer 2's account, including the individual gambling activity of the other junket players;

d. designated services provided to Customer 2 lacked transparency as the services were provided through the channel of junket programs at SCA;

Particulars

See paragraph 392 above.

e. Customer 2 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs or individual commission programs. Between the 2017 and 2022 financial years, SCA recorded escalating turnover of $32,415,753 for Customer 2, with cumulative losses of at least $1,053,297 on non-commission programs;

Particulars

Between the 2017 and 2020 financial years, Customer 2 recorded individual rated gambling activity for non-commission play at SCA on one SCA FMA number. For the 2021 and 2022 financial years, Customer 2 recorded rated gambling activity for non-commission play at SCA on a different SCA FMA number.

In the 2017 financial year, Customer 2's recorded individual rated gambling activity for non-commission play at SCA was an estimated buy-in of $1,328,800, turnover of $1,005,023 with wins of $46,900.

In the 2018 financial year, Customer 2's individual rated gambling activity for non-commission play at SCA was an estimated buy-in of $682,575, turnover of $3,996,208 with losses of $77,400.

In the 2019 financial year, Customer 2's individual rated gambling activity for non-commission play at SCA was an estimated buy-in of $646,000, turnover of $16,318,719 with losses of $874,097.

In the 2020 financial year, despite closures related to the COVID-19 pandemic, Customer 2's individual rated gambling activity for non-commission play at SCA was an estimated buy-in of $99,500, turnover of $11,094,369 with losses of $148,700.

In the 2021 and 2022 financial years, Customer 2's individual rated gambling activity for non-commission play at SCA was an estimated turnover of $1,434.

f. Customer 2 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA from play on individual commission programs, and a commission of $2,351,775 was recorded as payable by SCA to Customer 2 on individual commission programs;

Particulars

Between 13 August 2016 and 11 March 2021, Customer 2 played on 30 individual commission programs at SCA.

In the 2017 financial year, Customer 2's recorded gambling activity on individual commission programs at SCA was estimated as a buy-in of $1,909,158, turnover of $44,220,100 with losses of $60,050. A commission of $265,321 was payable by SCA to Customer 2 from play on individual commission programs.

In the 2018 financial year, Customer 2's recorded gambling activity on individual commission programs at SCA escalated to an estimated buy-in of $5,171,725, turnover of $121,216,362 with losses of $2,498,900. A commission of $676,940 was payable by SCA to Customer 2 from play on individual commission programs.

In the 2019 financial year, Customer 2's recorded gambling activity on individual commission programs at SCA was estimated as a buy-in of $4,019,693, turnover of $172,503,183 with wins of $8,155. A commission of $949,559 was payable by SCA to Customer 2 from play on individual commission programs.

In the 2020 financial year, despite closures related to the COVID-19 pandemic, Customer 2's recorded gambling activity on individual commission programs at SCA was estimated as a buy-in of $2,226,360, turnover of $82,727,730 with losses of $1,471,555. A commission of $455,382 was payable by SCA to Customer 2 from play on individual commission programs.

In the 2021 financial year, Customer 2's recorded gambling activity on individual commission programs at SCA was estimated as a buy-in of $168,400, turnover of $997,132 with wins of $158,000. A commission of $4,574 was payable by SCA to Customer 2 from play on individual commission programs.

g. Customer 2 received additional benefits from SCA in their capacity as an individual commission player;

Particulars

Customer 2 also received other benefits in their capacity as an individual commission program player, including non-gaming complimentary services. For example:

a. during their individual commission program which ran between 23 January 2019 and 6 February 2019, Customer 2 received benefits of $7,081 in complimentary value services; and

b. during their individual commission program which ran between 11 August 2019 and 10 September 2019, Customer 2 received benefits of $9,004 in complimentary value services and complimentary deductions on food and beverage.

h. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 2 by remitting large amounts of money into, out of and within the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCEG customer account channel

SCA made money available to Customer 2 in the following transactions.

On 10 September 2019, a third party company overseas transferred $300,000 on behalf of Customer 2 to one of SCEG's bank accounts, Horizon Tourism. A SCEG New Zealand casino then transferred the funds to Customer 2's SCA FMA.

On 20 September 2019, $235,000 was deposited into an account held by SGEG in Australia on behalf of Customer 2, which SCA made available to Customer 2 and which was deposited into Customer 2's FMA.

Remittances through the SCA customer account channel

In an internal report dated August 2020, Bank 1 identified Customer 2 as a top direct third party depositor into SCA's bank account during the period 1 September 2018 to 31 August 2019.

SCA made money available to Customer 2 in the following transactions:

a. on 4 February 2017, Customer 2 transferred $12,000 from their bank account to their SCA FMA;

b. between 22 February 2017 and 27 November 2017, Customer 2's mining company, Company 2, transferred a total of $1,630,100 to Customer 2's SCA FMA over 15 transactions;

c. on 10 May 2017, Customer 2 transferred $8,000 from their bank account to their SCA FMA;

d. on 8 October 2017, after settling a program at another SCEG casino, Customer 2 transferred $95,697 to their SCA FMA;

e. on 4 December 2018, Company 1 transferred $174,757 to Customer 2's SCA FMA. The funds were for Customer 2 to use as buy-in for gaming purposes;

f. on 14 December 2018, Company 1 transferred $205,882 to Customer 2's SCA FMA;

g. on 15 April 2019, Company 1 transferred $662,601 to Customer 2's SCA FMA: SMR dated 18 April 2019;

h. on 1 August 2019, Customer 2 transferred $80,000 to their SCA FMA; and

i. between 18 January 2020 and 28 January 2020, Customer 2 transferred a total of $350,000 to their SCA FMA over four transactions.

SCA accepted instructions to transfer funds from Customer 2's accounts for the following transactions.

a. On 3 October 2017, Customer 2 transferred $50,000 from their SCA FMA to another SCEG casino.

b. On 9 October 2017, SCA transferred $180,000 to Customer 2's company's bank account, following the settlement of Customer 2's individual commission program.

c. On 4 April 2018, SCA transferred $150,000 to Customer 2's bank account.

d. On 6 January 2020, SCA transferred $20,000 to Customer 2's bank account.

e. On 13 January 2020, SCA transferred $80,000 to Customer 2's bank account.

Remittances through the SkyCity New Zealand channel

On 10 September 2019, SCA credited $300,000 to Customer 2's FMA with these funds originating from Customer 2's FMA held at a SCEG New Zealand casino. SCA made the funds available to Customer 2.

Remittances from SCA FMAs to SCEG New Zealand FMAs

Between 29 December 2018 and 1 January 2019, a SCEG New Zealand casino credited $280,000 to Customer 2's FMA with funds originating from Customer 2's FMA held at SCA on the following occasions:

a. on 29 December 2018, SCA transferred $130,000 from Customer 2's FMA held at SCA to Customer 2's FMA held at a SCEG New Zealand casino;

b. on 31 December 2018, SCA transferred $100,000 from Customer 2's FMA held at SCA to Customer 2's FMA held at a SCEG New Zealand casino; and

c. on 1 January 2019, SCA transferred $50,000 from Customer 2's FMA held at SCA to Customer 2's FMA held at a SCEG New Zealand casino.

Remittances within the casino environment

SCA made money available to Customer 2 in the following transactions:

a. on 19 August 2018, Customer 2 received $50,000 into their SCA FMA from another customer's SCA FMA;

b. on 30 December 2018, Customer 2 received $100,000 into their SCA FMA from another customer's SCA FMA; and

c. between 9 March 2019 and 11 August 2019, Customer 2 received $1,075,000 into their SCA FMA over 11 transactions from another customer, Person 4's SCA FMA.

SCA accepted instructions to transfer funds from Customer 2's accounts for the following transactions.

a. On 5 August 2017, Customer 2 transferred $50,000 from their SCA FMA to another customer's SCA FMA.

b. On 23 October 2017, Customer 2 transferred $150,000 from their SCA FMA to their spouse's bank account.

c. On 31 May 2018, Customer 2 transferred $80,000 from their SCA FMA to their spouse's SCA FMA. On 3 June 2018, Customer 2 again transferred $80,000 from their SCA FMA to their spouse's SCA FMA.

d. On 25 April 2019, Customer 2 transferred $380,000 from their SCA FMA to Person 4's SCA FMA. SCA noted that Person 4 was not on site and the SCA host could not confirm any reasoning for this transfer, other than that Customer 2 had requested it. SCA completed the transfer.

e. Between 4 May 2019 and 22 June 2019, Customer 2 transferred a further $450,000 from their SCA FMA over four transactions to Person 4's SCA FMA.

f. Between 31 July 2019 and 29 January 2020, Customer 2 received $320,000 into their SCA FMA over four transactions from Customer 17's SCA FMA.

i. from at least 21 April 2017, SCA was aware that Customer 2 was associated with a number of customers – including Customer 17, Customer 21, Customer 27, Customer 31, Customer 39, Customer 31's spouse, Person 7, and their child, Person 21, and other customers in respect of whom SCA had formed suspicions, such as Person 2, Person 4, Person 5 and Person 6 – who conducted transactions involving the receipt and movement of significant amounts of cash with no apparent economic or visible purpose and were related to loan sharking activities;

i. the provision of designated services by SCA to Customer 2 and their associates raised red flags reflective of higher ML/TF risks;

Particulars

Red flags reflective of higher ML/TF risks included:

a. exchanging cash for chips on multiple gaming Cashiers, tables or Cages in several transactions: SMR dated 18 June 2018;

b. conducting separate cash and chip transactions below the reporting threshold in quick succession: SMR dated 18 June 2018;

c. using runners to conduct threshold transactions: SMR dated 23 May 2018, 6 March 2019; 15 March 2021;

d. handing chips or cash to one another: SMRs dated 21 April 2017, 24 May 2017, 9 April 2018, 23 May 2018, 13 June 2018, 18 June 2018, 10 July 2018, 11 January 2019, 7 February 2019, 19 February 2019, 15 May 2019, 13 June 2019;

e. handing unknown items to one another: SMRs dated 21 April 2017, 18 June 2018;

f. placing cash and chips into items such as envelopes, handbags, satchels, plastic bags, reusable bags, and wrapped jackets and bundles, or instructing SCA employees to do the same: SMRs dated 21 April 2017, 9 April 2018, 23 May 2018, 13 June 2018, 18 June 2018, 10 July 2018, 11 January 2019, 7 February 2019, 19 February 2019, 15 May 2019, 15 August 2019 and 8 November 2019;

g. covertly exchanging cash or chips between each other, including by passing them under tables, leaving them in open spaces and then signalling each other, and hiding them behind cushions on the couches within private gaming rooms: SMRs dated 13 June 2018, 18 June 2018, 11 January 2019, 6 March 2019, 15 May 2019, 25 October 2019; 15 March 2021

h. concealing cash and chips in their pockets and beneath their jackets: SMRs dated 21 April 2017, 9 April 2018, 18 June 2018, 18 April 2019, 15 May 2019, 15 August 2019 and 8 November 2019;

i. making and receiving phone calls at identical times and then conducting cash and chip exchanges shortly thereafter: SMRs dated 18 June 2018, 18 April 2019, 15 May 2019, 15 August 2019 and 8 November 2019;

j. carrying significant amounts of cash and chips into the SCA toilets away from the view of surveillance cameras, and sometimes swapping the cash between different carrying items inside the toilets: SMRs dated 2 May 2017, 13 June 2018, 18 June 2018, 10 July 2018, 11 January 2019, 7 February 2019, 15 May 2019, 13 June 2019, 15 August 2019, 18 September 2019, 3 October 2019 and 8 November 2019;

k. conducting significant cash and chip exchanges in the SCA toilets: SMRs dated 18 June 2018, 10 July 2018, 7 February 2019, 18 April 2019, 15 May 2019, 15 August 2019, 18 September 2019, 3 October 2019 and 8 November 2019;

l. depositing significant amounts of cash in the SCA toilets: SMR dated 7 February 2019;

m. using their bodies to hide chip and cash exchanges from the view of surveillance cameras: SMR dated 18 June 2018;

n. using EFTPOS facilities to conduct significant numbers of cash transactions in quick succession: SMR dated 25 May 2018;

o. withdrawing large amounts of cash from FMAs: SMRs dated 10 July 2018 and 11 January 2019, 19 February 2019, 25 October 2019;

p. depositing large amounts of chips into each other's FMAs: SMRs dated 21 April 2017 and 9 April 2018; and

q. removing significant amounts of chips from SCA: SMR dated 18 April 2019.

ii. SCA formed suspicions in respect of these customers; and

Particulars

SCA considered it suspicious that the customers, including Customer 2:

a. conducted transactions that were not supported by gambling activity: SMRs dated 13 June 2018, 18 June 2018, 11 January 2019, 18 April 2019, 18 September 2019, 3 October 2019 and 8 November 2019;

b. carried a significant quantity of chips for the purpose of lending or loaning funds to players like Customer 2 who gamed at significant levels: SMR dated 6 March 2019, 18 September 2019;

c. conducted transactions indicative of ML/TF typologies and vulnerabilities, including structuring, cashing-in large value chips with no evidence of play and loan sharking: SMRs dated 21 April 2017, 23 May 2018, 18 June 2018, 10 July 2018, 19 February 2019, 6 March 2019, 13 June 2019, 15 August 2019, 18 September 2019, 3 October 2019, 25 October 2019 and 8 November 2019;

d. conducted transactions that had no identifiable purpose and where the original source of funds was not clear: SMRs dated 24 May 2017, 9 April 2018, 13 June 2018, 18 June 2018 and 18 April 2019;

e. conducted transactions that did not appear to be gaming related and it appeared that a factor other than gaming was the driving factor between their exchanges: SMRs dated 18 June 2018, 18 April 2019 and 15 May 2019;

f. conducted transactions in a secretive manner that was designed to conceal and disguise their associations, and distance themselves and their motives from the transactions, by using agents and family members, initiating transactions through phone calls, and by conducting transactions with minimal contact and in settings such as the SCA toilets or other places away from SCA employees and gaming tables: SMRs dated 21 April 2017, 2 May 2017, 18 June 2018, 11 January 2019, 19 February 2019, 6 March 2019, 18 April 2019, 15 May 2019, 25 October 2019, 8 November 2019 and 15 March 2021;

g. there were no known connections or associations between some of the customers, including between Customer 31 and

Customer 2, and customers with whom they conducted transactions: SMR dated 18 June 2018;

h. appeared to be engaged in money lending between themselves, and with other customers, but sometimes did not receive repayments: SMRs dated 21 April 2017, 23 May 2018, 25 May 2018, 13 June 2018, 18 June 2018, 19 February 2019, 6 March 2019, 15 May 2019, 25 October 2019;

i. Customer 31 and their spouse Person 7 were the primary "points of call" for the customers at SCA, including Customer 2 and Customer 27, who had previously engaged in behaviour indicative of money laundering and which SCA had reported to the AUSTRAC CEO: SMR dated 15 May 2019; and

j. were exchanging, or conducting buy-ins with, large amounts of cash chips while they were on commission programs: SMRs dated 2 May 2017, 24 May 2017, 23 May 2018.

iii. Customer 2 and their associates engaged in a series of large cash, chip and other exchange transactions with no visible lawful purpose;

Particulars

Cash to chip transactions

Between 9 June 2018 and 13 June 2018, Customer 2 engaged in two cash to chip exchange transactions with SCA totalling $80,000.

On 13 June 2018, SCA identified that Customer 2's associates engaged in a cash to chip exchange transaction with SCA totalling $10,000.

Chip to cash transactions

Between 18 May 2018 and 9 June 2019, Customer 2 engaged in three chip to cash exchange transactions with SCA totalling $189,925.

Between 23 May 2017 and 13 June 2018, SCA identified that Customer 2's associates engaged in three chip to cash exchange transactions with SCA totalling $41,450.

Cash handovers

Between 19 April 2017 and 9 June 2019, SCA identified that Customer 2 appeared to engage in at least 14 cash handovers with other customers totalling at least $747,000.

Between 13 June 2018 and 7 November 2019, SCA identified that Customer 2's associates appeared to engage in at least 15 cash handovers with other customers totalling at least $1,231,000.

Chip handovers

Between 19 April 2017 and 23 October 2019, SCA identified that Customer 2 appeared to engage in at least seven chip handovers with other customers totalling at least $431,000.

Between 19 April 2017 and 1 October 2019, SCA identified that Customer 2's associates appeared to engage in at least five chip handovers with other customers totalling $620,000.

Cash withdrawals

Between 9 January 2019 and 7 November 2019, SCA identified that Customer 2 engaged in at least six cash withdrawals from their FMA totalling $728,000.

Other transactions

On 16 April 2019, SCA identified that Customer 2 engaged in two chip purchases with chip purchase vouchers, totalling $325,000.

On 4 March 2019, SCA identified that Customer 2 appeared to use a runner to conduct transactions on their behalf.

On 13 June 2018, SCA identified that Customer 2's associates engaged in five TITO ticket redemptions totalling $10,000.

Between 19 April 2017 and 29 June 2018, Customer 2 and their associates appeared to hand unknown items between themselves on at least two occasions.

j. Customer 2 was engaged in a series of other large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

Particulars

Between January 2017 and January 2020, Customer 2 was mentioned in an internal report titled 'AML Unusual Changes in Betting' on 26 occasions.

Large and unusual transactions in 2017

On 2 January 2017, Customer 24 presented $36,500 in chips at the Grange Room Cashier. Customer 24 advised that the chips belonged to Customer 2 and requested that they be deposited into Customer 2's account. Following a discussion with a VIP Host at the Cashier, Customer 24 retained $11,500 of the chips and exchanged $25,000 in chips for cash before departing with the VIP Host. Customer 24 then gave the cash to Customer 2. Shortly afterwards, Customer 2 reclaimed the commission chips from Customer 24 and exchanged them for cash.

On 7 January 2017, an SCA customer made a buy-in with $10,000 in cash and received CCF chips. SCA recorded that the customer conducted this transaction on behalf of Customer 2.

On 13 January 2017, Customer 17 and Customer 2 approached the Grange Cage together with chips totalling $50,000. Customer 2 claimed that the chips were theirs. SCA approved a cash out of $25,000. A short time afterwards, Customer 17 approached the Grange Cage with chips totalling $25,000 to cash out. When staff asked whether the chips were Customer 2's, Customer 17 claimed they were theirs. However, staff noted that Customer 17 settled their own program about 30 minutes before with a final payout of $609. Despite suspecting that the chips belonged to Customer 2, SCA processed the transaction against Customer 17's account.

On 3 February 2017, Customer 2 cashed out $10,000 at SCA. Two minutes later, Customer 2 handed the cash to another SCA customer. The other customer then made a buy-in with the cash. SCA considered that Customer 2 was providing the other customer with a short-term loan.

On 5 August 2017, Customer 2 informed SCA that they wanted to transfer funds to another customer. Customer 2 was playing on an individual commission program at the time, and was told that the transfer would take them below the front money minimum for the program. Shortly after, Customer 2 asked to settle their program as they said it was restrictive. Following the settlement, Customer 2 transferred $50,000 from their SCA FMA to the other customer's SCA FMA. The other customer used the funds to buy-in to an individual commission program.

On 9 October 2017, Customer 2 attended SCA with $30,000 in cash and requested a CPV for another SCA customer. Customer 2 informed SCA staff that the cash belonged to the other customer, so SCA completed the transaction. On 10 October 2017, Customer 2 cashed out $18,850 at SCA and then attended a gaming table and passed an unknown amount of money to another SCA customer. SCA noted that Customer 2 frequently handed out money to friends and associates, without receiving funds back.

On 17 October 2017, Customer 2 made a buy-in at a gaming table with $7,700 in cash and received cash chips. After losing their initial buy-in, Customer 2 left the gaming table and walked over to Person 3. The other SCA customer handed Customer 2 what appeared to be three $5,000 non-negotiable chips and one $5,000 commission chip. Customer 2 then commenced play at another gaming table using the non-negotiable chips. Five minutes later, the other customer approached the table where Customer 2 was playing. Customer 2 passed the customer two $5,000 non-negotiable chips and two $5,000 commission chips. The customer gave them straight back to Customer 2, and then Customer 2 gave the customer three $5,000 non-negotiable chips and one $5,000 commission chip instead.

Large and unusual transactions in 2018

On 8 February 2018, Customer 2 received a $100,000 non-negotiable plaque from Customer 11 at SCA. Customer 2 then exchanged the plaque for ones of a different value. SCA noted that Customer 2 had been losing that gaming day while Customer 11 had been winning, and it was not uncommon for players to share their luck with each other.

On or around 9 February 2018, Customer 2 engaged the services of Company 1 to transfer $200,000 to SCA's bank account. Once SCA received the funds, SCA deposited them into Customer 11's SCA FMA in circumstances where the connection between Customer 2 and Customer 11 regarding the funds was not clear.

On 20 February 2018, an SCA Gaming Operations Shift Manager reported that Customer 17 had again been handing non-negotiable chips to Customer 2, which was in breach of their NNEG individual program agreements. The shift manager stated that any further instances would result in SCA ceasing their gaming, and that Customer 2 had been informed of this.

On 24 February 2018, Customer 17 removed $30,000 in non-negotiable chips from a gaming table and passed them to Customer 2 under the table. Customer 2 then gambled with the chips.

On 27 February 2018, Customer 17 made a buy-in for a $50,000 CPV at SCA. Immediately after the transaction was completed, Customer 17 handed the chips to Customer 2. Customer 2 then gambled with the chips.

On 13 March 2018, SCA staff observed Customer 27 passing approximately $50,000 in $5,000 cash chips to Customer 2. This was in breach of Customer 2's individual commission program conditions. Customer 2 later passed the chips to Customer 15. Customer 15 then met with Customer 11, who passed Customer 15 $50,000 in CCF chips in exchange for the cash chips. Customer 15 then cashed out the CCF chips out on behalf of Customer 11.

On or around 20 March 2018, Customer 2 engaged the services of Company 1 to transfer $300,000 to SCA's bank account. Once SCA received the funds, SCA deposited them into Customer 11's SCA FMA in circumstances where the connection between Customer 2 and Customer 11 regarding the funds was not clear to SCA.

On 26 April 2018, Customer 11 cashed out $50,000 at SCA. SCA suspected that the cash may have been intended for, or passed to, Customer 2.

On 24 May 2018, SCA's CCTV cameras captured Customer 2 giving $100,000 in cash to Customer 27 on the Grange balcony. On the same day, Customer 2 cashed out $210,000 in $100 notes. Twenty minutes later, Person 5 asked SCA for a bag or envelope for their cash. The customer had $50,000 in $100 notes, rubber banded in the

same manner as Customer 2's cash. SCA suspected that cash may have changed hands between Customer 2 and Person 5.

On 31 May 2018, Customer 2 asked SCA staff to issue them a blank cheque for $80,000. SCA staff informed Customer 2 that this was not possible. Shortly after, Customer 2 requested that $80,000 be transferred from their FMA to their spouse's FMA. Once the transfer was completed, Customer 2's spouse asked for a $80,000 cheque to be issued in their name. SCA noted that the spouse did not game with the funds. On 3 June 2018, Customer 2 again transferred $80,000 to their spouse's SCA FMA. The spouse again did not game with the funds, and requested that a cheque for $80,000 be issued in their name. SCA noted that Customer 2's spouse was an infrequent visitor to SCA and had no recorded gaming. Given SCA knew that Customer 2's spouse had no intention of gaming with the funds, it considered the two funds transfers to be suspicious: SMR dated 4 June 2018.

On 15 July 2018, Customer 2 withdrew $50,000 in cash and a $10,000 CPV from their FMA. A VIP Host collected the cash on Customer 2's behalf, placed it in a large envelope and delivered it to Customer 2 at a gaming table. Customer 2 then hid the envelope under the table and passed it to Person 5, who was sitting next to them. Shortly after, Person 5 took the envelope to the Grange Cage and deposited the $50,000 in cash into their account. Person 5 then withdrew the funds as a CPV. Person 5 cashed in the CPV at a gaming table, received cash chips and commenced playing. SCA noted that during this gaming period, Customer 2 experienced significant wins while Person 5 experienced significant losses. SCA suspected that Customer 2 had lent Person 5 money.

On 18 July 2018, an SCA customer bought in with a $20,000 CPV at a gaming table and received chips. Shortly after, the customer handed Customer 2 those chips and a $5,000 CCF chip under the table. Customer 2 used the chips to play. SCA noted that both Customer 2 and the other player were known for lending funds to associates.

On 2 October 2018, Customer 2 and Customer 27 approached an SCA Cashier with $80,000 in cash chips. Customer 27 asked for the chips to be exchanged for non-negotiable chips, as Customer 2 was playing on a program. SCA recorded that it was obvious that Customer 27 was lending money to Customer 2.

On 17 November 2018, Customer 2 took what appeared to be three bundles of $10,000 in $100 notes from their bag and handed them to Person 3. That customer then handed $10,000 to a second customer, who used the funds to buy-in at a gaming table. SCA noted that the two customers were both known associates of Customer 2.

On 14 December 2018, Company 1 transferred $205,882 to Customer 2's SCA FMA. On 15 December 2018, Customer 2 attended SCA and withdrew $50,000 from their account for gaming purposes. An hour later, after winning approximately $50,000, Customer 2 returned to the Cage and deposited $85,500 back into their account. Customer 2 then withdrew $150,000 in cash and left the premises. SCA noted that Customer 2 stated on the receipt that the purpose of the transfer was for business investments. SCA therefore suspected that the transfer was not entirely for gaming-related purposes. SCA also noted that Customer 2 had experienced a significant win of $50,000 in the days prior to the telegraphic transfer on 14 December 2018. SCA considered it suspicious that Customer 2 transferred $205,882 for the purposes of gaming when they only utilised $50,000 of it, particularly where they were already in possession of $50,000 in winnings from the previous days. SCA noted that Customer 2 was the owner of Company 2, which exported iron ore primarily to foreign buyers. Customer 2 had significant assets in that country and had previously had difficulties accessing those assets due to restrictions in place in that country: SMR dated 18 December 2018.

On 30 December 2018, Customer 2 received $100,000 into their FMA from another customer's FMA. An SCA AML Adviser noted that the customer had never gamed at the casino and questioned why the customer was making this transfer. An SCA International Business Service Executive informed the AML Adviser that the customer was Customer 2's assistant and they had deposited the funds purely for the purpose of sending them to Customer 2 at a SCEG New Zealand casino. Customer 2 then transferred the $100,000 on 31 December 2018 from their SCA FMA to their account at the SCEG casino in New Zealand: see the particulars to paragraph 586.h above.

Large and unusual transactions in 2019

On 10 September 2019, Customer 2 received $300,000 into their SCA FMA via the SCEG Customer account channel: see particulars to paragraph 586.h above. The funds were deposited by an Australian mining company. Customer 2 informed SCA that their bank had previously closed their accounts following similar transactions to SCA's bank account. SCA conducted open source searches, which indicated that there was a link between the third party company and the company Customer 2 owned (Company 2). SCA noted that this link provided some comfort, but nonetheless considered it suspicious that Customer 2 was using a business account for recreational purposes: SMR dated 23 September 2019.

k. Customer 2 received a number of suspicious telegraphic transfers to their SCA FMA;

Particulars

2017

On or around 11 December 2017, Customer 2 engaged the services of Company 1 (an Australian remittance company) to transfer $69,500 to their SCA FMA. The funds were transferred to SCA's bank account on behalf of Customer 2 by another Australian third party company account, Company 3.

On 18 December 2017, Customer 2 engaged the services of Company 1 to transfer $193,050 to their SCA FMA. The funds were transferred to SCA's bank account on behalf of Customer 2 by another third party company account.

2018

On 5 March 2018, an unknown account transferred $100,000 to SCA's bank account on behalf of Customer 2. Customer 2 provided a receipt to SCA that had the sender's name blurred out. On 6 March 2018, a third party company account transferred $50,000 to SCA's bank account on behalf of Customer 2. SCA suspected that the transfer on 5 March 2018 was from the same third party, but was unable to confirm this. SCA considered it concerning that these transfers placed SCA in the middle of a transaction between two parties whose connection was unknown to SCA: SMR dated 8 March 2018.

On 19 October 2018, Company 3 transferred $374,824 on behalf of Customer 2 to SCA's bank account. SCA understood that Customer 2 had engaged Company 1, a remittance company, to make the deposit on their behalf. SCA noted that Customer 2 had previously used Company 1 and the funds in the other transaction were also deposited by a different third party company, Company 4. SCA considered it suspicious that Company 1 used multiple third party companies to make large foreign exchange transactions, in circumstances where it could not find any link between Company 1 and the third party companies who deposited the funds: SMR dated 24 October 2018. SCA ultimately released the funds to Customer 2's SCA FMA.

On or around 31 October 2018, Customer 2 engaged the services of Company 1 to transfer $295,857 to their SCA FMA. The funds were transferred to SCA's bank account on behalf of Customer 2 by another Australian third party company account, Company 3.

2019

On or around 27 February 2019, Customer 2 engaged the services of Company 1 to transfer $100,401 to their SCA FMA. The funds were transferred to SCA's bank account on behalf of Customer 2 by another third party company account. However, on 1 March 2019 SCA returned the funds to the sender, due to insufficient evidence

linking the transaction to Customer 2. On the same day, Customer 2 transferred $100,401 to their SCA FMA in a separate transaction.

On 20 September 2019, Customer 2 received $235,000 into their SCA FMA via the SCEG Customer Account channel. On 21 September 2019, Customer 2 attended SCA and was issued a $235,000 CPV. Customer 2 used the CPV at a gaming table and received $235,000 in cash chips. Customer 2 handed $35,000 in chips to Customer 27, and kept the remaining amount in their jacket pocket. Customer 2 then left the premises. SCA considered the transfer to be suspicious, and suspected that Customer 2 was utilising SCA's banking facilities for purposes other than gaming. SCA noted that there had been an increasing number of incidents involving Customer 2 with transactions that did not have a clear gaming purpose. SCA noted Customer 2's involvement in cash and chip exchanges with suspected loan sharks and their recent use of a company account for recreational purposes raised red flags: SMR dated 26 September 2019.

Unless otherwise specified, each of the above transactions took place via the SCA customer accounts channel.

l. Customer 2 was connected to other customers at SCA, including foreign PEPs, players who posed higher ML/TF risks such as Customer 1, Customer 17, Customer 21, Customer 24, Customer 27, Customer 31 and Customer 39, and players who SCA considered had acted suspiciously;

Particulars

See particulars to paragraphs 586.c, and 586.h to 586.j, above.

On 23 January 2017, SCA noted that Customer 24 had recently begun acting as a runner for Customer 2 and Customer 17. SCA recorded that Customer 24 had conducted a number of cash buy-ins on 19 and 20 January 2017 for $9,900, and considered that Customer 24 was structuring transactions to avoid reporting obligations. SCA also recorded that Customer 2 and Customer 17 were close associates with suspected business ties to each other, and Customer 2 had recently taken Customer 24 on as a personal assistant. SCA was concerned about the involvement of Customer 24 in Customer 2 and Customer 17's relationship: SMR dated 23 January 2017.

By at least October 2017, SCA was aware that Customer 2 was in business with another SCA customer. Customer 2 and the other customer's companies had signed a deal with the Australian government for a large mining project. In May 2019, it was publicly reported that this customer was a member of a foreign political party.

m. SCA was aware that Customer 2 frequently engaged in large buy-ins and cash outs, including with cash, CVIs and cheques:

Particulars

Cash and chips

SCA frequently recorded that Customer 2 made significant buy-ins or cash outs at SCA. For example:

a. on 1 January 2017, Customer 2 made a $10,000 cash buy-in. An hour later, Customer 2 cashed out $24,150 in chips for cash. A few hours later, Customer 2 made another $10,000 cash buy-in. Customer 2 then cashed out $19,200 in chips for cash;

b. on 4 August 2017, Customer 2 made a $50,000 CPV buy-in with funds they had received via a telegraphic transfer. Later that day, Customer 2 cashed out $78,000 in chips and deposited the funds into their FMA. Customer 2 then received a CPV for $50,000. Five minutes later, Customer 2 cashed out $20,450 in chips and deposited the funds into their FMA. Shortly after, Customer 2 cashed out $48,450 in cash from their FMA;

c. on 13 March 2018, Customer 2 made a cash buy-in for $20,000 and received a CPV. A couple of hours later, Customer 2 made a cash buy-in for $50,000 and received a non-negotiable CPV. Ten minutes later, Customer 2 cashed out $75,000 in cash chips. These funds were deposited into their FMA, and then Customer 2 received a $75,000 non-negotiable CPV. Half an hour later, Customer 2 deposited $60,000 in chips into their FMA. Customer 2 then exchanged $109,850 in cash chips for cash;

d. on 30 January 2019, Customer 2 made a $80,000 CPV buy-in. A few hours later, Customer 2 deposited $124,000 in chips into their FMA. Customer 2 then withdrew $40,000 in cash from their FMA;

e. on 12 July 2019, Customer 2 made a $100,000 CPV buy-in. Approximately an hour later, Customer 2 deposited $203,000 in chips into their FMA. Customer 2 then withdrew $10,000 in cash from their FMA;

f. on 3 January 2020, Customer 2 made a cash buy-in for $50,000 and received cash chips. Approximately 20 minutes later, Customer 2 deposited $60,000 in cash chips into their FMA, and exchanged $10,000 in cash chips for cash; and

g. on 8 March 2021, Customer 2 made two cash buy-ins totalling $50,000 and received CPVs. An hour later, Customer 2 deposited $180,750 in cash chips into their FMA. Ten minutes later, Customer 2 withdrew $156,550 in cash from their FMA.

Cheques

On a number of occasions, Customer 2 made buy-ins using cheques at SCA, including cheques drawn from different banks. For example, between 5 April 2018 and 6 June 2019, Customer 2 made buy-ins at SCA using at least 13 cheques totalling $1,455,000 drawn from three different Australian banks.

n. Customer 2, and persons associated with them, transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 23 December 2016 and 18 March 2021, SCA gave the AUSTRAC CEO 676 TTRs detailing transactions made by Customer 2 totalling $31,783,352, which comprised:

a. 183 TTRs totalling $14,367,822 in account deposits;

b. 168 TTRs totalling $9,498,271 in account withdrawals;

c. 315 TTRs totalling $7,747,755 in chip and cash exchanges; and

d. 10 TTRs totalling $169,503 in premium player commissions/rebates.

Large and suspicious cash transactions

See particulars to paragraphs 586.i and 586.j above.

o. Customer 2, and persons associated with them, engaged in other transactions indicative of other ML/TF typologies and vulnerabilities, including structuring;

Particulars

See paragraph 24 above.

See particulars to paragraphs 586.i and 586.j above.

For example, on 18 February 2017, an SCA customer approached a baccarat table with a handful of cash. Prior to handing over the cash, the customer deliberately removed one $100 note from the bundle. The total amount of cash presented to the table game staff was $9,900. The customer informed staff that the money belonged to Customer 2. The customer exchanged the cash for chips, and then walked over to Customer 2 and gave them the chips. SCA noted that Customer 2 regularly used runners to perform transactions on their behalf, and considered that Customer 2 was using their associates to structure their buy-ins to avoid reporting obligations: SMR dated 20 February 2017.

p. Customer 2 had access to private gaming rooms at SCA;

Particulars

See paragraph 145(e) above.

Customer 2 had access to private gaming rooms at SCA, including the Grange Room and the Platinum Room.

q. SCA was aware that Customer 2 frequently engaged in disorderly and aggressive behaviour at SCA; and

Particulars

On 25 February 2017, Customer 2 was banned from SCA's premises for 24 hours as a result of intoxication and abusive behaviour towards SCA staff. Approximately an hour after being banned, Customer 2 was spotted by VIP staff and the Grange desk. Customer 2 was escorted outside by SCA staff.

On 26 May 2017, Customer 2 was escorted off the SCA premises due to intoxication. Two hours later, Customer 2 returned to SCA and was observed in the Grange Room. SCA staff again asked Customer 2 to leave.

On 18 May 2018, an SCA Gaming Operations Shift Manager emailed other SCA staff to inform them that Customer 2 had been very upset, loud and disruptive in the Grange Room that day when conducting a cash out transaction.

On 28 September 2018, Customer 2 attempted to physically assault another SCA customer at a gaming table. SCA recorded that Customer 2 grabbed a chair in an attempt to strike the other customer. Customer 2 was escorted off the premises by SCA staff. Ten minutes later, security was notified that Customer 2 was back on the premises. Customer 2 was again removed from SCA.

r. SCA did not have adequate reason to believe that Customer 2's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 2 by SCA.

Particulars

See paragraph 516 above.

At all times on and from 7 December 2016, SCA understood that Customer 2 was the president of Company 2.

By April 2017, SCA suspected that Customer 2 and their associates were engaging in loan sharking and other activities indicative of ML/TF typologies: see particulars to paragraph 586.i above.

In December 2018, SCA suspected that Customer 2 was using a third party remittance company to transfer funds out of a foreign country and into SCA: see particulars to paragraphs 586.j and 586.k above.

In September 2019, SCA recorded that Customer 2 had been using their company account for recreational purposes, and had conducted

several transactions that did not have a clear gaming purpose: see particulars to paragraph 586.j above.

However, SCA did not request source of wealth information from Customer 2 until 9 August 2021. On the same date, SCA informed Customer 2 that they were banned from attending the casino until an assessment of their Source of Wealth Declaration had been completed. Customer 2 declined to provide this information.

At no time did SCA request source of funds information from Customer 2.

SCA's determination of the ML/TF risks posed by Customer 2

587. On and from 5 August 2016, Customer 2 was appropriately rated by SCA as a high risk customer for the purpose of the Act and Rules.

588. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 2 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 2.

Monitoring of Customer 2's transactions

589. At no time did SCA apply appropriate transaction monitoring to Customer 2's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities;

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not make or keep appropriate records of designated services provided to junket operators and junket players;

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

c. SCA did not carry out adequate due diligence on source of funds in respect of third party deposits received for the benefit of Customer 2 into its bank accounts;

Particulars

See paragraph 227 above.

d. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 2 through:

i. the junket channel; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

ii. the SCEG customer account channel, the SCA customer account channel and the SkyCity New Zealand channel, which were high risk remittance channels.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 2's KYC information

590. SCA did not review, update or verify Customer 2's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 2, including the nature, extent and purpose of Customer 2's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 2's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 2's risk profile* above, there were higher ML/TF risks associated with Customer 2's source of wealth or source of funds.

In and from April 2017, SCA suspected that Customer 2 and their associates were engaging in loan sharking / money lending behaviour, suggesting that there were real ML/TF risks as to Customer 2's source of funds: see particulars to paragraph 586.i above.

d. to the extent that SCA reviewed Customer 2's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 2.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

ECDD triggers in respect of Customer 2

591. SCA was required to apply the ECDD program to Customer 2 following any ECDD triggers in respect of Customer 2.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

592. Customer 2 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 23 January 2017 and 15 March 2021, SCA gave the AUSTRAC CEO 30 SMRs with respect to or pertaining to Customer 2.

b. determined by SCA to be high risk for the purpose of the Act and Rules prior to the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 2* above.

593. Each matter pleaded at paragraph 592 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

594. SCA did not conduct appropriate risk-based ECDD with respect to Customer 2 following an ECDD trigger because:

a. on each occasion prior to 9 August 2021 that SCA conducted ECDD in respect of Customer 2 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 2 and failed to appropriately consider whether the ML/TF risks posed by Customer 2 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501, 511 and 516 to 517 above.

Watchlist screenings

On 29 September 2017 and 16 April 2018, SCA conducted Jade watchlist screenings in respect of Customer 2.

Transaction reviews

In January 2017, February 2017, October 2017, March 2018, April 2018, May 2018 and December 2018, SCA staff (including AML Analysts) requested historical reviews of Customer 2's transactions at SCA. On each occasion, the SCA staff member who requested the review was advised of the findings.

On multiple occasions between April 2018 and March 2021, SCA conducted surveillance of Customer 2's transactions at SCA. On each occasion, SCA AML Analysts were advised of the findings and the suspicious behaviour was subsequently reported in an SMR to the AUSTRAC CEO.

ECDD screenings

On 8 August 2019 and 7 July 2021, SCA conducted ECDD in respect of Customer 2. These screenings consisted of reviews of:

a. historical SMRs submitted in respect of Customer 2, which reported Customer 2 engaging in transactions which had the risk of layering, Customer 2 utilising money remitters to send money from overseas into Australia due to restrictions with foreign governments and Customer 2 conducting large cash transactions on days with no recorded play;

b. Customer 2's source of wealth, which recorded their occupation as the president of Company 2. In 2014, Company 2 purchased a mine in Australia. Customer 2 also worked closely with their company's subsidiary;

c. Customer 2's known associates; and

d. open source information in respect of Customer 2, including media articles and business registration details regarding Customer 2's company. The searches revealed that Customer 2 was an Honorary President of an overseas industry body.

On 23 February 2021, SCA conducted source of wealth ECDD screening in respect of Customer 2. The screening identified that:

a. watchlist checks revealed no derogatory information with respect to Customer 2 or their company; and

b. Customer 2 was the director of two mining companies, including Company 2.

On 9 August 2021, SCA issued a ban in respect of Customer 2 pending them completing a Source of Wealth Declaration. Customer 2 refused to provide this information.

The ECDD conducted by SCA did not have appropriate regard to Customer 2's higher ML/TF risks: see *Customer 2's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 2's source of funds or source of wealth.

By reason of the matters set out in *Customer 2's risk profile* above, there were real risks that Customer 2's source of wealth and source of funds were not legitimate.

b. on any occasion prior to 9 August 2021 that senior management considered the higher ML/TF risks posed by Customer 2 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 2 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

'Transaction Monitoring Overview' reports

Between February 2018 and August 2019, Customer 2 was mentioned in seven 'Transaction Monitoring Overview' reports which were provided to the AML/CTF Senior Management Group, for discussion at its meetings.

Other senior management consideration

On 26 May 2019, the SCEG Group Director – International Business Operations advised other senior management how important Customer 2 was to the business, noting Customer 2's turnover and losses on an individual commission program.

On several occasions between April 2017 and October 2019, members of the SCA AML team notified the SCA Legal, Compliance & Regulatory Affairs Manager about the suspicious transactions conducted by Customer 2 and other customers:

a. On 21 April 2017, an SCA AML Analyst notified the SCA Legal, Compliance & Regulatory Affairs Manager of the suspicious transactions conducted by Customer 2 and other customers on 19 April 2017 which were the subject of an SMR dated 21 April 2017: see particulars to paragraph 586.i above.

b. On 4 May 2017, the SCEG Group General Manager Regulatory Affairs and AML was informed of the suspicious transactions. On 29 November 2018, an SCA AML Adviser provided details of a number of SMRs lodged with respect to Customer 2 and other customers, and linked Customer 2 to other customers who SCA considered acted suspiciously, including Customer 11, Customer 17, Customer 27 and Customer 31, to the SCA General Manager Legal,

Compliance & Regulatory Affairs and the SCA Legal & Compliance Advisor.

c. On 2 October 2019, an SCA AML Adviser notified the SCA Legal, Compliance & Regulatory Affairs Manager of the suspicious transactions conducted by Customer 2 and other customers on 1 October 2019 which were the subject of an SMR dated 3 October 2019: see particulars to paragraph 586.i above.

d. On 23 October 2019, an SCA AML Adviser notified the SCA Legal, Compliance & Regulatory Affairs of the suspicious transactions conducted by Customer 2 and other customers that day which were the subject of an SMR dated 25 October 2019: see particulars to paragraph 586.i above.

There are no records showing that the SCA Legal, Compliance & Regulatory Affairs Manager, or any other person from senior management, responded to any of the above reports from the SCA AML team.

On 9 February 2021, the SCEG SVP Marketing-Asia emailed an open source link about Customer 2's company to the SCEG Group General Manager International Gaming and the SCEG Commercial Manager.

Despite receiving the above information there are no records of senior management appropriately considering whether the ML/TF risks posed by Customer 2 were within SCA's risk appetite.

It was not until 9 August 2021 that SCA issued a ban in respect of Customer 2.

Contravention of s 36 of the Act in respect of Customer 2

595. By reason of the matters pleaded at paragraphs 583 to 594 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 2 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

596. By reason of the matters pleaded at paragraph 595, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 9 August 2021 with respect to Customer 2.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 3

597. Customer 3 was a customer of SCA during the relevant period. Between 7 December 2016 and 12 July 2017, SCA recorded turnover exceeding $430,000,000 for junkets operated by Customer 3.

Particulars

Customer 3 was a customer of SCA from at least 28 September 2016.

On 22 March 2022, SCA issued a ban in respect of Customer 3 at the direction of the SCA AML team because of Customer 3's role as junket operator for Customer 11 and Customer 12.

598. SCA provided Customer 3 with designated services within the meaning of table 1 and table 3, s 6 of the Act during the relevant period including services connected to Customer 3's role as a junket operator.

Particulars

In September 2016, SCA opened an FMA for Customer 3 which was closed on 22 March 2022 (item 11, table 3, s 6 of the Act).

While a customer of SCA, Customer 3 remitted funds to and from their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 3's risk profile* below.

599. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 3.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 3's risk profile

600. On and from 7 December 2016, Customer 3, and the provision of designated services to Customer 3 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 3's risk profile prior to the relevant period

a. by 7 December 2016 Customer 3 had the following risk history:

   i. SCA had formed suspicions for the purposes of s 41 of the Act with respect to Customer 3;

Particulars

SCA gave the AUSTRAC CEO an SMR on 8 November 2016. The SMR reported connections between Customer 3's junket and Customer 11, and between Customer 3's junket and threshold transactions conducted by Customer 11 and Customer 12. The SMR also reported that a SCEG New Zealand casino had reported

concerns about Customer 11 and Customer 12 being associated with suspected sex workers.

ii. Customer 3 and persons associated with their junket engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

Particulars

By 7 December 2016, SCA was aware that Customer 11 was regularly cashing out gaming chips under Customer 3's name when playing on Customer 3's junket. Customer 11 also took control of funds at settlement of Customer 3's junket programs.

SCA also identified that a number of threshold transactions conducted by Customer 3's junket had been reported to AUSTRAC as transactions conducted by Customer 11, and that a number of threshold transactions conducted by Customer 11 had been reported as conducted by Customer 3. For example:

a. On 30 September 2016, a transaction of $40,000 was conducted by Customer 11 but attributed by SCA to Customer 3.

b. On 2 October 2016, a transaction of $61,685 was conducted by Customer 11 but attributed by SCA to Customer 3.

c. On 26 October 2016, a transaction of $60,015 was conducted by Customer 11 but attributed by SCA to Customer 3.

d. On 27 October 2016, a transaction of $10,505 was conducted by Customer 11 but attributed by SCA to Customer 3.

e. On 29 October 2016, a transaction of $39,100 was conducted by Customer 11 but attributed by SCA to Customer 3.

f. On 30 October 2016, a transaction of $17,000 was conducted by Customer 11 but attributed by SCA to Customer 3.

g. On 2 November 2016, a transaction of $40,000 was conducted by Customer 11 but attributed by SCA to Customer 3.

This was despite Customer 3 never having attended SCA. Customer 12 operated all of Customer 3's junket programs at SCA.

iii. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 3 by remitting large amounts of money into and within the casino environment via their accounts, including through high risk remittance channels; and

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

For example, on 28 September 2016, Customer 3 received $2,011,136 into their SCA FMA via telegraphic transfer. SCA made these funds available to Customer 3.

Remittances within the casino environment

SCA made money available to Customer 3 in the following transactions:

a. on 28 September 2016, Customer 3 received $500,000 into their SCA FMA from another customer's SCA FMA; and

b. on 27 October 2016, Customer 3 received $700,000 and $300,000 in two transfers into their SCA FMA from another customer's SCA FMA.

SCA accepted instructions to transfer funds from Customer 3's accounts for the following transactions:

a. on 28 September 2016, Customer 3 transferred $1,300,000 from their SCA FMA to another customer's SCA FMA; and

b. on 1 October 2016, Customer 3 transferred $1,645,000 from their SCA FMA to another customer's SCA FMA.

c. on 1 October 2016, Customer 3 received $500,000 into their SCA FMA from another customer's SCA FMA;

d. on 2 October 2016, Customer 3 transferred $28,327 from their SCA FMA to Customer 12's SCA FMA; and

e. on 19 November 2016, Customer 3 transferred $30,000 and $800,000 in two transfers from their SCA FMA to another customer's SCA FMA.

iv. SCA recorded that Customer 3 transacted using large amounts of cash at SCA, despite Customer 3 never physically attending SCA's premises;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 20 March 2015 and 22 November 2016, SCA gave the AUSTRAC CEO 18 TTRs detailing incoming and outgoing payments made by Customer 3 totalling $7,918,684 which comprised:

a. six TTRs totalling $206,620 in chip and cash exchanges;

b. six TTRs totalling $5,773,728 in account deposits; and

c. six TTRs totalling $1,938,336 in account withdrawals.

Large cash transactions

On 30 September 2016, SCA recorded that Customer 3 withdrew $98,000 cash from their FMA.

On 1 October 2016, SCA recorded that Customer 3 deposited $90,000 into their FMA.

On 2 October 2016, Customer 3 received a $61,685 settlement in cash from SCA.

On 29 October 2016, SCA recorded that Customer 3 received $12,000 in cash from SCA.

Customer 3's risk profile during the relevant period

b. Customer 3 was a junket operator who facilitated the provision of high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA;

   i. between 7 December 2016 and 11 July 2017, Customer 3 operated 10 junkets at SCA;

   ii. between 1 July 2016 and 11 July 2017 SCA recorded that the total cumulative turnover of junkets operated by Customer 3 was $432,394,716;

Particulars

See paragraphs 399 to 401 above.

In the 2017 financial year, SCA recorded that junkets operated by Customer 3 had turnover of $338,876,204.

In the 2018 financial year, SCA recorded that junkets operated by Customer 3 had turnover of $93,518,512.

   iii. Customer 3 operated junkets in private gaming rooms;

Particulars

See paragraph 145(e) above.

Customer 3 operated junkets in private gaming rooms, including the Horizon Suites, Opal Room and Grange Room.

   iv. Customer 3 had at least one junket representative at SCA, Customer 12; and

   v. Customer 3 and their junket representative facilitated the provision of high value designated services to junket players at SCA, including players who posed higher ML/TF risks and who SCA considered had acted suspiciously such as the main player on the junket, Customer 11, who was a foreign PEP;

Particulars

See paragraphs 388 and 389 above.

For example, on and from 7 December 2016, SCA held concerns that Customer 11 controlled buy-ins and settlements for Customer 3's junket, taking control of funds at the conclusion of programs and regularly cashing out chips on programs under Customer 3's name, despite Customer 3 having never attended SCA.

See *Customer 11's risk profile*, below.

c. designated services provided to Customer 3 lacked transparency as the services were provided through the channel of junket programs at SCA;

Particulars

See paragraph 392 above.

d. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 3 by remitting large amounts of money into, out of and within the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

SCA made money available to Customer 3 in the following transactions:

a. on 20 April 2017, Customer 3 received $3,430,000 into their SCA FMA via telegraphic transfer. Customer 3 subsequently transferred $3,430,000 from their SCA FMA via telegraphic transfer;

b. on 2 May 2017, SCA received a deposit of $600,000 into its bank account by Company 5 for use by Customer 3's junket. SCA conducted a company search on Company 5, which showed that Company 5 was owned by an overseas company, Company 6. SCA did not find a link between Customer 3's junket and Company 5, and, when questioned, Customer 12 claimed that Company 5 was a finance company of which Customer 3 was a customer;

c. on 2 July 2017, Customer 3 received $3,800,000 into their SCA FMA via telegraphic transfer and transferred $3,800,000 from their SCA FMA via telegraphic transfer; and

d. on 8 February 2018, Customer 3 transferred $967,344 to their SCA FMA with the instruction to make it available to Customer 11's SCA FMA.

SCA accepted instructions to transfer funds from Customer 3's accounts for the following transactions:

a. On 15 April 2017, Customer 3 transferred $100,000 from their SCA FMA via a telegraphic transfer.

Remittances through the SkyCity New Zealand channel

For example, on 10 April 2017, SCA credited $3,374,600 to Customer 3's FMA with these funds originating from Customer 11's FMA held at a SCEG New Zealand casino. SCA made these funds available to Customer 3.

Remittances from SCA FMAs to SCEG New Zealand FMAs

SCA accepted instructions to transfer funds from Customer 3's accounts for the following transactions.

Between 23 January 2017 and 13 June 2017, SCA credited $6,929,290 to a SCEG New Zealand casino, with these funds originating from Customer 3's SCA FMA.

a. On 23 January 2017, Customer 3 transferred $1,800,000 and $1,750,000 via two telegraphic transfers to a SCEG New Zealand casino.

b. On 1 May 2017, Customer 3 transferred $1,250,000 via telegraphic transfer to a SCEG New Zealand casino.

c. On 3 May 2017, Customer 3 transferred $400,000 to a SCEG New Zealand casino.

d. On 13 June 2017, Customer 3 transferred $3,529,290 via telegraphic transfer to a SCEG New Zealand casino.

Remittances within the casino environment

SCA made money available to Customer 3 in the following transactions:

a. On 14 December 2016, Customer 3 received $1,200,000 into their SCA FMA from another customer's SCA FMA.

b. On 21 January 2017, Customer 3 received $1,200,000 into their SCA FMA from Customer 11's SCA FMA.

c. On 15 April 2017, Customer 3 received $3,374,600 into their SCA FMA from Customer 11's SCA FMA.

d. On 17 April 2017, Customer 3 received $3,400,000 into their SCA FMA from another customer's SCA FMA.

e. On 19 June 2017, Customer 3 received $3,051,563 into their SCA FMA from Customer 12's SCA FMA.

f. On 2 July 2017, Customer 3 received $3,800,000 into their SCA FMA from Customer 11's SCA FMA.

g. On 4 July 2017, Customer 3 received $41,960 and $79,587 in two transfers into their SCA FMA from Customer 12's SCA FMA.

SCA accepted instructions to transfer funds from Customer 3's accounts for the following transactions.

a. On 28 December 2016, Customer 3 transferred $1,000 from their SCA FMA to another customer's SCA FMA.

b. On 26 January 2017, Customer 3 transferred $5,000 from their SCA FMA to another customer's SCA FMA.

c. On 17 January 2017, Customer 3 transferred $14,763 and $1,700,000 in two transfers from their SCA FMA to another customer's SCA FMA.

d. On 23 January 2017, Customer 3 transferred $ 23,212 from their SCA FMA to Customer 12's SCA FMA, and $1,400,000 from their SCA FMA to another customer's SCA FMA.

e. On 15 April 2017, Customer 3 transferred $3,404,000 from their SCA FMA to another customer's SCA FMA.

f. On 20 April 2017, Customer 3 transferred $30,784 from their SCA FMA to Customer 12's SCA FMA.

g. On 3 May 2017, Customer 3 transferred $2,000,000 from their SCA FMA to Customer 12's SCA FMA.

h. On 17 June 2017, Customer 3 transferred $56,226 from their SCA FMA to Customer 12's SCA FMA.

i. On 17 June 2017, Customer 3 transferred $3,700,000 from their SCA FMA to Customer 11's SCA FMA.

j. On 17 June 2017, Customer 3 transferred $3,350,000 from their SCA FMA to another customer's SCA FMA.

k. On 19 June 2017, Customer 3 transferred $1,500 from their SCA FMA to another customer's SCA FMA.

l. On 26 June 2017, Customer 3 transferred $66,587 from their SCA FMA to Customer 12's SCA FMA.

m. On 26 June 2017, Customer 3 transferred $59,761 from their SCA FMA to Customer 11's SCA FMA.

n. On 10 July 2017, Customer 3 transferred $16,649 from their SCA FMA to Customer 12's SCA FMA.

e. Customer 3 was connected to other customers at SCA, including junket players, foreign PEPs, players who posed higher ML/TF risks and players who SCA considered had acted suspiciously such as Customer 11, Customer 12 and Customer 15;

Particulars

Between 1 December 2016 and 11 July 2017, Customer 11 was the main player on 10 junkets at SCA operated by Customer 3, for which Customer 12 was the junket representative. Customer 15 was also a player on these junkets.

Customer 3 is Customer 12's sibling. From at least February 2018, SCA was aware that Customer 12 was being investigated by an Australian government agency in respect of their income.

f. SCA recorded that Customer 3 transacted using large amounts of cash at SCA, despite Customer 3 never physically attending SCA's premises;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 24 January 2017 and 17 July 2017, SCA gave the AUSTRAC CEO 17 TTRs incoming and outgoing payments made by Customer 3 totalling $15,030,673, despite Customer 3 never having attended the SCA property. These comprised:

a. three TTRs totalling $70,500 in chip and cash exchanges;

b. four TTRs totalling $7,461,892 in account deposits;

c. nine TTRs totalling $7,471,441 in account withdrawals; and

d. one TTR totalling $26,840 for a premium player commission/rebate.

Large and suspicious cash transactions in 2016

On 14 December 2016, SCA's records indicated that Customer 3 exchanged $28,000 in SCA chips for cash, despite Customer 3 never having attended the SCA property.

Large and suspicious cash transactions in 2017

Between January 2017 and July 2017, SCA's records indicate that Customer 3 transacted with over $1,302,620 in cash through their SCA FMA, despite Customer 3 never having attended the SCA property.

a. On 6 January 2017, Customer 3 withdrew $5,000 in cash from their SCA FMA.

b. On 6 January 2017, Customer 3 deposited $215,000 in cash into their SCA FMA.

c. On 17 January 2017, Customer 3 deposited $302,000 in cash into their SCA FMA.

d. On 17 January 2017, Customer 3 withdrew $79,017 in cash from their SCA FMA.

e. On 23 January 2017, Customer 3 withdrew $300,000 in cash from their SCA FMA.

f. On 20 April 2017, Customer 3 deposited $20,000 in cash into their SCA FMA.

g. On 19 June 2017, Customer 3 received a $75,353 settlement in cash from SCA.

h. On 4 July 2017, Customer 3 deposited $12,620 in cash into their SCA FMA.

i. On 10 July 2017, Customer 3 deposited $258,000 in cash into their SCA FMA.

j. On 10 July 2017, Customer 3 withdrew $4,500 in cash from their SCA FMA.

k. On 11 July 2017, Customer 3 received a $26,840 cash settlement from SCA.

l. On 12 July 2017, Customer 3 withdrew $4,000 in cash from their SCA FMA.

g. SCA issued cheques to Customer 3, and credited Customer 3's FMA with amounts from cheques, despite Customer 3 never having attended the SCA property;

Particulars

On 16 December 2016, SCA issued Customer 3 a cheque in the amount of $1,201,000 to buy back front money.

On 26 December 2016, SCA credited Customer 3's FMA with $1,200,000, which was received via a cheque.

On 6 January 2017, SCA issued Customer 3 a cheque in the amount of $1,200,000 to buy back front money.

On 26 June 2017, SCA issued Customer 3 a cheque in the amount of $3,800,000 to buy back front money.

h. Customer 3 and persons associated with their junket engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

Particulars

From 7 December 2016, SCA was aware that Customer 11 was regularly cashing out gaming chips under the junket operator's name when playing on Customer 3's junket, and took control of funds at settlement from Customer 3's junket programs.

a. On 14 December 2016, a transaction of $22,500 cashing out non-negotiable and commission chips was conducted by Customer 11 but attributed by SCA to Customer 12. Customer 12 claimed the transaction related to play conducted by Customer 3, but Customer 3 was not in the country and all table play was confirmed to be Customer 11's.

b. Between 21 and 22 January 2017, a transaction of $40,000 was conducted by Customer 11 but attributed by SCA to Customer 3.

c. On 24 January 2017, four transactions conducted by Customer 11 were attributed by SCA to Customer 3.

d. On 15 April 2017, a transaction of $20,000 was conducted by Customer 11 but attributed by SCA to Customer 3, despite Customer 3 not being onsite.

i. in 2018 and 2019, Customer 3 was the subject of law enforcement enquiries on three occasions at SCA; and

Particulars

On 5 January 2018, 17 January 2019 and 14 February 2019 SCA received a request from a law enforcement agency regarding Customer 3.

j. SCA did not have adequate reason to believe that Customer 3's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 3 by SCA.

Particulars

See paragraph 516 above.

On and from 7 December 2016, SCA recorded high levels of turnover in respect of Customer 3's junkets and attributed large volumes of transactions to Customer 3. Customer 3's junket had a high turnover estimated at $432,394,716 over 12 junket programs operated by Customer 3 at SCA between 28 September 2016 and 11 July 2017. However, at no time did Customer 3 physically attend the SCA property.

On and from 7 December 2016, SCA understood Customer 3's occupation to be as a "trade manager".

SCA was aware that Customer 3 had not visited the SCA property, despite operating junkets there. Further, SCA was aware that Customer 3 was closely connected to Customer 11 and Customer 12, both of whom conducted transactions on Customer 3's SCA FMA.

From at least 29 July 2019, SCA was aware of media reports that Customer 11 and Customer 12 were suspected of being involved in money laundering at other Australian casinos.

Despite this, at no time did SCA obtain or verify Customer 3's source of wealth or source of funds information.

SCA's determination of the ML/TF risks posed by Customer 3

601. SCA was unable to appropriately identify or assess the ML/TF risks posed by Customer 3 because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 3.

a. On and from 7 December 2016, Customer 3 should have been recognised by SCA as a high risk customer for the purpose of the Act and Rules for the reasons pleaded above: see *Customer 3's risk profile* above.

Particulars

Sections 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

b. It was not until 11 September 2019 that Customer 3 was rated high risk by SCA for the purpose of the Act and Rules.

Monitoring of Customer 3's transactions

602. At no time did SCA apply appropriate transaction monitoring to Customer 3's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities;

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not make or keep appropriate records of designated services provided to junket operators;

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

c. SCA did not carry out adequate due diligence on source of funds in respect of third party deposits received for the benefit of Customer 3 into its bank accounts; and

Particulars

See paragraph 227 above.

d. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 3 through:

i. the junket channel; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

ii. the SCA customer account channel and the SkyCity New Zealand channel, which were high risk remittance channels.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, verification and update of Customer 3's KYC information

603. SCA did not review, update or verify Customer 3's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 3, including the nature, extent and purpose of Customer 3's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update or verify Customer 3's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 3's risk profile* above, there were real risks that Customer 3's source of wealth and source of funds were not legitimate.

On and from 7 December 2016, SCA recorded large volumes of transactions as having been conducted by Customer 3, despite Customer 3 never having visited the SCA property.

At no stage did SCA obtain or verify source of wealth or source of funds information from Customer 3, despite significant cash transactions and telegraphic transfers into and out of Customer 3's SCA FMA in connection with their junket.

d. to the extent that SCA reviewed Customer 3's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 3.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

Failure to apply appropriate due diligence suited to the high ML/TF risks

604. Had SCA conducted ongoing customer due diligence on and from 7 December 2016 by:

a. appropriately identifying and assessing the ML/TF risks posed by Customer 3;

b. applying appropriate risk-based transaction monitoring to Customer 3; and

c. appropriately reviewing and updating Customer 3's KYC information, having regard to the high ML/TF risks,

SCA would have been required by the Act and Rules to apply the ECDD Program to Customer 3 at a time before the date of the ECDD triggers pleaded below: see *ECDD triggers in respect of Customer 3*.

ECDD triggers in respect of Customer 3

605. SCA was required to apply the ECDD program to Customer 3 following any ECDD triggers in respect of Customer 3.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3), and 15.10 of the Rules.

606. Customer 3 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

On 4 May 2017, SCA gave the AUSTRAC CEO an SMR pertaining to Customer 3.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 3* above.

607. Each matter pleaded at paragraph 606 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

608. SCA did not conduct appropriate risk-based ECDD with respect to Customer 3 following an ECDD trigger because:

a. on each occasion prior to 22 March 2022 that SCA conducted ECDD in respect of Customer 3 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 3 and failed to appropriately consider whether the ML/TF risks posed by Customer 3 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

On 5 December 2019, SCA conducted ECDD in respect of Customer 3.

On 22 March 2022, SCA issued a ban in respect of Customer 3 following in-house investigations by the AML team and adverse open source media.

The ECDD conducted by SCA did not have appropriate regard to Customer 3's higher ML/TF risks: see *Customer 3's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 3's source of funds or source of wealth.

By reason of the matters set out in *Customer 3's risk profile* above, there were real risks that Customer 3's source of wealth and source of funds were not legitimate.

b. on any occasion prior to 22 March 2022 that senior management considered the higher ML/TF risks posed by Customer 3 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 3 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

On 17 November 2017, the SCA AML/CTF Senior Management Group considered Customer 3's junket for the purposes of risk controls and monitoring.

On 26 August 2020, the SCEG Group General Manager Regulatory Affairs and AML and the SCEG Commercial Manager identified that Customer 3's junket licence was due to expire the following day. They agreed that a note should be made on the system that the licence was not to be renewed without approval from the compliance or international business teams. They also agreed that it was only necessary to ban Customer 3 from gaming at the casino as a junket operator, rather than as an individual. In particular, they noted that there were no reasons 'on the AML side' for banning them, and it would be sufficient to let SCA know that Customer 3 was a person of interest.

On 3 September 2020, the SCEG Group General Manager Regulatory Affairs and AML emailed the SCEG AML Compliance and Intelligence Manager and the SCA General Manager Legal, Compliance & Regulatory Affairs communicating that Customer 3's junket approval had expired and that it would not be renewed. The email noted that Customer 3's association with Customer 12 would be relevant to any decision by SCA to continue its business relationship with Customer 3. At no time was Customer 3's relationship with Customer 11, who had by that time been recognised by SCA as a foreign PEP, considered in the context of the ML/TF risks of continuing a business relationship with Customer 3.

Prior to October 2021, there are no records demonstrating that SCA senior management conducted its own due diligence for the purposes of determining whether it was appropriate to continue a business relationship with Customer 3.

On 14 October 2021, in an internal memorandum SCA recommended that SCA's business relationship with Customer 3 be terminated due to increased scrutiny around junkets and the lack of information surrounding the origin of funds deposited into SCA's FMA in association with Customer 3's junket.

However, it was not until 22 March 2022 that SCA issued a ban in respect of Customer 3 following in-house investigations by the AML team.

Contravention of s 36 of the Act in respect of Customer 3

609. By reason of the matters pleaded at paragraphs 597 to 608 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 3 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

610. By reason of the matters pleaded at paragraph 609, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 22 March 2022 with respect to Customer 3.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 4

611. Customer 4 was a customer of SCA during the relevant period. Between 15 December 2016 and 16 December 2016, SCA recorded turnover exceeding $45,000,000 for junkets operated by Customer 4.

Particulars

Customer 4 was a customer of SCA from at least 7 August 2015.

On 22 March 2022, SCA issued a ban in respect of Customer 4 at the direction of the SCA AML team.

612. SCA provided Customer 4 with designated services within the meaning of table 1 and table 3, s 6 of the Act during the relevant period including services connected to Customer 4's role as a junket operator and gambling as a junket player.

Particulars

On 7 August 2015, SCA opened an FMA for Customer 4 which was closed on 22 March 2022 (item 11, table 3, s 6 of the Act).

Between 30 July 2015 and 12 December 2016, SCA provided lines of credit for Customer 4 on two occasions with a limit ranging from $5,000,000 to $8,000,000 (item 6, table 1, s 6 of the Act).

See *Customer 4's risk profile* below.

613. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 4.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 4's risk profile

614. On and from 7 December 2016, Customer 4, and the provision of designated services to Customer 4 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 4's risk profile prior to the relevant period

a. by 7 December 2016, Customer 4 had the following risk history:

i. Customer 4 was a junket operator who facilitated the provision of high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA;

Particulars

Customer 4 operated a junket at SCA between 7 August 2015 and 8 August 2015.

The junket had a recorded buy-in of at least $10,000,000 and a turnover of at least $24,525,000.

Customer 4 operated their junket in private gaming rooms at SCA including the Grange Room, the Horizon Room and a VIP Room.

The junket that Customer 4 operated between 7 August 2015 and 8 August 2015 had one junket player.

On 23 December 2015, SCA recorded that Customer 4 was one of the largest junket operators in the world, and had been for over ten years.

ii. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 4 by remitting large amounts of money out of the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

For example, on 14 August 2015, SCA accepted instructions to transfer $600,700 from Customer 4's account to Customer 4's personal bank account overseas. The payment was reported as an outgoing IFTI which recorded the funds as Customer 4's winnings at SCA.

iii. Customer 4 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 12 August 2015 and 17 August 2015, SCA gave the AUSTRAC CEO two TTRs detailing outgoing payments made by Customer 4 totalling $800,700, which comprised:

a. one TTR detailing a $200,000 chip and cash exchange; and

b. one TTR detailing a $600,700 account deposit.

iv. on 7 August 2015, SCA provided Customer 4 with a significant amount of credit upon request, up to a limit of $5,000,000; and

Particulars

See paragraphs 321 to 323, and 342 above.

v. by 2015, SCEG was aware of a number of media articles reporting that Customer 4 had been arrested by a foreign government and was connected to corruption and money laundering activities in other foreign countries;

Particulars

SCEG conducted open source searches in respect of Customer 4 on 28 July 2015, 23 December 2015 and 6 December 2016 which returned a number of media articles, that reported that:

a. a number of junket operators, including Customer 4, had been detained by a foreign government in connection with corruption charges involving a former foreign political party chief. The arrests were a result of underground money transfers; and

b. Customer 4 was one of the junket operators detained in those arrests.

It is not known whether SCEG provided the adverse information regarding Customer 4 arising from these searches to SCA: see paragraph 528 above.

Customer 4's risk profile during the relevant period

b. Customer 4 was a junket operator who facilitated the provision of high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA;

i. between 15 December 2016 and 16 December 2016, Customer 4 operated a junket at SCA;

ii. between 15 December 2016 and 16 December 2016, SCA recorded that the junket operated by Customer 4 had buy-in of $2,336,650, and turnover of $45,509,680 with losses of $85,000;

iii. on 16 December 2016, SCA paid benefits of $344,454 to Customer 4 in their capacity as a junket operator;

iv. on 15 December 2016, SCA provided Customer 4 and their junket programs with a significant amount of credit upon request, up to a limit of $8,000,000;

Particulars

See paragraphs 321 to 323, and 342 above.

v. Customer 4 operated junkets in private gaming rooms;

Particulars

See paragraph 145(e) above.

Customer 4 operated junkets in private gaming rooms, including the Grange Room and the Horizon Room.

vi. Customer 4 had two junket representatives at SCA; and

vii. Customer 4 facilitated the provision of high value designated services to two junket players at SCA;

Particulars

See paragraphs 388 and 389 above.

c. Customer 4 was a junket player who received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA through junket programs;

i. between 15 December 2016 and 16 December 2016, Customer 4 was a player on the junket they operated at SCA; and

ii. at no time did SCA record Customer 4's individual gambling activity on junket programs they attended as a junket player;

d. designated services provided to Customer 4 lacked transparency as the services were provided through the channel of junket programs at SCA;

Particulars

See paragraph 392 above.

e. SCA provided designated services (items 31 and 32, table 1, s6 of the Act) to Customer 4 by remitting large amounts of money within the casino environment via their accounts;

Particulars

See paragraphs 232 to 312 above.

For example, on 24 February 2017, SCA accepted instructions to transfer $429,454 from their Customer 4's SCA FMA to a SCEG New Zealand casino.

f. Customer 4 engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

Particulars

For example, on 16 December 2016, an SCA VIP Cashier recorded that Customer 4 had deposited HKD$30,000,000 into their SCA FMA. On the same date, SCA Cashiers recorded that Customer 4 had made three large buy-ins totalling HKD$20,000,000 at the SCA Grange and VIP Cashiers.

g. Customer 4 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

For example, on 27 February 2017, SCA gave the AUSTRAC CEO a TTR detailing an account withdrawal of $429,454 made by Customer 4.

h. SCA provided Customer 4 with a significant amount of credit upon request, up to a limit of $8,000,000;

Particulars

See paragraphs 321 to 323, and 342 above.

See paragraph 614.b.iv above.

i. on 14 December 2016 and 15 December 2016, SCA provided information to law enforcement agencies in respect of Customer 4 and their junket;

Particulars

On 14 December 2016 and 15 December 2016, SCA sent correspondence to law enforcement agencies providing information regarding Customer 4.

j. Customer 4 had access to private gaming rooms at SCA;

Particulars

See paragraph 145(e) above.

See paragraph 614.b.v above.

k. by October 2020, a media report named Customer 4 as a high-profile junket operator with alleged links to organised crime;

Particulars

The media article reported on the Bergin ILGA Inquiry, and named Customer 4 as a junket operator known to senior management at the other Australian casino. The Bergin ILGA Inquiry heard that many of the junket operators who operated at the other Australian casino had reported links to organised crime.

SCA's due diligence records did not contain details of this media article.

l. SCEG was aware of a number of media articles which reported that Customer 4 had been arrested by a foreign government and was connected to corruption and money laundering activities in two foreign countries; and

Particulars

SCEG conducted open source searches in respect of Customer 4 on 7 April 2017, 26 September 2017, 1 November 2017, 28 November 2017, 27 December 2017, 27 January 2018, 1 March 2018, 28 May 2018, 26 June 2018 and 3 September 2018.

SCEG's open source searches for Customer 4 returned a number of media reports, including articles which reported that:

a. a number of junket operators, including Customer 4, had been arrested in a foreign country by a foreign government in connection with corruption charges against a former foreign political party chief. The arrests were a result of underground money transfers;

b. Customer 4 was one of the junket operators detained in those arrests;

c. Customer 4, in their capacity as a junket operator, was known for collecting gambling debts in return for a commission; and

d. junket operators operating in the same foreign country in which Customer 4 was arrested were diverting their junket businesses to other jurisdictions with less restrictive gambling laws to enable businesspeople and officials to gamble undetected by that foreign country. The article reported that the junket operators facilitated arrangements such as flying cash in private jets and questionable money-transfers between jurisdictions, which represented an expansion of organised crime.

It is not known whether SCEG provided the adverse information in respect of Customer 4 arising from these searches to SCA: see paragraph 528 above.

m. SCA did not have adequate reason to believe that Customer 4's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 4 by SCA.

Particulars

See paragraph 516 above.

By 8 August 2015, SCA recorded Customer 4's occupation as a property developer.

In December 2016, SCEG noted that while Customer 4 had provided a business card stating that they were the director of a company, SCEG was unable to verify Customer 4's connection to that company.

During the relevant period, SCA understood that Customer 4 was a junket operator. At no time did SCA take steps to verify Customer 4's occupation, source of wealth or source of funds in circumstances where:

a. publicly accessible media articles, of which at least SCEG was aware, reported that Customer 4 was a significant international junket operator linked to corruption and money laundering activities in foreign countries, and had been arrested by a foreign government;

b. in 2016, SCA recorded turnover on the junket operated by Customer 4 exceeding $45,000,000; and

c. in 2016, SCA provided information to law enforcement agencies in respect of Customer 4 on two occasion.

SCA's determination of the ML/TF risks posed by Customer 4

615. SCA was unable to appropriately identify or assess the ML/TF risks posed by Customer 4 because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 4.

a. On and from 7 December 2016, Customer 4 should have been recognised by SCA as a high risk customer for the purpose of the Act and Rules for the reasons pleaded above: see *Customer 4's risk profile.*

Particulars

Sections 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

b. At no time was Customer 4 rated high risk by SCA for the purpose of the Act and Rules.

Monitoring of Customer 4's transactions

616. At no time did SCA apply appropriate transaction monitoring to Customer 4's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities;

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not make or keep appropriate records of designated services provided to junket operators and junket players; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

c. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 4 through the junket channel.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

The review, update and verification of Customer 4's KYC information

617. SCA did not review, update or verify Customer 4's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 4, including the nature, extent and purpose of Customer 4's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 4's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 4's risk profile* above, there were real risks that Customer 4's source of wealth and source of funds were not legitimate.

d. to the extent that SCA reviewed Customer 4's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 4.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

By December 2016, SCEG was aware that Customer 4 had links to corruption and money laundering activities in foreign countries, and had been arrested by a foreign government: see paragraph 614.a.v. It is not known whether SCEG provided the adverse information in respect of Customer 4 to SCA: see paragraph 528 above.

In December 2018, SCEG approved a line of credit for Customer 4 with a limit of NZD$10,000,000 on the condition of it being guaranteed by Customer 4's associate, Person 8. The application was endorsed by the SCEG Senior Vice President of International Business in Asia who highly recommended Customer 4's guarantor Person 8, stating that they had personally known the guarantor since 2009.

SCEG recorded that Person 8 was a PEP. Attached to the SCEG credit approval form was a news announcement by a foreign securities exchange regarding action taken against Person 8 and their spouse for unauthorised and improper trading.

At no time prior to 22 March 2022 did SCA senior management consider the higher ML/TF risks posed by Customer 4, or appropriately consider the ML/TF risks posed by Customer 4 were within SCA's ML/TF risk appetite.

At no time did SCA rate Customer 4 high risk, and it was not until 22 March 2022 that SCA issued a ban in respect of Customer 4.

Failure to apply appropriate due diligence suited to the high ML/TF risks

618. Had SCA conducted ongoing customer due diligence on and from 7 December 2016 by:

a. appropriately identifying and assessing the ML/TF risks posed by Customer 4;

b. applying appropriate risk-based transaction monitoring to Customer 4; and

c. appropriately reviewing and updating Customer 4's KYC information, having regard to the high ML/TF risks,

SCA would likely have rated Customer 4 as a high risk customer for the purpose of the Act and Rules at a time before Customer 4 was issued with a ban at SCA.

Particulars

Section s 36(1)(a) of the Act.

Rules 15.2 and 15.5 of the Rules.

619. Had SCA rated Customer 4 as a high risk customer for the purpose of the Act and Rules, it would have been required by the Act and Rules to apply the ECDD Program to Customer 4 at a time before 22 March 2022 when Customer 4 was issued with a ban at SCA.

Particulars

Rules 15.9 of the Rules.

Contravention of s 36 of the Act in respect of Customer 4

620. By reason of the matters pleaded at paragraphs 611 to 619 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 4 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2 and 15.5 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions:
s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

621. By reason of the matters pleaded at paragraph 620, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 22 March 2022 with respect to Customer 4.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 5

622. Customer 5 was a customer of SCA during the relevant period. Between 6 August 2017 and 22 March 2022, SCA recorded turnover exceeding $52,900,000 for the junket operated by Customer 5.

Particulars

Customer 5 was a customer of SCA from 6 August 2017.

On 22 March 2022, SCA issued a ban in respect of Customer 5 following investigations by the AML team, due to Customer 5's status as a corporate junket operator.

623. SCA provided Customer 5 with designated services within the meaning of table 1 and table 3, s 6 of the Act during the relevant period including services connected to Customer 5's role as a junket operator.

Particulars

On 6 August 2017, SCA opened an FMA for Customer 5 which was closed on 22 March 2022 (item 11, table 3, s 6 of the Act).

Between 7 August 2017 and 30 July 2019, SCA provided lines of credit for Customer 5 on two occasions with a limit ranging from $500,000 to $800,000 (item 6, table 1, s 6 of the Act).

While a customer of SCA, Customer 5 remitted funds to and from their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 5's risk profile* below.

624. At all times from 6 August 2017, SCA was required to conduct ongoing customer due diligence in respect of Customer 5.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 5's risk profile

625. On and from 6 August 2017, Customer 5, and the provision of designated services to Customer 5 by SCA, posed higher ML/TF risks because of the following red flags:

a. Customer 5 was a junket operator who facilitated the provision of high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA;

i. between 8 August 2017 and 16 August 2019 SCA recorded that the total cumulative turnover of junkets operated by Customer 5 in the relevant period was $52,993,620;

Particulars

See paragraphs 399 to 401 above.

In the 2018 financial year, SCA recorded that junkets operated by Customer 5 had turnover of $446,900.

Customer 5 operated one of SCEG's top six junkets for the 2019 financial year based on turnover, with an estimated turnover of $460,680,979.

In the 2020 financial year, despite closures related to the COVID-19 pandemic, SCA recorded that junkets operated by Customer 5 had turnover of $52,546,720.

ii. between 7 August 2017 and 30 July 2019, SCA provided Customer 5 and their junket programs with significant amounts of credit upon request, up to limits of $800,000;

Particulars

See paragraphs 321 to 323, and 342 above.

Between 7 August 2017 and 30 July 2019, SCA provided two lines of credit with limits of $500,000 and $800,000 for Customer 5.

iii. Customer 5 operated junkets in private gaming rooms;

Particulars

See paragraph 145(e) above.

Customer 5 operated junkets in private gaming rooms, including the Grange Room.

iv. Customer 5 had one junket representative at SCA; and

v. Customer 5 and their junket representative facilitated the provision of high value designated services to at least five junket players at SCA;

Particulars

See paragraphs 388 and 389 above.

b. designated services provided to Customer 5 lacked transparency as the services were provided through the channel of junket programs at SCA;

Particulars

See paragraph 392 above.

c. SCA held suspicions that the junkets operated by Customer 5 facilitated the provision of high value designated services to organised crime figures;

Particulars

See paragraphs 382 to 418 above.

SCA was aware that there were links between junkets operated by Customer 5 and organised crime figures. One of the organised crime syndicates linked to Customer 5's junket was alleged to have engaged in money laundering at another Australian casino.

d. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 5 by remitting money out of and within the casino environment;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

SCA accepted instructions to transfer funds from Customer 5's accounts for the following transactions:

a. on 17 August 2019, Customer 5 transferred $98,796 from their SCA FMA to their personal bank account; and

b. on 16 April 2021, Customer 5 transferred $25,144 from their SCA FMA to their personal bank account overseas.

Remittances through the SkyCity New Zealand channel

For example, on 6 September 2019, SCA received $30,000 into Customer 5's SCA FMA from a SCEG New Zealand casino. SCA made these funds available to Customer 5.

Remittances from SCA FMAs to SCEG New Zealand FMAs

For example, on 23 November 2019, SCA accepted instructions to transfer $10,000 from Customer 5's SCA FMA to Customer 5's FMA at a SCEG New Zealand casino.

Remittances within the casino environment

SCA accepted instructions to transfer funds from Customer 5's accounts for the following transactions:

a. on 6 August 2017, Customer 5 transferred $75,000 to another customer's SCA FMA; and

b. on 8 August 2017, Customer 5 transferred $34,560 to the same customer's SCA FMA.

e. Customer 5 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

Between 9 August 2017 and 23 April 2021, SCA gave the AUSTRAC CEO five TTRs detailing account withdrawals made by Customer 5 totalling $109,704.

f. in 2018, Customer 5 was the subject of law enforcement enquiries on one occasion at SCA;

Particulars

On 30 November 2018, SCA received a request from a foreign law enforcement agency in relation to an investigation regarding an organised crime syndicate. SCA was aware from this date that some participants on Customer 5's junkets to Australia were linked to organised crime, including alleged money laundering at Australian casinos.

g. Customer 5 had access to private gaming rooms at SCA; and

Particulars

See paragraph 145(e) above.

Customer 5 had access to a private gaming room at SCA, including the Grange Room.

h. SCA did not have adequate reason to believe that Customer 5's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 5 by SCA.

Particulars

See paragraph 516 above.

Customer 5's junket at SCA had a high turnover.

On 6 August 2017, SCA understood Customer 5 's occupation to be as the director of a hotel.

Between 2018 and 2021, SCEG estimated that Customer 5's junket activities with SCEG generated over $3,300,000 in commissions. Customer 5 operated one of SCEG's top six junkets for the 2019 financial year based on turnover, with an estimated turnover of $460,680,979. Despite closures related to the COVID-19 pandemic, Customer 5's junket turnover at SCA alone during the 2020 financial year was estimated at $52,546,720.

By March 2021, SCA was aware that Customer 5's primary source of wealth was the commissions paid to their junket business. SCA expressed doubts about the legitimacy of junket earnings as a source of wealth and did not consider that it held sufficient verified source of wealth information for Customer 5.

SCA was also aware that there were links between junkets operated by Customer 5 and organised crime figures. While SCEG obtained publicly available information about Customer 5's shareholdings, it could not verify the extent and value of those shareholdings. Despite this, SCA did not take appropriate steps to review, update or verify a non-junket source of wealth for Customer 5.

SCA's determination of the ML/TF risks posed by Customer 5

626. SCA was unable to appropriately identify or assess the ML/TF risks posed by Customer 5 because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 5.

a. On and from August 2017, Customer 5 should have been recognised by SCA as a high risk customer for the purpose of the Act and Rules for the reasons pleaded above: see *Customer 5's risk profile.*

Particulars

Sections 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

b. It was not until 13 September 2019 that Customer 5 was rated high risk by SCA for the purpose of the Act and Rules.

Monitoring of Customer 5's transactions

627. At no time did SCA apply appropriate transaction monitoring to Customer 5's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities;

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not make or keep appropriate records of designated services provided to junket operators; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

c. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 5 through:

i. the junket channel; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

ii. the SCA customer account channel and the SkyCity New Zealand channel, which were high risk remittance channels.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 5's KYC information

628. SCA did not review, update or verify Customer 5's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 5, including the nature, extent and purpose of Customer 5's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 5's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 5's risk profile* above, there were real risks that Customer 5's source of wealth and source of funds were not legitimate.

d. to the extent that SCA reviewed Customer 5's KYC information on and from 6 August 2017, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 5.

Particulars

Sections 36(1)(a) and (b) of the Act r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

On 8 August 2017, SCA screened Customer 5's PEP status, and found they were not a PEP.

On 7 September 2019, SCA performed open source searches on Customer 5, which returned information detailing their business interests, including that:

a. Customer 5's junket was a registered business overseas;

b. Customer 5 had a significant shareholding in two overseas companies, with a combined value of over $1,000,000; and

c. the hotel Customer 5 stated they were the Executive Director of was located overseas and not publicly listed.

By December 2019, SCEG had undertaken a review of the KYC information held in relation to the top six junket operators, which included Customer 5, as a result of adverse media regarding casino and junket operations in Australia generally. Despite this, Customer 5's junket operator agreement was renewed by SCEG in January 2020.

Failure to apply appropriate due diligence suited to the high ML/TF risks

629. Had SCA conducted ongoing customer due diligence on and from 6 August 2017 by:

a. appropriately identifying and assessing the ML/TF risks posed by Customer 5;

b. applying appropriate risk-based transaction monitoring to Customer 5; and

c. appropriately reviewing and updating Customer 5's KYC information, having regard to the high ML/TF risks,

SCA would have been required by the Act and Rules to apply the ECDD Program to Customer 5 at a time before the date of the ECDD triggers pleaded below: see *ECDD triggers in respect of Customer 5*.

ECDD triggers in respect of Customer 5

630. SCA was required to apply the ECDD program to Customer 5 following any ECDD triggers in respect of Customer 5.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1) and 15.10 of the Rules.

631. Customer 5 was determined to be high risk by SCA for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 5* above.

632. The matter pleaded at paragraph 631 was an ECDD trigger.

Particulars

See paragraphs 496 and 504 above.

633. SCA did not conduct appropriate risk-based ECDD with respect to Customer 5 following an ECDD trigger because:

a. on each occasion prior to 22 March 2022 that SCA conducted ECDD in respect of Customer 5 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 5 and failed to appropriately consider whether the ML/TF risks posed by Customer 5 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501, 511 and 516 to 517 above.

Between 25 November 2019 and 2 September 2021, SCA conducted ECDD in respect of Customer 5 on a number of occasions, including in December 2019 and January 2020 when Customer 5 applied to renew their junket agreement with a SCEG New Zealand casino.

On 28 April 2021, the ECDD screening in respect of Customer 5 identified that:

a. Customer 5's source of income was their junket business, which was a registered overseas company. Customer 5 was a director of this company and had a 22% shareholding. The junket earned large commissions from both Australian and overseas casinos, including over $3,000,000 from SCEG between 2018 and 2021; and

b. Customer 5 was also a shareholder of a number of other overseas companies and an executive director of an overseas hotel, with personal assets estimated at over $1,700,000. However this information could not be verified.

In December 2019 and January 2020, SCEG conducted ECDD in respect of Customer 5 as part of Customer 5's application to renew their junket agreement with a SCEG New Zealand casino.

In October 2021, SCEG reviewed existing customers who had listed that junket income was their source of income and who potentially intended to visit SCEG properties as individual customers, including Customer 5. These customers were asked to undergo ECDD in anticipation of a future visit as individuals with front money in excess of $1,000,000. There is no further evidence of ECDD being conducted on Customer 5 by SCEG.

SCEG exited the junket market in June 2021. However, it was not until 22 March 2022 that SCA issued a ban in respect of Customer 5 due to their status as a corporate junket operator.

The ECDD conducted by SCA did not have appropriate regard to Customer 5's higher ML/TF risks: see *Customer 5's risk profile* above.

The ECDD conducted by SCA did not have appropriate regarding to the higher ML/TF risks posed by Customer 5's source of funds or source of wealth.

By reason of the matters set out above, there were real risks that Customer 5's source of wealth and source of funds were not legitimate: see *Customer 5's risk profile*

b. on any occasion prior to 22 March 2022 that senior management considered the higher ML/TF risks posed by Customer 5 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 5 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

Customer 5 was mentioned in a 'Transaction Monitoring Overview' report for the period 1 August 2019 to 1 February 2021. The report noted that Customer 5 had a significant front money balance of between $25,000 and $35,000 over this period.

In August 2019, following media reports relating to alleged money laundering at another Australian casino, SCEG reviewed its top six junkets to assess what level of information it held in respect of those persons. Customer 5 operated one of SCEG's top six junkets for the 2019 financial year based on turnover, with an estimated turnover of $460,680,979.

On 4 December 2019, the Audit and Risk Committee considered the findings of this review of SCEG's top six junkets in an AML update paper. The Audit and Risk Committee found that there were some gaps in KYC information for some of those junket operators, and that the AML/CTF Senior Management Group would consider addressing those gaps by seeking additional information from the customers

concerned or engaging an external third party to collect this information.

On 17 May 2021, an internal memorandum from the AML Compliance and Intelligence Manager to the Group GM of Regulatory Affairs and AML concluded that Customer 5 had not sufficiently identified and verified their annual income from their junket business or other sources. SCEG also noted in the memorandum that since November 2018, SCEG had been aware that some participants on Customer 5's junkets in Australia were linked to organised crime and alleged money laundering at Australian casinos.

SCEG exited the junket market in June 2021. However, it was not until 22 March 2022 that SCA issued a ban in respect of Customer 5, due to their status as a corporate junket operator.

Contravention of s 36 of the Act in respect of Customer 5

634. By reason of the matters pleaded at paragraphs 622 to 633 above, on and from 6 August 2017 to 22 March 2022, SCA:

a. did not monitor Customer 5 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

635. By reason of the matters pleaded at paragraph 634, SCA contravened s 36(1) of the Act on and from 1 September 2016 to 22 March 2022 with respect to Customer 5.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 6

636. Customer 6 was a customer of SCA during the relevant period. SCA recorded turnover exceeding $71,000,000 for junkets operated by Customer 6 at SCA during the relevant period.

Particulars

Customer 6 was a customer of SCA from at least 11 March 2019.

On 29 March 2022, SCA issued a ban in respect of Customer 6 at the direction of the AML team.

637. SCA provided Customer 6 with designated services within the meaning of table 1 and table 3, s 6 of the Act during the relevant period including services connected to Customer 6 in their role as a junket operator.

Particulars

On 11 March 2019, SCA opened an FMA for Customer 6 which was closed on 29 March 2022 (item 11, table 3, s 6 of the Act).

Between 8 February 2019 and 10 February 2020, SCA provided lines of credit for Customer 6 on six occasions with a limit ranging from $2,000,000 to $5,000,000 (item 6, table 1, s 6 of the Act).

See *Customer 6's risk profile* below.

638. At all times from 11 March 2019, SCA was required to conduct ongoing customer due diligence in respect of Customer 6.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 6's risk profile

639. On and from 11 March 2019, Customer 6, and the provision of designated services to Customer 6 by SCA, posed higher ML/TF risks because of the following red flags:

a. Customer 6 was a junket operator who facilitated the provision of high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA;

i. between 28 April 2019 and 10 December 2019, Customer 6 operated five junkets at SCA;

Particulars

Between 28 April 2019 and 2 May 2019, Customer 6 operated a junket at SCA.

Between 3 June 2019 and 7 June 2019, Customer 6 operated a junket at SCA.

Between 17 August 2019 and 22 August 2019, Customer 6 operated a junket at SCA.

Between 9 October 2019 and 13 October 2019, Customer 6 operated a junket at SCA.

In early December 2019, Customer 6 operated a junket at SCA.

ii. SCA recorded that the total cumulative turnover of junkets operated by Customer 6 in the relevant period was at least $71,517,734 with buy-ins totalling $10,109,294 and cumulative losses of at least $1,164,230;

Particulars

See paragraphs 399 to 401 above.

The junket that Customer 6 operated between April and May 2019 had a recorded turnover of at least $9,492,400 with losses of at least $549,300.

The junket that Customer 6 operated in June 2019 had a recorded turnover of at least $7,351,800 with wins of at least $118,700.

The junket that Customer 6 operated in August 2019 had a recorded turnover of at least $7,433,500 with losses of at least $780,900.

The junket that Customer 6 operated in October 2019 had a recorded turnover of at least $4,422,000 with wins of at least $379,000.

The junket that Customer 6 operated in December 2019 had a recorded turnover of at least $4,106,600 with losses of at least $292,545.

iii. between 2 May 2019 and 10 December 2019, total benefits of $716,169 were payable to Customer 6 by SCA in their capacity as a junket operator;

Particulars

On 2 May 2019, total benefits of $151,878 were payable to Customer 6 in their capacity as a junket operator which included a commission on junket turnover.

On 7 June 2019, total benefits of $117,628 were payable to Customer 6 in their capacity as a junket operator which included a commission on junket turnover.

On 22 August 2019, total benefits of $208,936 were payable to Customer 6 in their capacity as a junket operator which included a commission on junket turnover and bonus player chips.

On 13 October 2019, total benefits of $122,022 were payable to Customer 6 in their capacity as a junket operator which included a commission on junket turnover, an airfare reimbursement and bonus player chips.

On 10 December 2019, total benefits of $115,705 were payable to Customer 6 in their capacity as a junket operator which included a commission on junket turnover and bonus player chips.

iv. between 8 February 2019 and 10 February 2020, SCA provided significant amounts of credit upon request for Customer 6 and their junket, up to limits of $5,000,000;

Particulars

See paragraphs 321 to 323, and 342 above.

Between February 2019 and December 2019, SCA provided Customer 6 with drawdowns from lines of credit totalling at least $23,000,000. Drawdowns were made on five occasions in amounts of between $3,000,000 and $5,000,000.

On 10 February 2020, SCA provided a line of credit for Customer 6 in the amount of $2,000,000, however, the junket program was subsequently cancelled.

v. Customer 6 operated junkets in private gaming rooms;

Particulars

See paragraph 145(e) above.

Customer 6 operated junkets in private gaming rooms including the Grange Room, the Opal Room, the Platinum Room, the Horizon Room, the Barossa Room, the McLaren Room, VIP Eight and Suite 86.

vi. Customer 6 had seven junket representatives at SCA; and

Particulars

The junket that Customer 6 operated between April and May 2019 had two junket representatives.

The junket that Customer 6 operated in June 2019 had one junket representative.

The junket that Customer 6 operated in August 2019 had one junket representative.

The junket that Customer 6 operated in October 2019 had two junket representatives.

The junket that Customer 6 operated in December 2019 had one junket representative.

vii. Customer 6 and their junket representatives facilitated the provision of high value designated services to at least 15 junket players at SCA;

Particulars

See paragraphs 388 and 389 above.

The junket that Customer 6 operated in December 2019 had two non-gaming visitors in addition to nine junket players.

b. designated services provided to Customer 6 lacked transparency as the services were provided through the channel of junket programs at SCA;

Particulars

See paragraph 392 above.

c. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 6 by remitting large amounts of money into, out of and within the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

SCA made money available to Customer 6 in the following transactions:

a. on 12 March 2019, Customer 6 received $1,353,491 into their SCA FMA from another SCEG casino;

b. on 2 September 2019, SCA reported an incoming telegraphic transfer in the amount of $287,868 where Customer 6 was named as the beneficiary; and

c. on 2 March 2021, SCA reported an incoming telegraphic transfer in the amount of $515,256 where Customer 6 was named as the beneficiary.

SCA accepted instructions to transfer funds from Customer 6's accounts for the following transactions:

a. on 24 June 2019, Customer 6 transferred $700,000 from their SCA FMA to another Australian casino; and

b. on 26 February 2021, Customer 6 transferred $515,256 from their SCA FMA to another Australian casino.

Remittances from SCA FMAs to SCEG New Zealand FMAs

SCA accepted instructions to transfer funds from Customer 6's accounts for the following transactions:

a. on 20 June 2019, Customer 6 transferred $34,451 from their SCA FMA to a SCEG New Zealand casino;

b. on 7 December 2019, Customer 6 transferred $89,152 from their SCA FMA to a SCEG New Zealand casino;

c. on 14 October 2020, Customer 6 transferred $100,000 from their SCA FMA to a SCEG New Zealand casino; and

d. on 2 March 2021, Customer 6 transferred NZD$526,103 from their SCA FMA to a SCEG New Zealand casino.

d. Customer 6 and persons associated with their junket transacted using large amounts of cash and CVIs, and high-value cheques at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 14 March 2019 and 12 March 2021, SCA gave the AUSTRAC CEO 11 TTRs detailing incoming and outgoing payments made by Customer 6 totalling $3,610,380, which comprised:

a. one TTR totalling $10,000 in chip and cash exchanges;

b. one TTR totalling $287,868 in marker redemptions;

c. four TTRs totalling $1,873,651 in account deposits; and

d. five TTRs totalling $1,438,860 in account withdrawals.

Large cash and CVI transactions in 2019

Between 12 March 2019 and 9 December 2019, SCA frequently recorded that Customer 6 conducted significant transactions involving cash and CVIs at SCA including:

a. on 12 March 2019, Customer 6 transferred $1,353,491 into their FMA;

b. on 28 April 2019, SCA issued Customer 6 with a CPV totalling $3,000,000;

c. on 29 April 2019, Customer 6 made a buy-in using a $3,000,000 CPV; and

d. on 1 May 2019, Customer 6 exchanged $2,000,000 in cash for a CPV in the same amount.

Large transactions involving cheques in 2019

Between 28 April 2019 and 9 October 2019, SCA recorded that Customer 6 made significant transactions involving cheques. For example:

a. on 28 April 2019, a cheque for $3,000,000 was deposited into Customer 6's FMA;

b. on 7 June 2019, Customer 6 redeemed a cheque for $3,000,000 at SCA;

c. on 17 August 2019, a cheque for the equivalent of more than $4,900,000 in a foreign currency was deposited into Customer 6's FMA;

d. on 22 August 2019, Customer 6 supplied a cheque for the equivalent of more than $280,000 in a foreign currency; and

e. on 9 October 2019, a cheque for $5,000,000 was deposited into Customer 6's FMA.

e. between 8 February 2019 and 10 February 2020, SCA provided Customer 6 with significant amounts of credit upon request, up to limits of $5,000,000;

Particulars

See paragraphs 321 to 323, and 342 above.

See paragraph 639.a.iv above.

f. during the relevant period, Customer 6's parents, Person 9 and Person 31, were known to SCA as junket operators, and junket players on Customer 6's junket; and

Particulars

Person 31 had been known to SCA as a junket operator of Company 9 since 2004.

SCA was aware that Person 9 was also a junket operator. Person 9 was personally known to the SCEG President of Asian Market and Communications Strategy who in October 2019 stated that they had been doing business with Person 9 for over five years.

The SCEG International Business Executive Vice President stated that they had personally known Person 9 and Person 31 for more than 25 years.

SCA was also aware that Person 9 and Person 31 were both junket players on Customer 6's junkets at SCA during the relevant period.

g. SCA did not have adequate reason to believe that Customer 6's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 6 by SCA.

Particulars

See paragraph 516 above.

During the relevant period, SCA recorded Customer 6's occupation as a junket operator.

Junkets operated by Customer 6 between April 2019 and December 2019 had a recorded turnover exceeding $71,517,000. However, at no time was SCA's understanding of Customer 6's source of wealth commensurate with this high recorded turnover.

On 27 November 2019, SCEG noted that Customer 6's income and source of wealth information was unknown. SCEG observed that there was no public information available regarding Customer 6 or Company 9 and therefore Customer 6's purported connection to Company 9 could not be independently verified.

In November 2020, SCEG recorded that Customer 6 had failed to provide adequate source of wealth information.

SCA's determination of the ML/TF risks posed by Customer 6

640. On 1 April 2019, Customer 6 was appropriately rated by SCA as a high risk customer for the purpose of the Act and Rules.

Particulars

On 1 April 2019, Customer 6 was rated high risk for the purpose of the Act and Rules.

Customer 6's risk rating was lowered to medium risk on 5 December 2019, not being high risk for the purpose of the Act and Rules.

On 6 January 2020, SCA elevated Customer 6's risk rating to high risk, which was high risk for the purpose of the Act and Rules.

On 25 March 2022, Customer 6's risk rating was elevated to significant risk, which was high risk for the purpose of the Act and Rules.

641. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 6 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 6.

Monitoring of Customer 6's transactions

642. At no time did SCA apply appropriate transaction monitoring to Customer 6's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities;

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not make or keep appropriate records of designated services provided to junket operators; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

c. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 6 through:

i. the junket channel; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

ii. the SCA customer account channel, which was a high risk remittance channel.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 6's KYC information

643. SCA did not review, update or verify Customer 6's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 6, including the nature, extent and purpose of Customer 6's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 6's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out above, there were higher ML/TF risks associated with Customer 6's source of wealth or source of funds: see *Customer 6's risk profile* above.

d. to the extent that SCA reviewed Customer 6's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 6.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

ECDD triggers in respect of Customer 6

644. SCA was required to apply the ECDD program to Customer 6 following any ECDD triggers in respect of Customer 6.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1) and 15.10 of the Rules

645. Customer 6 was determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 6* above.

646. The matter pleaded at paragraph 645 was an ECDD trigger.

Particulars

See paragraphs 496 and 504 above.

647. SCA did not conduct appropriate risk-based ECDD with respect to Customer 6 following an ECDD trigger because:

a. on each occasion prior to 29 March 2022 that SCA conducted ECDD in respect of Customer 6 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 6 and failed to appropriately consider whether the ML/TF risks posed by Customer 6 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501, 511 and 516 to 517 above.

On 10 October 2019, SCA conducted ECDD in respect of Customer 6 but did not have appropriate regard to Customer 6's higher ML/TF risks: see *Customer 6's risk profile* above.

The ECDD screening in respect of Customer 6 identified that:

a. Customer 6 had conducted transactions totalling more than $250,000 in one month;

b. Customer 6's occupation, source of funds and source of wealth was as a junket operator; and

c. five of Customer 6's known associates were junket representatives of Customer 6's junkets.

Junkets operated by Customer 6 between April 2019 and December 2019 had recorded turnover exceeding $71,517,000. However, at no time was SCA's understanding of Customer 6's source of wealth commensurate with this high recorded turnover.

SCEG relationship

In November 2019, the SCEG Senior Vice President of International Business in Asia and the SCEG President of Asian Market and Communications Strategy supported and endorsed SCEG's decision to approve a line of credit for Customer 6. In doing so, the SCEG President of Asian Market and Communications Strategy stated that they shared a bond with Customer 6 as they had attended the same university overseas together, and that they had no reservation in continuing the business relationship with Customer 6 and their family.

Database alerts

Between 4 June 2019 and 5 June 2021, SCA received three open source Dow Jones watchlist alerts in respect of Customer 6.

On 19 November 2019, SCA received a Jade rule alert report in respect of Customer 6 but resolved to take no further action following a review conducted by SCA's AML team.

However, it was not until 29 March 2022 that SCA issued a ban in respect of Customer 6.

The ECDD conducted by SCA did not have appropriate regard to Customer 6's higher ML/TF risks: see *Customer 6's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 6's source of funds or source of wealth.

By reason of the matters set out above, there were higher risks associated with Customer 6's source of wealth and source of funds: see *Customer 6's risk profile*.

b. on any occasion prior to 29 March 2022 that senior management considered the higher ML/TF risks posed by Customer 6 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 6 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

Between February 2019 and August 2020, Customer 6 was named in 'Transaction Monitoring Overview' reports which were considered by the AML/CTF Senior Management Group.

In April 2019, the International Business Patron Account Controller at a SCEG New Zealand casino notified SCA senior management that:

a. $3,000,000 in credit had been approved for Customer 6 in preparation for their junket arranged at SCA between 28 April 2019 and 2 May 2019;

b. a particular SCEG New Zealand casino was holding a signed blank personal cheque from Customer 6; and

c. SCA would need to prepare an unsigned counter-cheque for buy-in on the junket.

A document titled 'CCF Risk Matrix – Customer 6' circulated by the International Business Patron Account Controller rated Customer 6 as the highest possible risk for source of wealth, noting that a particular SCEG New Zealand casino had no evidence or information in respect of Customer 6's source of wealth.

On 20 November 2020, a SCEG Commercial Manager provided the SCEG General Manager Regulatory Affairs and AML and an SCA AML Compliance & Intelligence Manager with information regarding:

a. Customer 6's junket operations at other Australian and overseas casinos;

b. Customer 6's stated occupation as a junket operator;

c. the total commission paid to Customer 6 between January 2019 and March 2020; and

d. a property overseas owned by Customer 6's parents which was said to be indicative of their family's wealth.

The SCEG Commercial Manager noted that the Sales Team had encountered strong resistance from Customer 6 in relation to providing source of wealth information, on the basis of confidentiality.

Following this, there are no records demonstrating that SCA senior management conducted any further own due diligence for the purposes of determining whether it was appropriate to continue a business relationship with Customer 6 prior issuing a ban in respect of Customer 6 on 29 March 2022.

SCEG's review of Customer 6

On 27 November 2020, the SCEG Compliance Team requested further information regarding Customer 6's annual income. The SCEG Compliance Team subsequently noted that Customer 6 was

resistant to providing this information and had left most of the Source of Wealth Declaration blank.

On 9 December 2020, the SCEG General Manager Regulatory Affairs and AML advised a SCEG Commercial Manager and an SCA AML Compliance & Intelligence Manager that Customer 6 had not provided any information regarding their source of wealth in Customer 6's Source of Wealth Declaration.

On 18 May 2021, a SCEG Commercial Manager advised the SCEG General Manager Regulatory Affairs and AML that although SCEG had ceased conducting business with customers in their capacity as junket operators, including Customer 6, those individuals would still be able to visit SCEG casinos as an individual.

On 25 March 2022, after SCA had elevated Customer 6's risk rating from high risk to significant risk, an SCA AML Compliance Analyst asked the SCA Chief Operating Officer to determine whether SCA should continue a business relationship with Customer 6. On 27 March 2022, the SCA Chief Operating Officer determined that SCA should discontinue its business relationship with Customer 6.

On 29 March 2022, SCA issued a ban in respect of Customer 6.

Contravention of s 36 of the Act in respect of Customer 6

648. By reason of the matters pleaded at paragraphs 636 to 647 above, on and from 11 March 2019, SCA:

a. did not monitor Customer 6 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

649. By reason of the matters pleaded at paragraph 648, SCA contravened s 36(1) of the Act on and from 1 April 2019 to 29 March 2022 with respect to Customer 6.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 7

650. Customer 7 was a customer of SCA during the relevant period. Between 2018 and 2020, SCA recorded turnover exceeding $8,000,000 for Customer 7 and exceeding $20,000,000 for junkets operated by Customer 7.

Particulars

Customer 7 was a customer of SCA from at least 29 July 2015.

On 22 March 2022, SCA issued a ban in respect of Customer 7 at the direction of the SCA AML team.

651. SCA provided Customer 7 with designated services within the meaning of table 1 and table 3, s 6 of the Act during the relevant period including services connected to Customer 7's role as a junket operator.

Particulars

Before 7 December 2016, SCA opened an FMA for Customer 7 which remained open as at 28 October 2022.

Between 4 February 2018 and 28 November 2019, SCA provided lines of credit for Customer 7 on two occasions each with a limit of $5,000,000.

See *Customer 7's risk profile* below.

652. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 7.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 7's risk profile

653. On and from 7 December 2016, Customer 7, and the provision of designated services to Customer 7 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 7's risk profile prior to the relevant period

a. by 7 December 2016, Customer 7 had the following history:

   i. SCA had formed suspicions for the purposes of s 41 of the Act with respect to Customer 7;

Particulars

On 15 February 2016, SCA gave the AUSTRAC CEO an SMR which reported that Customer 7 had provided approximately $370,050 in chips to two other SCA customers with whom they played regularly and that SCA could not determine whether Customer 7's conduct involved attempts to launder money or to repay funds from previous gambling trips: SMR dated 15 February 2016.

SCA's contemporaneous records identified that chip movement between the three players was a common occurrence.

   ii. Customer 7 was a junket operator who facilitated the provision of high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA;

Particulars

See paragraphs 321 to 323, 342 and 382 to 418 above.

Between 9 June 2015 and 29 April 2016:

a. Customer 7 operated six junkets at SCA, one of which was partly funded by a player on the junket;

b. SCA recorded that the total cumulative turnover of junkets operated by Customer 7 was estimated at $2,220,603,025;

c. total commissions of at least $2,266,854 were payable by SCA to Customer 7 in their capacity as a junket operator;

d. SCA provided Customer 7 and their junket with significant amounts of credit upon request, including at least four lines of credit totalling $23,000,000 with limits of between $3,000,000 and $10,000,000;

e. Customer 7 had seven junket representatives at SCA; and

f. Customer 7 and their junket representatives facilitated the provision of high value designated services to at least 13 junket players at SCA.

iii. Customer 7 received high value financial and gambling services (table 3, s 6 of the Act) at SCA other than through junket programs;

Particulars

Between 1 July 2015 and 30 June 2016, Customer 7's recorded individual rated gambling activity at SCA was estimated as a buy-in of $15,290,490 and a turnover of $308,859,068, with wins of $4,005,570.

iv. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 7 by remitting large amounts of money into, out of and within the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCEG customer account channel

For example, on 26 February 2016, SCEG accepted instructions to transfer $129,784 to Customer 7's personal bank account overseas through an account held by SCEG in a foreign currency.

Remittances through the SCA customer account channel

SCA made money available to Customer 7 in the following transactions:

a. between 11 September 2015 and 29 April 2016, Customer 7 transferred $16,659,751 from their personal bank account in Australia to their SCA FMA;

b. between 29 July 2015 and 14 August 2015, Customer 7 transferred $5,849,721 in a foreign currency from their personal bank account overseas to their SCA FMA; and

c. on 12 February 2016, Customer 7 transferred $50,000 from their FMA held at a SCEG casino to their SCA FMA.

SCA accepted instructions to transfer funds from Customer 7's accounts for the following transactions:

a. on 28 November 2013, Customer 7 transferred $1,256,100 from their SCA FMA to the account of an overseas third party;

b. between 16 August 2015 and 29 April 2016, Customer 7 transferred $7,713,626 from their FMA at SCA to their personal bank account in Australia; and

c. on 4 March 2016, Customer 7 transferred $145,984 from their SCA FMA to their personal bank account overseas. Shortly after this transaction, SCA transferred another $300,000 from Customer 7's FMA at a SCEG casino to their personal bank account overseas.

Remittances through the SkyCity New Zealand channel

SCA made money available to Customer 7 in the following transactions.

On 12 September 2012, SCEG transferred $940,668 to Customer 7's personal account through SCA's account;

On 19 July 2013, SCEG transferred $825,780 to Customer 7's account at another Australian casino through SCA's account;

Between 18 November 2013 and 27 April 2016, SCA credited $18,186,777 to Customer 7's FMA, with these funds originating from Customer 7's SCA FMA held at a SCEG New Zealand casino.

Remittances from SCA FMAs to SCEG New Zealand FMAs

SCA accepted instructions to transfer funds from Customer 7's accounts for the following transactions.

Between 19 November 2013 and 24 February 2016, SCA debited $12,480,029 from Customer 7's SCA FMA with these funds transferred to Customer 7's FMA held at a SCEG New Zealand casino.

v. Customer 7 transacted using large amounts of cash and chips; and

Particulars

See paragraphs 376 to 381 above.

Between 26 November 2013 and 3 May April 2016, SCA gave the AUSTRAC CEO 31 TTRs detailing incoming and outgoing payments made by Customer 7 at SCA totalling $44,129,699, which comprised:

a. eight TTRs totalling $13,821,072 in account deposits and

b. eight TTRs totalling $23,992,884 in account withdrawals;

c. nine TTRs totalling $177,730 in cash and chip exchanges;

d. five TTRs totalling $6,115,756in other cash transactions; and

e. one TTR totalling $22,256 for a cash commission payment.

Between 30 July 2015 and 29 April 2016, Customer 7 deposited a total of $32,357,600 in chips into their FMA at SCA across 14 transactions.

vi. SCA provided Customer 7 with significant amounts of credit upon request, up to limits of $10,000,000;

Particulars

See paragraphs 321 to 323, and 342 above.

See particulars to paragraph 653.a.ii above.

Between 31 January 2015 and 27 April 2016, SCA provided Customer 7 with $15,000,000 in lines of credit, comprised of three lines of credits with limits between $2,000,000 and $5,000,000, including one line of credit on 23 June 2015 with a limit of $5,000,000 with an additional trip limit of $3,000,000.

Customer 7's risk profile from 7 December 2016

b. Customer 7 was a junket operator who facilitated the provision of high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA;

i. between 6 February 2018 and 3 December 2019, Customer 7 operated two junkets at SCA;

Particulars

Between 6 February 2018 and 9 February 2018, Customer 7 operated a junket at SCA.

Between 30 November 2019 and 3 December 2019, Customer 7 operated a junket at SCA.

Both junkets were partly funded by another SCA customer.

ii. SCA recorded that the total cumulative turnover of junkets operated by Customer 7 in the relevant period was at least $20,839,000 with cumulative losses of $237,060;

Particulars

See paragraphs 399 to 401 above.

The junket that Customer 7 operated in February 2018 had a recorded turnover of at least $22,047,000 with wins of at least $764,000.

The junket that Customer 7 operated in November 2019 and December 2019 had a recorded turnover of at least $1,950,000 with losses of at least $727,000.

iii. in the relevant period, total benefits of $293,024 were payable by SCA to Customer 7 in their capacity as a junket operator;

Particulars

On 9 February 2018, total benefits of $283,200 were payable by SCA to Customer 7 in their capacity as a junket operator which included a commission on junket turnover.

On 3 December 2019, total benefits of $9,824 were payable by SCA to Customer 7 in their capacity as a junket operator which included a commission on junket turnover.

iv. between 4 February 2018 and 3 December 2019, SCA provided Customer 7 and their junket with significant amounts of credit upon request, up to limits of $5,000,000;

Particulars

See paragraphs 321 to 323, and 342 above.

On 4 February 2018, SCA provided two lines of credit of $5,000,000 and $3,000,000 for Customer 7's junket that operated in February 2018.

On 28 November 2019, SCA provided a line of credit of $5,000,000 for Customer 7's junket that operated in November 2019 and December 2019.

v. Customer 7 operated junkets in private gaming rooms;

Particulars

See paragraph 145(e) above.

In February 2018, Customer 7 operated junkets in private gaming rooms, including the Barossa Room and the McLaren Room at SCA.

vi. in the relevant period, Customer 7 had five junket representatives at SCA; and

Particulars

The junket that Customer 7 operated in February 2018 had three junket representatives.

The junket that Customer 7 operated in November and December 2019 had two further junket representatives.

vii. Customer 7 and their junket representatives facilitated the provision of high value designated services to at least six junket players at SCA;

Particulars

See paragraphs 388 and 389 above.

The junket that Customer 7 operated in February 2018 had at least six junket players. At settlement, one of the junket players transferred $755,225 to their personal bank account overseas. That junket player had also partly funded the junket.

The junket that Customer 7 operated between November 2019 and December 2019 had at least two junket players. At settlement, Customer 7 deposited $38,224 into their FMA. A junket player transferred $677,017 to their personal bank account. That junket player had also partly funded the junket.

c. designated services provided to Customer 7 lacked transparency as the services were provided through the channel of junket programs at SCA;

Particulars

See paragraph 392 above.

d. Customer 7 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket program. Between 2017 and 2020, SCA recorded a high turnover estimated at $8,262,704 for Customer 7, with cumulative wins of $170,935;

Particulars

Between 1 July 2017 and 30 June 2018, Customer 7's recorded individual gambling activity at SCA was estimated as buy-in of $526,450 and turnover of $6,904,181, with wins of $274,550 on table games.

Between 1 July 2019 and 30 June 2020, Customer 7's recorded individual gambling activity at SCA was estimated as buy-in of $110,450 and turnover of $1,358,523, with losses of $103,615 on table games.

e. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 7 by remitting large amounts of money into, out of and within the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

SCA accepted instructions to transfer funds from Customer 7's accounts for the following transactions:

a. on 17 March 2020, Customer 7 transferred $38,224 from their SCA FMA to their personal bank account in Australia; and

b. on 23 February 2018, Customer 7 transferred $266,773 from their SCA FMA to their account at another Australian casino.

Remittances within the casino environment

For example, on 30 November 2019, Customer 7 received $150,000 into their SCA FMA from another customer's account.

See particulars to paragraph 653.b.vii above

f. Customer 7 transacted using large amounts of cash and chips at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 8 February 2018 and 18 March 2020, SCA gave the AUSTRAC CEO eight TTRs detailing incoming and outgoing payments made by Customer 7 at SCA totalling $922,095, which comprised:

a. one TTR totalling $266,773 for an account deposit;

b. four TTRs totalling $584,571 in account withdrawals; and

c. three TTRs totalling $70,750 in cash and chip exchanges.

Large cash and chip transactions

Between 8 February 2018 and 30 November 2019, Customer 7 deposited a total of $7,705,000 in chips into their FMA at SCA in four transactions.

On 30 November 2019, Customer 7 deposited $1,000 in cash into their SCA FMA. On the same day, Customer 7 also deposited a $9,824 commission that they received from a junket program settlement into their SCA FMA.

g. between 28 January 2017 and 10 February 2017, SCA provided Customer 7 with significant amounts of credit upon request, up to limits of $5,000,000;

Particulars

See paragraphs 321 to 323, and 342 above.

See paragraph 653.b.iv above.

Between 28 January 2017 and 10 February 2017, SCA provided Customer 7 with at least $3,050,000 in lines of credit other than through junket programs, with limits of between $50,000 and $3,000,000.

h. by 2 August 2019, SCA was aware of reports that Customer 7 was associated with another person thought to be connected to criminal activity and who had come under scrutiny at another Australian casino; and

Particulars

On 2 August 2019, SCA identified that Person 10, who was allegedly linked to criminal activity and had come under scrutiny for activity at another Australian casino, had travelled to a SCEG New Zealand casino as part of a junket operated by Customer 7 in November 2014.

i. SCA did not have adequate reason to believe that Customer 7's source of wealth or source of funds were sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 7 by SCA.

Particulars

See paragraph 516 above.

On and from 7 December 2016, SCA recorded that Customer 7 was a property developer.

On and from 23 December 2016, SCA recorded that Customer 7 was also an international junket operator.

It was not until 28 November 2019 that SCA independently verified that Customer 7 operated an international junket business. However, SCA also noted that it did not have any supporting information about Customer 7's finances or assets. Prior to this date, SCA's records indicated that the only evidence that it had in its possession to support Customer 7's claimed occupation was a business card that Customer 7 had provided.

SCA's determination of the ML/TF risks posed by Customer 7

654. SCA was unable to appropriately identify or assess the ML/TF risks posed by Customer 7 because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 7.

a. On and from 7 December 2016, Customer 7 should have been recognised by SCA as a high risk customer for the purpose of the Act and Rules for the reasons pleaded above: see *Customer 7's risk profile* above.

Particulars

Sections 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

b. It was not until 2 March 2018 that Customer 7 was rated high risk by SCA for the purpose of the Act and Rules.

Monitoring of Customer 7's transactions

655. At no time did SCA apply appropriate transaction monitoring to Customer 7's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities;

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not make or keep appropriate records of designated services provided to junket operators; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

c. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 7 through:

i. the junket channel; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

ii. the SCA customer account channel, which was a high risk remittance channel.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 7's KYC information

656. SCA did not review, update or verify Customer 7's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 7, including the nature, extent and purpose of Customer 7's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 7's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters pleaded in *Customer 7's risk profile* above, there were higher ML/TF risks associated with Customer 7's source of wealth and source of funds.

d. to the extent that SCA reviewed Customer 7's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 7.

Particulars

See paragraph 138(h) above.

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

Between 23 December 2016 and 30 January 2018, SCA conducted screening in respect of Customer 7 as part of its assessment of Customer 7's credit applications. This process focussed on Customer 7's creditworthiness rather than their ML/TF risks.

SCA's records indicate that it did not perform AML/CTF screening in respect of Customer 7 between 7 December 2016 and 2 March 2018 beyond identifying that they were a junket operator, conducting open source media searches that identified no relevant information and recording its belief that Customer 7 had been referred to SCA by a "reputable source" that Customer 7's "ability to pay" had been verified.

On 6 February 2018, SCA conducted watchlist screening in respect of Customer 7 and identified no adverse information.

The due diligence conducted by SCA in respect of Customer 7 did not have appropriate regard to the higher ML/TF risks posed by Customer 7 and their source of funds or source of wealth: see *Customer 7's risk profile* above.

Failure to apply appropriate due diligence suited to the high ML/TF risks

657. Had SCA conducted ongoing customer due diligence on and from 7 December 2016 by:

a. appropriately identifying and assessing the ML/TF risks posed by Customer 7;

b. applying appropriate risk-based transaction monitoring to Customer 7; and

c. appropriately reviewing and updating Customer 7's KYC information, having regard to the high ML/TF risks,

SCA would have been required by the Act and Rules to apply the ECDD Program to Customer 7 at a time before the date of the ECDD trigger pleaded below: see *ECDD triggers in respect of Customer 7*.

ECDD triggers in respect of Customer 7

658. SCA was required to apply the ECDD program to Customer 7 following any ECDD triggers in respect of Customer 7.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1) and 15.10 of the Rules.

659. Customer 7 was determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

On 2 March 2018, SCA determined that the ML/TF risk posed by Customer 7 was high risk for the purpose of the Act and Rules: see *SCA's determination of the ML/TF risks posed by Customer 7* above.

660. The matter pleaded at paragraph 659 was an ECDD trigger.

Particulars

See paragraphs 496 and 504 above.

661. SCA did not conduct appropriate risk-based ECDD with respect to Customer 7 following the ECDD trigger because:

a. on each occasion prior to 22 March 2022 that SCA conducted ECDD in respect of Customer 7 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 7 and failed to appropriately consider whether the ML/TF risks posed by Customer 7 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501, 511 and 516 to 517 above.

Between 2 March 2018 and 23 December 2021, SCA conducted ECDD in respect of Customer 7 but did not have appropriate regard to the higher ML/TF risks posed by Customer 7 and their source of funds and source of wealth: see *Customer 7's risk profile* above.

Between 1 July 2017 and 30 June 2020, Customer 7 recorded individual rated gaming turnover at SCA exceeding $8,260,000. Junkets operated by Customer 7 between February 2018 and December 2019 had a recorded turnover exceeding $20,000,000. However, at no time was SCA's understanding of Customer 7's source of wealth and source of funds commensurate with this high recorded turnover.

At no point did SCA have adequate reason to believe that Customer 7's source of wealth and source of funds were sufficient to explain the high value financial and gambling services they received at SCA. At no point did SCA verify Customer 7's income, or verify that Customer 7 was actually a property developer as they claimed.

By 2019, SCA was also aware of reports that Customer 7 was associated with another person thought to be connected to criminal activity and who had come under scrutiny at another Australian casino.

This conduct took place against a background where Customer 7 had operated junkets at SCA since 9 June 2015, and those junkets had recorded extremely high turnover. For example, by 7 December 2016, SCA recorded that the turnover for Customer 7's junkets exceeded $2,220,000,000.

Database alerts

Between 22 March 2018 and 2 December 2021, SCA received four open source Dow Jones watchlist alerts and 16 transaction alerts in respect of Customer 7 but resolved to take no further action following a manual review conducted by SCA's AML team.

Credit screening

Between 28 November 2019 and 4 March 2020, SCA conducted screening in respect of Customer 7 as part of its assessment of Customer 7's credit applications. This process focussed on Customer 7's creditworthiness rather than their ML/TF risks.

During this screening, SCA independently verified that Customer 7 operated an international junket business, although it did not have any supporting information about their finances or assets. It also conducted open source media searches that identified no relevant matches.

ECDD screening

On 24 April 2019, SCA conducted ECDD screening in respect of Customer 7. The screening consisted of:

a. a review of Customer 7's source of funds, source of wealth and occupation. SCA recorded Customer 7's occupation as a property manager and junket operator. However, SCA did not record the income that Customer 7 derived from these occupations, or identify how it understood that Customer 7 held these occupations, besides attaching a photograph of a junket business card that Customer 7 had provided;

b. a review of Customer 7's known associates;

c. a review of open source information in respect of Customer 7; and

d. SCA concluded that it could not identify any adverse information in relation to Customer 7.

On 23 December 2021, SCA conducted ECDD in respect of Customer 7. This screening consisted of:

a. a review of Customer 7's source of wealth, source of funds and occupation. SCA verified that Customer 7 conducted international junket operations from ABN searches, third party credit reports, and a business card that Customer 7 had provided to SCA. However, SCA did not record Customer 7's income, and its records indicated that it did not take any steps to verify that Customer 7 was actually a property developer, as it had previously recorded;

b. Customer 7's gaming history; and

c. Customer 7's known associates.

It was not until 22 March 2022 that SCA issued a ban in respect of Customer 7 on the basis that they were a commercial junket operator.

The ECDD conducted by SCA did not have appropriate regard to Customer 7's higher ML/TF risks: see *Customer 7's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 7's source of funds or source of wealth.

By reason of the matters set out above, there were higher ML/TF risks associated with Customer 7's source of wealth and source of funds: see *Customer 7's risk profile* above.

b. At no time prior to February 2022 did senior management consider the higher ML/TF risks posed by Customer 7 in response to an ECDD trigger, or appropriately consider whether the ML/TF risks posed by Customer 7 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

On or around 21 February 2022, SCA's AML/CTF team determined that Customer 7 should be banned from SCA's premises on the basis that they were a commercial junket operator who operated junkets as a business.

The last junket that Customer 7 operated at SCA ended on 3 December 2019: see *Customer 7's risk profile* above.

On or around 21 March 2022, the SCA AML/CTF General Manager requested approval from the SCA Chief Operating Officer to issue a ban in respect of Customer 7 on the basis that Customer 7 was a commercial junket operator.

On 22 March 2022, SCA issued a ban in respect of Customer 7.

Contravention of s 36 of the Act in respect of Customer 7

662. By reason of the matters pleaded at paragraphs 650 to 661 above, from 7 December 2016, SCA:

a. did not monitor Customer 7 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

663. By reason of the matters pleaded at paragraph 662, SCA contravened s 36(1) of the Act from 7 December 2016 to 22 March 2022 with respect to Customer 7.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 8

664. Customer 8 was a customer of SCA during the relevant period. Between December 2018 and March 2022, SCA recorded turnover exceeding $42,000,000 for junkets operated by Customer 8.

Particulars

Customer 8 was a customer of SCA from at least 28 December 2018.

On 31 March 2022, SCA issued a ban in respect of Customer 8 at the direction of the AML team.

665. SCA provided Customer 8 with designated services within the meaning of table 1 and table 3, s 6 of the Act during the relevant period including services connected to Customer 8's role as a junket operator.

Particulars

On 28 December 2018, SCA opened an FMA for Customer 8 which was closed on 31 March 2022 (item 11, table 3, s 6 of the Act).

On 9 April 2019 and 21 May 2019, SCA provided lines of credit for Customer 8 with a limit $2,000,000 (item 6, table 1, s 6 of the Act).

See *Customer 8's risk profile* below.

666. At all times from 28 December 2018, SCA was required to conduct ongoing customer due diligence in respect of Customer 8.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 8's risk profile

667. On and from 28 December 2018, Customer 8, and the provision of designated services to Customer 8 by SCA, posed higher ML/TF risks because of the following red flags:

a. Customer 8 was a junket operator who facilitated the provision of high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA;

   i. between 21 May 2019 and 26 May 2019, Customer 8 operated a junket at SCA;

   ii. SCA recorded that the total cumulative turnover of the junket operated by Customer 8 in the relevant period was $42,371,570;

Particulars

In 2019, SCA recorded that the junket operated by Customer 8 had a buy-in of $5,000,000, turnover of $42,371,570 with wins of $5,414,600.

   iii. total benefits of $63,800 were payable by SCA to Customer 8 in their capacity as a junket operator;

Particulars

In 2019, total benefits of $63,800 were payable by SCA to Customer 8 in their capacity as a junket operator which included complimentary services and non-gaming complimentary services such as hotel rooms, food and beverage.

iv. on 9 April 2019 and 21 May 2019, SCA provided Customer 8 and their junket program with a significant amount of credit upon request, up to a limit of $2,000,000;

Particulars

See paragraphs 321 to 323, and 342 above.

v. Customer 8 operated junkets in private gaming rooms;

Particulars

See paragraph 145(e) above.

Customer 8 operated junkets in private gaming rooms, including the Horizon Suites and Salon 88.

vi. Customer 8 had two junket representatives at SCA; and

vii. Customer 8 and their junket representatives facilitated the provision of high value designated services to five junket players at SCA;

Particulars

See paragraphs 388 and 389 above.

On 26 May 2019, a junket player on Customer 8's junket program, Person 11, removed plaques totalling $6,300,000 from a safe in Salon 88 and deposited them into Customer 8's SCA FMA. A few hours later, Customer 8's junket made a buy-in at a gaming table for $6,300,000, which was issued in plaques. Person 11 took the plaques and placed the plaques back in the safe.

b. designated services provided to Customer 8 lacked transparency as the services were provided through the channel of junket programs at SCA;

Particulars

See paragraph 392 above.

c. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 8 by remitting large amounts of money into and out of the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCEG customer account channel

On 11 June 2019, SCA accepted instructions to transfer $2,091,482 from their account to a SCEG New Zealand casino on behalf of Customer 8. These funds were Customer 8's winnings from the

junket program they operated at SCA. On 12 June 2019, the SCEG New Zealand casino transferred the funds from their Cage account to Customer 8's personal bank account overseas on behalf of SCA. SCA had the SCEG New Zealand casino transfer the funds to Customer 8's personal bank account overseas because Customer 8 wanted the funds to be sent in a foreign currency and this could not be done by SCA itself.

This transaction reflects a complex transaction chain involving the remittance of money, and carried a number of ML/TF risks: see paragraphs 382 to 418 above.

Remittances through the SkyCity New Zealand channel

SCA made money available to Customer 8 in the following transactions.

On 28 December 2018, SCA credited $1,000,867 to Customer 8's SCA FMA, with these funds originating from Customer 8's FMA held at a SCEG New Zealand casino. The funds had been won as part of a junket program that Customer 8 had operated at that the SCEG New Zealand casino. After being deposited in Customer 8's SCA FMA, the funds were cashed out at SCA by Customer 8's personal assistant, Person 16.

d. Customer 8 was connected to other customers at SCA, including, players who posed higher ML/TF risks, such as Customer 20, and players who SCA considered had acted suspiciously;

Particulars

For example, SCA recorded in its iTrak system that Customer 20 was a known associate of Customer 8.

See particulars to paragraphs 667.a and 667.g.

e. Customer 8, and persons associated with their junket, transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 2 January 2019 and 17 June 2019, SCA gave the AUSTRAC CEO four TTRs detailing outgoing payments made by Customer 8 totalling $3,174,755 which comprised:

a. one TTR totalling $42,400 for a chip and cash exchange; and

b. three TTRs totalling $3,132,355 in account withdrawals.

Large and suspicious cash transactions in 2019

On 22 May 2019, a customer on Customer 8's junket withdrew $60,000 in cash from Customer 8's SCA FMA. The cash withdrawal

was approved by the SCEG Group General Manager International Gaming.

f. on 9 April 2019 and 21 May 2019, SCA provided Customer 8 with a significant amount of credit upon request, up to a limit of $2,000,000;

Particulars

See paragraphs 321 to 323, and 342 above.

See paragraph 667.a.iv above.

g. by July 2019, media reports stated that Person 11 brought proceedings against Customer 8 and Person 10 in relation to the junket Customer 8 operated in May 2019 at SCA; and

Particulars

In July 2019, a media article reported that Person 11 accused Person 10 in an Australian court of misappropriating their junket winnings at SCA. The dispute related to the junket that Customer 8 had operated in May 2019 at SCA.

In March 2021, media articles reported that Person 11 had brought proceedings in an Australian court against Customer 8 and Person 10 for fraud, and against SCA for negligence and breach of trust. The proceedings related to the above dispute.

h. SCA did not have adequate reason to believe that Customer 8's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 8 by SCA.

Particulars

See paragraph 516 above.

On 28 December 2018, Customer 8 provided SCA with details of their occupation. Customer 8 informed SCA that their occupation was a junket operator. Customer 8 also provided a business card which suggested that they were the Chief Executive Officer of an overseas company.

In April 2019, Customer 8 had stated in a credit application that they were the Chief Executive Officer of a different overseas company. As part of its review of Customer 8's credit application, SCEG recorded that Customer 8's annual income or salary was unknown, it had no other source of wealth or source of funds information in respect of Customer 8 that was publicly available.

As part of its review of Customer 8's credit application in May 2019, SCEG recorded that Customer 8's company had not listed its key executives or made its financial statements available online, and there was limited information that was publicly available as to Customer 8's connection to the company.

On or around 25 February 2021, SCA conducted an open source search on Customer 8 which identified that:

a. Customer 8 was the Chief Executive Officer of a company that ran a junket business overseas; and

b. Customer 8 was the shareholder, legal representative and Chief Executive Officer of another overseas company. This other overseas company was primarily involved in providing financial guarantees for enterprises. Based on the company's registered capital, SCA estimated that Customer 8's equity portion in the company was approximately NZD$440,000.

At no time did SCA request source of funds or source of wealth information from Customer 8.

SCA's determination of the ML/TF risks posed by Customer 8

668. On and from 21 May 2019, Customer 8 was appropriately rated by SCA as a high risk customer for the purpose of the Act and Rules.

Particulars

On or around 14 October 2021, Customer 8 was rated significant risk, which was high risk for the purpose of the Act and Rules.

669. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 8 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 8.

Monitoring of Customer 8's transactions

670. At no time did SCA apply appropriate transaction monitoring to Customer 8's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities;

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not make or keep appropriate records of designated services provided to junket operators; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

c. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 8 through:

i. the junket channel; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

ii. the SCEG customer account channel and the SkyCity New Zealand channel, which were high risk remittance channels.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 8's KYC information

671. SCA did not review, update or verify Customer 8's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 8, including the nature, extent and purpose of Customer 8's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 8's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters pleaded in *Customer 8's risk profile* above, there were higher ML/TF risks associated with Customer 8's source of wealth or source of funds.

d. to the extent that SCA reviewed Customer 8's KYC information on and from 28 December 2018, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 8.

Particulars

Sections 36(1)(a) and (b), r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

ECDD triggers in respect of Customer 8

672. SCA was required to apply the ECDD program to Customer 8 following any ECDD triggers in respect of Customer 8.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1) and 15.10 of the Rules.

673. Customer 8 was determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 8* above.

674. The matter pleaded at paragraph 673 was an ECDD trigger.

Particulars

See paragraphs 496 and 504 above.

675. SCA did not conduct appropriate risk-based ECDD with respect to Customer 8 following an ECDD trigger because:

a. on each occasion prior to 31 March 2022 that SCA conducted ECDD in respect of Customer 8 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 8 and failed to appropriately consider whether the ML/TF risks posed by Customer 8 were within SCA's ML/TF risk appetite; and

Particulars

Rule 15.10 of the Rules.

See paragraphs 501, 511 and 516 to 517 above.

Watchlist screenings

On four occasions between 27 December 2018 and 20 May 2019, SCA conducted a watchlist screening in respect of Customer 8.

Transaction reviews

On 3 June 2019, SCA surveillance staff conducted a review of Person 11's transactions on 26 May 2019, involving Customer 8's junket. The SCA General Manager Legal, Compliance & Regulatory Affairs was informed of the findings: see particulars to paragraph 667.a.vii above.

Credit application

In April 2019 and May 2019, SCEG conducted ECDD screening in respect of Customer 8 as part of its assessment of Customer 8's credit applications. This screening included reviews of:

a. Customer 8's gaming and credit history;

b. previous lines of credit that had been issued to Customer 8, both at SCEG casinos and other casinos;

c. Customer 8's occupation; and

d. "derogatory information" in respect of Customer 8.

On both occasions, SCEG rated Customer 8 as medium/moderate risk and determined to grant Customer 8's applications for credit. However, the consideration of these credit applications was largely focussed on credit risk rather than ML/TF risks.

There are no records of SCA conducting its own due diligence for the purposes of considering whether it was within its own ML/TF risk appetite to provide designated services to Customer 8, including lines of credit: see paragraphs 382 to 418 above.

ECDD screenings

On 31 October 2019 and 23 January 2020, SCA conducted ECDD in respect of Customer 8. The ECDD conducted by SCA did not have appropriate regard to Customer 8's higher ML/TF risks: see *Customer 8's risk profile* above.

On 25 February 2021, SCA prepared a document on Customer 8 and the other SCA customers involved in legal proceedings brought by Person 11, including Person 10 and Person 11. As part of the preparation of this document, SCA conducted an open source search on Customer 8 which identified information relating to Customer 8's occupation and source of wealth: see *Customer 8's risk profile* above.

On 14 October 2021, SCA conducted ECDD in respect of Customer 8. The screening recorded that:

a. under instructions from the SCEG Group General Manager International Gaming, Customer 8 (along with other SCA customers) was considered "SkyCity undesirable" and was not permitted to game at SCEG casinos; and

b. open source information served to elevate Customer 8 as a person of interest, as they were named in legal proceedings with SCA and Person 11. The ECDD screening identified a number of media articles which had reported on the proceedings.

As a result of the open source information and other documentation considered, SCA escalated Customer 8's risk rating to significant risk. SCA also recommended that Customer 8's business relationship with SCA be terminated.

It was not until 31 March 2022 that SCA issued a ban in respect of Customer 8.

The ECDD conducted by SCA did not have appropriate regard to Customer 8's higher ML/TF risks: see *Customer 8's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 8's source of funds or source of wealth.

By reason of the matters set out in *Customer 8's risk profile* above, there were higher risks associated with Customer 8's source of wealth and source of funds.

b. on any occasion prior to 31 March 2022 that senior management considered the higher ML/TF risks posed by Customer 8 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 8 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

On 3 January 2019, an SCA AML Adviser notified the SCA General Manager Legal, Compliance & Regulatory Affairs and the SCEG AML Compliance and Intelligence Manager of a large transfer by Customer 8 from a SCEG New Zealand casino to SCA: see particulars to paragraph 667.c above. The SCEG AML Compliance and Intelligence Manager stated that they were not concerned about the transfer because the funds appeared to be genuine winnings, and the transfer was between parties with a known relationship.

On 2 February 2020, the SCEG Group General Manager International Gaming determined that Customer 8 was an undesirable junket operator and was not permitted to engage in gaming at SCEG casinos.

In November 2019, March 2021, April 2021 and May 2021, the legal proceedings brought by Person 11 against Customer 8 and SCA were noted in SCEG's Legal and Regulatory Affairs Update meeting. SCA directors attended these meetings.

It was not until 31 March 2022 that SCA issued a ban in respect of Customer 8.

Contravention of s 36 of the Act in respect of Customer 8

676. By reason of the matters pleaded at paragraphs 664 to 675 above, on and from 28 December 2018, SCA:

a. did not monitor Customer 8 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

677. By reason of the matters pleaded at paragraph 676, SCA contravened s 36(1) of the Act on and from 28 December 2018 to 31 March 2022 with respect to Customer 8.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 9

678. Customer 9 was a customer of SCA during the relevant period. Between 25 August 2017 and 28 August 2017, SCA recorded turnover exceeding $31,400,000 for a junket operated by Customer 9.

Particulars

Customer 9 was a customer of SCA from at least 24 August 2017.

On 22 March 2022, SCA issued a ban in respect of Customer 9 at the direction of the SCA AML team due to Customer 9's association with Customer 14.

679. SCA provided Customer 9 with designated services within the meaning of table 1 and table 3, s 6 of the Act during the relevant period including services connected to Customer 9's role as a junket operator.

Particulars

On 24 August 2017, SCA opened an FMA for Customer 9 (item 11, table 3, s 6 of the Act).

While a customer of SCA, Customer 9 remitted funds to their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 9's risk profile* below.

680. At all times from 24 August 2017, SCA was required to conduct ongoing customer due diligence in respect of Customer 9.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 9's risk profile

a. Customer 9 was a junket operator who facilitated the provision of high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA;

   i. between 26 August 2017 and 28 August 2017, Customer 9 operated a junket at SCA;

   ii. SCA recorded that the total cumulative turnover of the junket operated by Customer 9 in in August 2017 was $31,444,102 with losses of $1,686,520;

   iii. total benefits of $230,782 were payable to Customer 9 by SCA in their capacity as a junket operator;

   iv. Customer 9 operated junkets in private gaming rooms;

Particulars

See paragraph 145(e) above.

Customer 9 operated junkets private gaming rooms, including Suite 86 and Suite 89.

v. Customer 9 had one junket representative at SCA; and

vi. Customer 9 and their junket representative facilitated the provision of high value designated services to seven junket players at SCA including players who posed higher ML/TF risks such as Customer 14;

Particulars

See paragraphs 388 and 389 above.

b. designated services provided to Customer 9 lacked transparency as the services were provided through the channel of junket programs at SCA;

Particulars

See paragraph 392 above.

c. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 9 by remitting large amounts of money into the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

For example, on 24 August 2017, Customer 9 received $3,000,000 into their SCA FMA from another Australian casino for use as front money for a junket they operated. SCA made the funds available to Customer 9.

d. Customer 9 was connected to other customers at SCA, including junket players, foreign PEPs, customers who posed higher ML/TF risks such as Customer 11 and Customer 14, and customers who SCA considered had acted suspiciously;

Particulars

From 26 August 2017 to 28 August 2017, the main players on the junket operated by Customer 9 were Customer 11 and Customer 14.

By October 2016, media reports named Customer 14 as the most lucrative private junket provider at another Australian casino. Customer 14 had previously been excluded from SCEG casinos due to behavioural issues at other Australian casinos. Due to this previous exclusion, Customer 14's visit on Customer 9's 2017 junket program was approved personally by the President of International Business: see *Customer 14's risk profile* below.

From November 2016, SCA held suspicions with respect to Customer 11 and their repeated attempts to disguise the source and beneficiary of funds, which were reported in the SMRs given to the AUSTRAC CEO on a number of occasions.

In September 2020, Customer 9 was named in public inquiries into another Australian casino as a junket operator associated with the junket operated by Customer 14, including because the junkets

operated by Customer 9 and Customer 14 shared a junket representative.

By February 2022, SCA was aware that Customer 9 was on board a private jet with Customer 14 and Customer 11 which had been searched by a law enforcement agency in connection with suspicions of money laundering.

On 22 March 2022, SCA issued a ban in respect of Customer 9 at the direction of the SCA AML team due to Customer 9's association with Customer 14.

Customer 11's risk profile above*, Customer 14's risk profile* below*.*

e. Customer 9 transacted using large amounts of cash at SCA; and

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 28 August 2017 and 29 August 2017, SCA gave the AUSTRAC CEO six TTRs detailing outgoing payments made by Customer 9 totalling $541,882, which comprised:

a. five TTRs totalling $505,250 in chip and cash exchanges; and

b. one TTR totalling $36,632 in account withdrawals.

f. SCA did not have adequate reason to believe that Customer 9's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 9 by SCA.

Particulars

See paragraph 516 above.

In August 2017, SCA recorded Customer 9's occupation as Assistant Manager of a foreign company, but did not verify those details.

From 2017, Customer 9's gambling activity was not consistent with SCA's understanding of their source of wealth.

SCA's determination of the ML/TF risks posed by Customer 9

681. SCA was unable to appropriately identify or assess the ML/TF risks posed by Customer 9 because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 9.

a. On and from 24 August 2017, Customer 9 should have been recognised by SCA as a high risk customer for the purpose of the Act and Rules for the reasons pleaded above: see *Customer 9's risk profile.*

Particulars

Sections 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

b. At no time was Customer 9 rated high risk for the purpose of the Act and Rules by SCA.

Monitoring of Customer 9's transactions

682. At no time did SCA apply appropriate transaction monitoring to Customer 9's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities;

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not make or keep appropriate records of designated services provided to junket operators; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

c. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 9 through:

i. the junket channel; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

ii. the SCA customer account channel, which was a high risk remittance channel.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 9's KYC information

683. SCA did not review, update or verify Customer 9's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 9, including the nature, extent and purpose of Customer 9's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 9's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 9's risk profile* above, there were real risks that Customer 9's source of wealth and source of funds were not legitimate.

d. to the extent that SCA reviewed Customer 9's KYC information on and from 24 August 2017, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 9.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

Failure to apply appropriate due diligence suited to the high ML/TF risks

684. Had SCA conducted ongoing customer due diligence on and from 24 August 2017 by:

a. appropriately identifying and assessing the ML/TF risks posed by Customer 9;

b. applying appropriate risk-based transaction monitoring to Customer 9; and

c. appropriately reviewing and updating Customer 9's KYC information, having regard to the high ML/TF risks;

SCA would likely have rated Customer 9 as a high risk customer for the purpose of the Act and Rules at a time before 22 March 2022 when Customer 9 was issued with a ban at SCA.

Particulars

Section 36(1)(a) of the Act.

Rules 15.2 and 15.5 of the Rules

685. Had SCA rated Customer 9 as a high risk customer for the purpose of the Act and Rules, it would have been required by the Act and Rules to apply the ECDD Program to Customer 9 at a time before 22 March 2022 when Customer 9 was issued with a ban at SCA.

Particulars

Rules 15.9 of the Rules.

Contravention of s 36 of the Act in respect of Customer 9

686. By reason of the matters pleaded at paragraphs 678 to 685 above, on and from 24 August 2017, SCA:

a. did not monitor Customer 9 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2 and 15.5 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

687. By reason of the matters pleaded at paragraph 686, SCA contravened s 36(1) of the Act on and from 24 August 2017 to 22 March 2022 with respect to Customer 9.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 10

688. Customer 10 was a customer of SCA during the relevant period. Between 2018 and 2019, SCA recorded turnover exceeding $1,100,000 for Customer 10's individual rated gambling activity and junkets operated by Customer 10.

Particulars

Customer 10 was a customer of SCA from at least 21 December 2013.

On 29 March 2022, SCA issued a ban in respect of Customer 10 at the direction of the AML team.

689. SCA provided Customer 10 with designated services within the meaning of table 1 and table 3, s 6 of the Act during the relevant period including services connected to Customer 10's gambling as a junket player, facilitated through one junket operator, and role as a junket operator and a junket representative.

Particulars

Prior to 2015, SCA opened an FMA for Customer 10 which was closed on 29 March 2022 (item 11, table 3, s 6 of the Act).

While a customer of SCA, Customer 10 remitted funds to and from their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 10's risk profile* below.

690. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 10.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 10's risk profile

691. On and from 7 December 2016, Customer 10, and the provision of designated services to Customer 10 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 10's risk profile prior to the relevant period

a. by 7 December 2016, Customer 10 had the following risk history:

   i. Customer 10 was a junket player who received gambling services (table 3, s 6 of the Act) at SCA through junket programs; and

Particulars

Between 20 March 2016 and 24 March 2016, Customer 10 was a junket player on and a junket representative for a junket at SCA.

At no time did SCA record Customer 10's individual gambling activity on junket programs they attended as a junket player.

   ii. Customer 10 received gambling services (table 3, s 6 of the Act) at SCA other than through junket programs;

Particulars

Between 2013 and 2015, Customer 10's recorded individual rated gambling activity for table games at SCA was estimated as a buy-in of $50,065, turnover of $123,305 and with losses of $17,040.

Customer 10's risk profile during the relevant period

b. Customer 10 was a junket operator who facilitated the provision of high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA. Between 27 April 2019 and 1 May 2019, Customer 10 operated one junket at SCA. SCA recorded that the total cumulative turnover of the junket operated by Customer 10 in the relevant period was $965,900 with wins of $28,200;

   i. between 27 April 2019 and 1 May 2019, total benefits of $15,454 were payable to Customer 10 by SCA in their capacity as a junket operator;

Particulars

In 2019, total benefits of $15,454 were payable to Customer 10 in their capacity as a junket operator which included a commission on junket turnover.

   ii. Customer 10 operated junkets in private gaming rooms;

Particulars

See paragraph 145(e) above.

   iii. Customer 10 had one junket representative at SCA; and

   iv. Customer 10 and their junket representative facilitated the provision of high value designated services to three junket players at SCA;

Particulars

See paragraphs 388 and 389 above.

c. Customer 10 was a junket player who received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA through a junket program;

i. between 21 January 2020 and 28 January 2020, Customer 10 was a junket player on and a junket representative for one junket at SCA operated by one operator, Person 12; and

ii. at no time did SCA record Customer 10's individual gambling activity on the junket program they attended as a junket player;

d. designated services provided to Customer 10 lacked transparency as the services were provided through the channel of junket programs at SCA;

Particulars

See paragraph 392 above.

e. Customer 10 received financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs;

i. between 2018 and 2019, SCA recorded turnover estimated at $190,360 for Customer 10, with cumulative losses of $19,200;

Particulars

In 2018, Customer 10's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $62,700, turnover of $178,043 with losses of $21,200.

In 2019, Customer 10's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $40,300, turnover of $12,317 with wins of $2,000.

f. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 10 by remitting large amounts of money into, out of and within the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCEG customer account channel

SCA made money available to Customer 10 in the following transactions.

Between 23 April 2019 and 26 April 2019, a total of $500,000 was transferred to SCA for the benefit of Customer 10 through the SCEG Customer account channel.

a. On 23 April 2019, $272,254 was deposited into an account held by SCEG in Australia on behalf of Customer 10, which SCA made available to Customer 10 and which was used as a buy-in for the junket operated by Customer 10 at SCA.

b. On 26 April 2019, $227,746 was deposited into an account held by SCEG in Australia on behalf of Customer 10, which SCA made available to Customer 10 and which was used as a buy-in for the junket operated by Customer 10 at SCA.

Remittances through the SCA customer account channel

SCA made money available to Customer 10 in the following transactions.

Between 16 September 2019 and 21 January 2020, Customer 10 received a total of $1,553,000 into their SCA FMA from another Australian casino:

a. On 16 September 2019, Customer 10 received $500,000 into their SCA FMA from the other casino. Customer 10 then transferred the funds from their SCA FMA to Person 12's SCA FMA.

b. On 30 September 2019, Customer 10 received $50,000 into their SCA FMA from the other casino. These funds were then transferred to Person 12, and were used for a junket program buy-in.

c. On 4 November 2019, Customer 10 received $488,000 into their SCA FMA from the other casino. These funds were then transferred to Person 12 and were used for a junket program buy-in.

d. On 15 November 2019, Customer 10 received $490,000 into their SCA FMA from the other casino.

e. On 21 January 2020, Customer 10 received $25,000 into their SCA FMA from the other casino. On the same day, Customer 10 transferred a total of $81,537 to Person 12's SCA FMA. At this time, Customer 10 was the authorised junket representative and a junket player on the operator's junket at SCA.

SCA accepted instructions to transfer funds from Customer 10's accounts for the following transactions:

a. on 2 January 2019, SCA transferred $500 from its bank account to an unknown account on behalf of Customer 10; and

b. on 2 May 2019, following the settlement of their junket program, Customer 10 transferred $512,896 from their SCA FMA to their bank account.

Remittances through the SkyCity New Zealand channel

On 21 January 2020, SCA credited $15,600 to Customer 10's FMA with these funds originating from Customer 10's FMA held at a SCEG New Zealand casino. SCA made the funds available to Customer 10.

Remittances within the casino environment

SCA made money available to Customer 10 in the following transactions.

On 5 September 2019, Customer 10 received $100,000 into their SCA FMA from another SCA customer. This customer had been a

junket player on the junket Customer 10 operated at SCA in April 2019. The funds were then immediately transferred from Customer 10's SCA FMA to another Australian casino. SCA was informed that the reason for the transfer was that the junket player was playing on a junket program being operated by Customer 10 at the other casino.

On 11 October 2019, Customer 10 received $400,000 from a junket operator, Person 12's SCA FMA. These funds were returned to Customer 10 after they had transferred the junket operator $500,000 on 16 September 2019 for a junket buy-in, and the junket player on the program had only used $100,000. Customer 10 then transferred the funds to another Australian casino.

On 27 November 2019, Customer 10 received $580,589 into their SCA FMA from Person 12's SCA FMA. On 28 November 2019, Customer 10 transferred the funds from their SCA FMA to their account at another Australian casino.

On 10 February 2020, Customer 10 received $551,684 into their SCA FMA from Person 12's SCA FMA. Customer 10 then transferred the funds from their SCA FMA to their account at another Australian casino.

On 17 November 2019, Customer 10 transferred $470,000 from their SCA FMA to Person 12's SCA FMA.

g. Customer 10 transacted using large amounts of cash and chips at SCA; and

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 28 December 2018 and 11 February 2020, SCA gave the AUSTRAC CEO 20 TTRs detailing incoming and outgoing payments made by Customer 10 totalling $5,438,569, which comprised:

a. one TTR totalling $18,000 in a cash for chip exchange;

b. nine TTRs totalling $2,168,600 in account deposits; and

c. 10 TTRs totalling $3,251,969 in account withdrawals.

Large cash and chip transactions

On 26 December 2018, Customer 10 made a buy-in with $18,000 in cash and received cash chips.

On 1 May 2019, Customer 10 cashed out $128,200 in non-negotiable chips and deposited the funds into their SCA FMA. Shortly after, Customer 10 withdrew $28,200 in cash from their SCA FMA.

On 18 November 2019, Customer 10 made a buy-in with a $20,000 CPV.

h. SCA did not have adequate reason to believe that Customer 10's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 10 by SCA.

Particulars

See paragraph 516 above.

By 7 December 2016, SCA recorded Customer 10's occupation as a property investor.

On 26 December 2018, Customer 10 informed SCA that they were a personal assistant to a director.

At no time did SCA request source of funds or source of wealth information from Customer 10. SCA was therefore unable to determine whether Customer 10's access to funds and level of gaming at SCA was commensurate with their stated occupation.

SCA's determination of the ML/TF risks posed by Customer 10

692. On and from 1 May 2019, Customer 10 was appropriately rated by SCA as a high risk customer for the purpose of the Act and Rules.

Particulars

On 25 March 2022, Customer 10's risk rating was elevated to significant, which was high risk for the purpose of the Act and Rules.

693. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 10 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 10.

Monitoring of Customer 10's transactions

694. At no time did SCA apply appropriate transaction monitoring to Customer 10's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities;

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not make or keep appropriate records of designated services provided to junket operators, junket representatives and junket players; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

c. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 10 through:

i. the junket channel; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

ii. the SCEG customer account channel, the SCA customer account channel and the SkyCity New Zealand channel, which were high risk remittance channels.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 10's KYC information

695. SCA did not review, update or verify Customer 10's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 10's, including the nature, extent and purpose of Customer 10's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 10's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 10's risk profile* above, there were higher ML/TF risks associated with Customer 10's source of wealth or source of funds.

d. to the extent that SCA reviewed Customer 10's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 10.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

ECDD triggers in respect of Customer 10

696. SCA was required to apply the ECDD program to Customer 10 following any ECDD triggers in respect of Customer 10.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1) and 15.10 of the Rules.

697. Customer 10 was determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 10* above.

698. The matter pleaded at paragraph 697 was an ECDD trigger.

Particulars

See paragraphs 496 and 504 above.

699. SCA did not conduct appropriate risk-based ECDD with respect to Customer 10 following an ECDD trigger because:

a. on each occasion prior to March 2022 that SCA conducted ECDD in respect of Customer 10 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 10 and failed to appropriately consider whether the ML/TF risks posed by Customer 10 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501, 511 and 516 to 517 above.

Junket approval

In August 2019, SCEG conducted due diligence in respect of Customer 10 to determine whether it would allow Customer 10 to operate junket programs at New Zealand. As part of this process, SCEG conducted an open source check with respect to Customer 10.

There are no records demonstrating that SCA conducted its own due diligence for the purposes of determining whether it was within its own ML/TF risk appetite to approve Customer 10 to be a junket operator at SCA: see paragraphs 382 to 418 above.

Alerts

On 29 April 2019, SCA conducted a Jade watchlist check with respect to Customer 10. The check did not return any results.

ECDD screening

On 14 November 2019, ECDD screening in respect of Customer 10 identified that:

a. Customer 10 had stated that their occupation was as a personal assistant to a director of a company; and

b. the ABN for a business that matched Customer 10's name had been cancelled on 11 March 2019.

On 27 May 2021, SCA conducted watchlist checks and open source searches with respect to Customer 10, as they had over $1,000,000 in their FMA.

It was not until 29 March 2022 that SCA issued a ban in respect of Customer 10.

The ECDD conducted by SCA did not have appropriate regard to Customer 10's higher ML/TF risks: see *Customer 10's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 10's source of funds or source of wealth.

By reason of the matters set out in *Customer 10's risk profile* above, there were higher risks associated with Customer 10's source of wealth and source of funds.

b. on any occasion prior to March 2022 that senior management considered the higher ML/TF risks posed by Customer 10 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 10 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

Customer 10 was mentioned in a 'Transaction Monitoring Overview' report for the period 1 August 2019 to 1 November 2019, which was provided to the AML/CTF Senior Management Group for discussion at their meeting. The report noted that Customer 10 had received $400,000 into their SCA FMA from Person 12's FMA. The funds were then transferred to another Australian casino.

On 25 March 2022, after elevating Customer 10's risk rating to significant risk, an SCA AML Compliance Analyst emailed the SCA Chief Operating Officer to determine whether SCA should continue a business relationship with Customer 10. On 27 March 2022, the SCA Chief Operating Officer determined that SCA should discontinue its business relationship with Customer 10.

On 29 March 2022 SCA issued a ban in respect of Customer 10.

Contravention of s 36 of the Act in respect of Customer 10

700. By reason of the matters pleaded at paragraphs 688 to 699 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 10 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

701. By reason of the matters pleaded at paragraph 700, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 29 March 2022 with respect to Customer 10.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 11

702. Customer 11 was a customer of SCA during the relevant period. Between 7 December 2016 and 13 November 2018, SCA recorded turnover exceeding $600,000,000 for Customer 11, excluding their play on junkets, which was not individually recorded.

Particulars

Customer 11 was a customer of SCA from at least 16 March 2015.

On 22 March 2022, SCA issued a ban in respect of Customer 11.

703. SCA provided Customer 11 with designated services within the meaning of table 1 and table 3, s 6 of the Act during the relevant period including services connected to Customer 11's gambling as a junket player, facilitated through a junket operator.

Particulars

On 16 March 2015, SCA opened an FMA for Customer 11, which remained open as at 28 October 2022 (item 11, table 3, s 6 of the Act).

Between 6 January 2018 and 30 September 2018, SCA provided lines of credit for Customer 11 on five occasions with limits ranging from $1,000,000 to $2,000,000 (item 6, table 1, s 6 of the Act).

While a customer of SCA, Customer 11 remitted funds to and from their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 11's risk profile* below.

704. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 11.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 11's risk profile

705. On and from 7 December 2016, Customer 11, and the provision of designated services to Customer 11 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 11's risk history as at 7 December 2016

a. by 7 December 2016 Customer 11 had the following risk history:

i. SCA had formed suspicions for the purposes of s 41 of the Act with respect to Customer 11;

Particulars

SCA gave the AUSTRAC CEO an SMR on 8 November 2016.

The SMR reported that Customer 11 was the main player on Customer 3's junket and a number of threshold transactions reported to AUSTRAC had identified Customer 3 as having conducted the transaction when it had in fact been conducted by Customer 11.

ii. between 27 September 2016 and 30 November 2016, Customer 11 was a junket player who received high value financial and gaming services (tables 1 and 3, s 6 of the Act) at SCA through junket programs;

Particulars

Customer 11 played on two junkets at SCA operated by Customer 3, from 27 September 2016 to 2 October 2016, and from 26 October 2016 to 31 October 2016. Customer 12 was the junket representative on both junket programs.

iii. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 11 by remitting large amounts of money within the casino environment via their accounts;

Particulars

See paragraphs 232 to 312 above.

On 4 October 2016, Customer 11 received $100,000 into their SCA FMA from Person 3's SCA FMA. SCA made these funds available to Customer 11.

On 8 October 2016, SCA accepted instructions to transfer $100,000 from Customer 11's SCA FMA to Person 3's SCA FMA.

iv. Customer 11 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 5 October 2016 and 22 November 2016, SCA gave the AUSTRAC CEO 12 TTRs detailing incoming and outgoing payments made by Customer 11 totalling $500,549, which comprised:

a. nine TTRs totalling $260,690 in chip and cash exchanges;

b. one TTR totalling $100,000 for an account deposit; and

c. two TTRs totalling $139,859 in account withdrawals.

v. Customer 11 engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose and appeared to be an attempt to disguise the source and beneficiary of funds; and

Particulars

See paragraph 24 above.

By 7 December 2016, SCA was aware that:

a. Customer 11 was regularly cashing out gaming chips under Customer 3's name when playing on Customer 3's junket; and

b. Customer 11 had taken control of funds at settlement of Customer 3's junket programs.

Between 20 September 2016 and 2 November 2016, SCA recorded seven threshold transactions totalling $268,305 conducted by Customer 11 that were incorrectly attributed to Customer 3.

On 2 October 2016, SCA issued Customer 11 with a cheque for $2,700,000, $2,011,136 of which was from Customer 11's FMA and had been deposited as settlement from play on Customer 3's junket.

Between 7 December 2016 and 14 September 2017, Customer 11 was included in an internal report titled 'Telegraphic Transfer – Third Party or Unusual' on six occasions.

Customer 11's risk profile during the relevant period

b. at all times, Customer 11 was a foreign PEP;

Particulars

See paragraphs 123 and 505 above.

Customer 11 was an immediate family member of a person holding a prominent public position in a foreign government body. SCA was aware that Customer 11 was a foreign PEP by 1 August 2019, and recorded this in SCA's system on 8 October 2019.

c. Customer 11 was a junket player who received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA through junket programs;

i. between 14 December 2016 and 11 July 2017, Customer 11 was the main player on ten junket programs at SCA operated by one junket operator Customer 3, with Customer 12 as the junket representative;

ii. between 25 and 28 August 2017, Customer 11 was a main player on a junket operated by junket operator Customer 9;

iii. the combined turnover of those junket programs was estimated at $463,838,818; and

iv. at no time did SCA record Customer 11's individual gambling activity on junket programs they attended as a junket player;

d. designated services provided to Customer 11 lacked transparency as the services were provided through the channel of junket programs at SCA;

Particulars

See paragraph 392 above.

e. between December 2017 and 20 October 2018, Customer 11 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA from play on individual commission programs, with a total commission of $4,166,062 recorded as payable by SCA to Customer 11;

Particulars

From December 2017 to early February 2018, Customer 11 played on an individual commission program with losses of $7,193,166.

In the 2018 financial year, Customer 11's recorded gambling activity on individual commission programs at SCA was estimated as a buy-in of $21,747,754, turnover of $571,680,366, and with losses of $229,975. Rebates of $3,933,581 were payable by SCA to Customer 11 from their play on individual commission programs.

In the 2019 financial year, Customer 11's recorded gambling activity on individual commission programs at SCA was estimated as a buy-in of $4,698,684, turnover of $33,787,166, and with losses of $2,305,155. In 2019, rebates of $232,481 were payable by SCA to Customer 11 from their play on individual commission programs.

f. Customer 11 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs and individual commission programs. Between 7 December 2016 and 13 November 2018, SCA recorded high losses of $20,843,275 for Customer 11; and

Particulars

In 2016, Customer 11's recorded individual rated gambling activity at SCA was estimated as a buy-in of $3,000 for table games with wins of $21,800.

In 2017, Customer 11's recorded individual rated gambling activity at SCA escalated to an estimated buy-in of $6,285,750 for table games with wins of $723,955.

In 2018, Customer 11's recorded individual rated gambling activity at SCA further escalated to an estimated buy-in of $61,283,320 for table games with losses of $21,589,030.

In the 2019 financial year, Customer 11 was one of the top six SCEG customers by turnover.

g. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 11 by remitting large amounts of money into and within the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCEG customer account channel

On 3 September 2017, SCA accepted instructions to transfer $1,750,000 from Customer 11's SCA FMA to their FMA at a SCEG New Zealand casino through the SCEG customer account channel.

Remittances through the SCA customer account channel

SCA made money available to Customer 11 in the following transactions:

a. On 8 February 2018, SCA received a telegraphic transfer of $967,344 from Customer 3 with the instruction to make the funds available to Customer 11.

b. On or around 9 February 2018, Customer 2 engaged the services of Company 1 to transfer $200,000 to SCA's bank account. Once SCA received the funds, SCA deposited them into Customer 11's SCA FMA in circumstances where the connection between Customer 2 and Customer 11 regarding the funds was not clear.

c. On or around 20 March 2018, Customer 2 engaged the services of Company 1 to transfer $300,000 to SCA's bank account. Once SCA received the funds, SCA deposited them into Customer 11's FMA in circumstances where the connection between Customer 2 and Customer 11 regarding the funds was not clear.

d. In 2018, Customer 11 transferred $20,266,905 to their SCA account in 18 transactions, including:

    i. on 16 April 2018, Customer 11 transferred $3,500,000 from their personal bank account in Australia to their SCA FMA;

    ii. on 11 May 2019, Customer 11 transferred $1,000,000 from their personal bank account in Australia to their SCA FMA;

iii. On 5 June 2018, Customer 11 transferred $2,600,000 from their personal bank account in Australia to their SCA FMA;

iv. On 20 June 2018, Customer 11 transferred $1,700,000 from their personal bank account in Australia to their SCA FMA; and

v. On 30 November 2018, Customer 11 received $1,600,000 into their SCA FMA via telegraphic transfer.

e. Between 1 September 2018 and 13 November 2018, Customer 11 credited $6,800,000 to the SCA Cage account across eight transactions via transfers from Australian bank accounts.

Remittances through the SkyCity New Zealand channel

SCA made money available to Customer 11 in the following transactions:

Between 10 April 2017 and 2 October 2018, SCA credited $3,736,168 to Customer 11's FMA with these funds originating from Customer 11's FMA held at a SCEG New Zealand casino.

Remittances within the casino environment

SCA made money available to Customer 11 in the following transactions:

a. On 17 June 2017, Customer 11 received $3,700,000 into their SCA FMA from Customer 3's SCA FMA.

b. On 26 June 2017, Customer 11 received $59,761 into their SCA FMA from Customer 3's SCA FMA.

c. On 18 January 2018, Customer 11 received $626,792 into their SCA FMA from Customer 15's SCA FMA. This money had been transferred into Customer 15's SCA FMA from a SCEG New Zealand casino's DAB account, as a result of a HKD$4,000,000 transfer from a third party company, Company 7. On 23 January 2018, SCA reported suspicions to the AUSTRAC CEO that Company 7 had been used by Customer 11 to move money out of a foreign country in a way that avoided government detection and distanced Customer 11 from the transaction.

SCA accepted instructions to transfer funds from Customer 11's accounts for the following transactions:

a. On 15 April 2017, Customer 11 transferred $3,374,600 from their SCA FMA to Customer 3's SCA FMA.

b. On 2 July 2017, Customer 11 transferred $3,800,000 from their SCA FMA to Customer 3's SCA FMA.

h. Customer 11 was connected to other customers at SCA, including junket operators and junket players, and players who posed higher ML/TF risks such as Customer 2, Customer 3, Customer 9, Customer 12, Customer 14 and Customer 15;

Particulars

From 8 February 2018 to 26 April 2018, Customer 11 was involved in a series of suspicious transactions with Customer 2: Customer 2 received $150,000 in cash and CVIs from Customer 11, and Customer 2 facilitated the transfer of $500,000 to Customer 11's SCA FMA from Company 1.

Between 7 December 2016 and 11 July 2017, Customer 11 a junket player on ten junkets at SCA operated by Customer 3, for which Customer 12 was the junket representative.

On 26 August 2018, Customer 11 was a junket player on a junket operated by Customer 9. Customer 14 was also a junket player on that junket.

By July 2019, SCA was aware that Customer 11 had been on board a private jet with Customer 14 when it was searched by a law enforcement agency in connection with suspicions of money laundering.

SCA was aware that Customer 11 and Customer 12 were business partners.

From at least February 2018, SCA was aware that an Australian government agency was investigating Customer 12 in respect of their income and was concerned that Customer 11 may be assisting Customer 12 to move money and avoid detection: SMR dated 19 February 2018.

Customer 15 was Customer 11's personal assistant. On 18 January 2018, Customer 15 transferred $626,792 from their SCA FMA into Customer 11's SCA FMA, which had been transferred to SCA via a SCEG account by Company 7. SCA determined that Customer 11 was the originator of the funds and had used Company 7 to move the funds out of a foreign country without government detection.

In March 2018, Customer 15 conducted chip exchanges involving Customer 11. SCA suspected that Customer 11 used Customer 15 to distance themselves from transactions conducted through SCA.

See *Customer 2's risk profile* above, *Customer 3's risk profile* above*, Customer 9's risk profile* above*, Customer 12's risk profile* below*, Customer 14's risk profile* below *and Customer 15's risk profile* below.

i. Customer 11 transacted using large amounts of cash, including taking large volumes of cash into and out of SCA in bags;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 15 December 2016 and 13 November 2018, SCA gave the AUSTRAC CEO 195 TTRs detailing incoming and outgoing payments made by Customer 11 totalling $28,441,815, which comprised:

a. 149 TTRs totalling $4,445,141 in chip and cash exchanges;

b. 30 TTRs totalling $16,598,537 in account deposits;

c. 12 TTRs totalling $3,208,137 in account withdrawals;

d. two TTRs totalling $4,000,000 in marker redemptions; and

e. two TTRs totalling $190,000 in premium player commissions.

Large and suspicious cash transactions in 2017

On 26 June 2017, SCA refunded Customer 11 $59,761 in cash from their SCA FMA.

On 28 August 2017, Customer 11 withdrew $20,000 in cash from their SCA FMA.

On 2 September 2017, SCA refunded Customer 11 $50,992 in cash from their SCA FMA.

Large and suspicious cash transactions in 2018

On 14 January 2018, Customer 11 made a cash deposit of $280,000 into their SCA FMA.

On 15 January 2018, Customer 11 made a cash deposit of $99,000 into their SCA FMA.

On 24 January 2018, Customer 11 made a cash deposit of $100,000 into their SCA FMA.

On 27 January 2018, Customer 11 made a cash deposit of $300,000 into their SCA FMA.

On 28 January 2018, Customer 11 made a cash deposit of $100,000 into their SCA FMA.

On 30 January 2018, Customer 11 made a cash deposit of $900,000 into their SCA FMA.

On 5 February 2018, Customer 11 made a cash deposit of $100,000 into their SCA FMA and deposited a $70,000 cheque to obtain CPVs.

On 5 February 2018, Customer 11 made a cash deposit of $70,000 into their SCA FMA.

On 6 February 2018, Customer 11 made a cash deposit of $100,000 into their SCA FMA. On the same day, Customer 11 left SCA's premises with a carry bag containing $228,500 in cash.

From 6 February 2018 to 7 February 2018, Customer 11 conducted multiple cash outs totalling $294,250. Customer 11 placed the cash in their personal safe at SCA.

On 8 February 2018, Customer 11 removed $230,000 in cash from their personal safe at SCA and left SCA with the cash.

On 8 February 2018, Customer 11 entered the premises with a carry bag containing what appeared to be $130,000 in cash. A total of $440,400 in cash was then used by Customer 11 for a buy-in at the Cage, which comprised the $130,000 in the carry bag and $310,400 Customer 11 had collected from their personal safe at SCA.

On 17 March 2018, Customer 11 made a cash deposit of $150,000 into their SCA FMA.

On 26 April 2018, SCA refunded Customer 11 $50,000 in cash from their SCA FMA.

j. between 6 January 2018 and 30 September 2018, SCA provided Customer 11 with significant amounts of credit upon request, up to limits of $2,000,000;

Particulars

See paragraphs 321 to 323, and 342 above.

Between 6 January 2018 and 30 September 2018, SCA provided Customer 11 with at least $6,000,000 in credit, up to limits between $1,000,000 and $2,000,000, on four occasions.

k. SCA issued Customer 11 with cheques in large amounts;

Particulars

On 16 December 2016, SCA issued Customer 11 with a cheque for $1,200,000, which was drawn on funds from their SCA FMA.

On 29 December 2016, SCA issued Customer 11 with a cheque for $1,200,000, which was a return of a cheque for the same amount that was used as a buy-in.

On 7 January 2017, SCA issued Customer 11 with a cheque for $1,200,000, which was drawn on funds from their SCA FMA.

On 18 January 2017, SCA issued Customer 11 with a cheque for $1,200,000, which was drawn on funds from their SCA FMA.

On 17 June 2017, SCA issued Customer 11 with a cheque for $3,700,000, $3,529,290 of which was drawn on funds from their SCA FMA as settlement from play on Customer 3's junket.

On 26 June 2017, SCA issued Customer 11 with a cheque for $3,800,000, which was drawn on funds from their SCA FMA.

On 28 December 2017, SCA issued Customer 11 with a cheque for $342,883, which was drawn on funds from their SCA FMA.

l. Customer 11 engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose and appeared to be an attempt to disguise the source and beneficiary of funds;

Particulars

See paragraph 24 above.

Large and unusual transactions on junkets

From 7 December 2016, SCA was aware that Customer 11 regularly cashed out gaming chips under Customer 3's name when playing on Customer 3's junket and had taken control of funds at settlement of Customer 3's junket programs.

On the following occasions, Customer 11 was involved in transactions indicative of attempts to disguise the source and beneficiary of funds:

a. on 14 December 2016, a transaction of $22,500 (cashing out non-negotiable and commission chips) was conducted by Customer 11 but attributed by SCA to Customer 12. Customer 12 claimed the chips came from Customer 3's play, but Customer 3 was not in Australia and all table play was confirmed to be Customer 11's;

b. in January 2017, four transactions were conducted by Customer 11 but attributed by SCA to Customer 3 despite Customer 3 not being present at SCA at the time; and

c. on 15 April 2017, a transaction of $20,000 was conducted by Customer 11 but attributed by SCA to Customer 3, despite Customer 3 not being present at SCA at the time.

SCA held concerns about the repeated nature of such transactions. On 11 April 2017, an SCA AML Analyst emailed the Vice President of International VIP Services asking that all international business and cash handling staff to ensure that any TTR was attributed to Customer 11 when they redeemed chips. Despite this, the transaction on 15 April 2017 was attributed to Customer 3 not Customer 11.

Large and unusual transactions on ICPs

On 18 January 2018, Customer 15 transferred $626,792 from their SCA FMA to Customer 11's SCA FMA. These funds had been deposited into Customer 15's FMA from the overseas SCEG account, having been transferred from Company 7. SCA determined the originator of funds was Customer 11, who used Company 7 to move funds out of a foreign country without government detection and Customer 15's account was used to further distance Customer 11 from the transaction.

On 24 January 2018, Customer 12 carried out a number of chip redemptions on behalf of Customer 11. Customer 12 was not at SCA to game and their attendance was not recorded in any arrival logs.

On 8 February 2018, Customer 2 received a $100,000 non-negotiable plaque from Customer 11 at SCA. Customer 2 then swapped the plaques for plaques of a different value.

On or around 9 February 2018, Customer 2 engaged the services of Company 1 to transfer $200,000 to SCA's bank account. Once SCA received the funds, SCA deposited them into Customer 11's SCA FMA in circumstances where the connection between Customer 2 and Customer 11 regarding the funds was not clear.

On or around 20 March 2018, Customer 2 engaged the services of Company 1 to transfer $300,000 to SCA's bank account. Once SCA received the funds, SCA deposited them into Customer 11's SCA FMA in circumstances where the connection between Customer 2 and Customer 11 regarding the funds was not clear.

On 13 March 2018, Customer 15 was observed assisting in the exchange of $50,000 of chips between Customer 11, Customer 2 and Customer 27 and cashing those chips out on behalf of Customer 11.

On 26 April 2018, Customer 11 cashed out $50,000 at SCA. SCA suspected that the cash may have been intended for, or passed to, Customer 2.

m. Customer 11 was the subject of law enforcement enquiries at SCA;

Particulars

On 14 February 2018, SCA received a request from a law enforcement agency in relation to Customer 11.

By February 2018, SCA was aware that an Australian government agency was investigating Customer 12 in respect of their income: SMR dated 19 February 2018.

n. Customer 11 had access to private gaming rooms at SCA;

Particulars

See paragraph 145(e) above.

Customer 11 had access to private gaming rooms at SCA, including the Grange Room and Horizon Suites.

o. by 29 July 2019, SCA was aware of a number of media articles which reported that Customer 11 was associated with alleged money laundering and organised crime, and was related to a high-ranking foreign official; and

Particulars

On 29 July 2019, a media report named Customer 11:

a. as a person allegedly involved in international money laundering and corruption; and

b. as a close relative of a high-ranking foreign official.

p. SCA did not have adequate reason to believe that Customer 11's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 11 by SCA.

Particulars

See paragraph 516 above.

From at least March 2017, SCA was aware that it did not have source of wealth information for Customer 11.

At all times, Customer 11 was a foreign PEP. SCA identified Customer 11 as a foreign PEP in October 2019.

Between 29 March 2016 and 20 October 2018, Customer 11 had an estimated individual buy-in of $67,558,270. Customer 11's individual turnover on junkets was not recorded.

Between 22 August 2017 and 2 October 2018, Customer 11 deposited cheques totalling over $6,700,000 into their SCA FMA.

SCA was aware that:

a. from at least August 2017, there were reports that Customer 11 was formerly the chairperson of a company that had been found to be a special interest entity due to having sanctions applied by a foreign government; and

b. from January 2018, Customer 11 had used a third party to transfer $626,792 into their SCA FMA to avoid detection by another foreign government and obscure the source of funds.

SCA did not at any time obtain any source of wealth information from Customer 11.

SCA's determination of the ML/TF risks posed by Customer 11

706. On and from 15 December 2016, Customer 11 was appropriately rated by SCA as a high risk customer for the purpose of the Act and Rules.

707. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 11 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 11.

Monitoring of Customer 11's transactions

708. At no time did SCA apply appropriate transaction monitoring to Customer 11's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers;

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not make or keep appropriate records of designated services provided to junket players;

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

c. SCA did not carry out adequate due diligence on source of funds in respect of third party deposits received for the benefit of Customer 11 into its bank accounts; and

Particulars

See paragraph 227 above.

Customer 11 received money through their SCA FMA deposited by third parties.

d. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 11 through:

i. the junket channel; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

ii. the SCEG customer account channel, the SCA customer account channel and the SkyCity New Zealand channel, which were high risk remittance channels.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 11's KYC information

709. SCA did not review, update or verify Customer 11's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 11, including the nature, extent and purpose of their transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 11's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 11's risk profile* above, there were higher ML/TF risks associated with Customer 11's source of wealth or source of funds.

d. to the extent that SCA reviewed Customer 11's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 11.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

ECDD triggers in respect of Customer 11

710. SCA was required to apply the ECDD program to Customer 11 following any ECDD triggers in respect of Customer 11. In particular, because Customer 11 was a foreign PEP, SCA was required to:

a. undertake detailed analysis of Customer 11's KYC information including taking reasonable measures to identify the source of Customer 11's wealth and the source of Customer 11's funds; and

b. seek senior management approval to continue a business relationship with Customer 11 and whether SCA should continue to provide a designated service to Customer 11.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.10(2), 15.10(6) and 15.11 of the Rules.

711. Customer 11:

a. at all times from 7 December 2016 was a foreign PEP;

Particulars

See *Customer 11's risk profile* above.

b. was the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 4 May 2017 and 19 February 2018, SCA gave the AUSTRAC CEO three SMRs with respect to Customer 11.

c. was determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

On 15 December 2016, SCA determined that the ML/TF risk posed by Customer 11 was high risk for the purpose of the Act and Rules:

see *SCA's determination of the ML/TF risks posed by Customer 11* above.

712. Each matter pleaded at paragraph 711 was an ECDD trigger.

Particulars

See paragraphs 496, 501, and 504 to 506 above.

713. It was not until August 2019 that SCA identified that Customer 11 was a foreign PEP, and only as a result of media reporting, identified Customer 11 as a close family member of a high-ranking foreign official.

714. SCA did not conduct appropriate risk-based ECDD with respect to Customer 11 following the ECDD triggers:

a. on each occasion prior to 22 March 2022 that SCA conducted ECDD in respect of Customer 11 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 11 and failed to appropriately consider whether the ML/TF risks posed by Customer 11 were within SCA's ML/TF risk appetite. In particular, SCA failed to monitor Customer 11 as a foreign PEP because:

i. SCA's analysis of Customer 11's KYC information failed to appropriately consider the ML/TF risks posed by Customer 11;

ii. SCA's analysis of Customer 11's source of wealth and source of funds failed to appropriately consider the ML/TF risks posed by Customer 11; and

iii. any senior management approval regarding Customer 11 failed to appropriately consider the ML/TF risks posed by Customer 11 and the provision of designated services to Customer 11 by SCA and to whether those risks were within SCA's ML/TF risk appetite.

Particulars for (i) to (iii)

Rules 15.10 of the Rules.

See paragraphs 501, 505, 511 and 516 to 517 above.

Between 28 November 2017 and 26 November 2019, SCA conducted ECDD in respect of Customer 11 on 12 occasions, including open source information searches, which identified that:

a. in November 2017, it had been reported that the company Customer 11 was formerly chairperson of had been found to be a special interest entity due to having sanctions applied to it by a foreign government;

b. Customer 11 was a foreign PEP; and

c. Customer 11 was associated with other SCA customers whom SCA considered suspicious.

On 29 November 2018, the SCA General Manager Legal, Compliance & Regulatory Affairs and the SCA Legal & Compliance Advisor were advised of the details of a number of SMRs lodged with

respect to Customer 2 and other customers, and of links between Customer 2 and other customers who SCA considered acted suspiciously, including Customer 11.

On 1 August 2019, the SCEG AML Compliance and Intelligence Manager sent an internal memorandum to the SCEG General Manager for Regulatory Affairs and AML, also copying the SCEG General Counsel/Company Secretary about media allegations regarding another Australian casino and the customers of SCEG named in those media reports, including Customer 11. The memorandum acknowledged Customer 11's status as a foreign PEP and SCEG's obligation to conduct ECDD in respect of Customer 11.

On 8 August 2019, at a meeting between the SCEG General Counsel/Company Secretary, the SCEG General Manager Regulatory Affairs and AML, and the SCEG Chief Financial Officer, senior management agreed that Customer 11 would not be offered any designated services at SCEG pending confirmation of their source of wealth and repayment of a NZD$2,500,000 debt to a SCEG New Zealand casino.

In November 2019, SCA identified that it did not hold any source of wealth or source of funds information for Customer 11.

SCEG continued its business relationship with Customer 11 until at least June 2020 without having obtained any source of wealth or source of funds information from Customer 11.

It was not until 22 March 2022 that SCA issued a ban in respect of Customer 11.

The ECDD conducted by SCA did not have appropriate regard to Customer 11's higher ML/TF risks: see *Customer 11's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 11's source of funds or source of wealth.

By reason of the matters set out above, there were higher ML/TF risks associated with Customer 11's source of wealth or source of funds: see *Customer 11's risk profile*.

Contravention of s 36 of the Act in respect of Customer 11

715. By reason of the matters pleaded at paragraphs 702 to 714 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 11 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

716. By reason of the matters pleaded at paragraph 715, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 22 March 2022 with respect to Customer 11.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 12

717. Customer 12 was a customer of SCA during the relevant period. Between 7 December 2016 and 24 July 2017, SCA recorded a turnover exceeding $3,400,000 for Customer 12.

Particulars

Customer 12 was a customer of SCA from at least 1 July 2012.

On 4 September 2020, SCA issued a ban in respect of Customer 12.

718. SCA provided Customer 12 with designated services within the meaning of table 1 and table 3, s 6 of the Act during the relevant period including services connected to Customer 12's role as a junket representative.

Particulars

On 15 November 2012, SCA opened an FMA for Customer 12 which was closed on 2 December 2020.

While a customer of SCA, Customer 12 remitted funds to and from their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 12's risk profile* below.

719. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 12.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 12's risk profile

720. On and from 7 December 2016, Customer 12, and the provision of designated services to Customer 12 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 12's risk profile prior to the relevant period

a. by 7 December 2016 Customer 12 had the following risk history:

i. SCA had formed suspicions for the purposes of s 41 of the Act with respect to Customer 12;

Particulars

SCA gave the AUSTRAC CEO an SMR on 8 November 2016.

The SMR reported that SCA held concerns about Customer 11's participation in Customer 3's junket, for which Customer 12 was the junket representative. The SMR also reported that a SCEG New Zealand casino had reported concerns about Customer 11 and Customer 12 being associated with suspected sex workers.

ii. SCA was aware that Customer 12 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 2 July 2014 and 31 October 2016, SCA gave the AUSTRAC CEO 13 TTRs detailing incoming and outgoing payments made by Customer 12 totalling $432,251, which comprised:

a. seven TTRs totalling $129,826 in chip and cash exchanges;

b. one TTR totalling $57,200 for an account deposit;

c. three TTRs totalling $205,224 in account withdrawals; and

d. two TTRs totalling $40,000 in other cash transactions.

Large cash transactions

On 28 September 2016, Customer 12 withdrew $29,000 in cash from their SCA FMA.

On 30 October 2016, Customer 12 withdrew $20,000 in cash from their SCA FMA.

iii. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 12 by remitting large amounts of money out of and within the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

SCA accepted instructions to transfer funds from Customer 12's accounts for the following transactions.

a. On 26 March 2015, Customer 12 transferred $1,687,612 from their SCA FMA to another Australian casino for the benefit of Customer 11.

b. On 22 November 2016, Customer 12 transferred $156,233 from their SCA FMA to another Australian casino.

Remittances within the casino environment

SCA made money available to Customer 12 in the following transactions.

a. On 2 October 2016, Customer 12 received $28,327 into their SCA FMA from Customer 3's SCA FMA.

b. On 19 November 2016, Customer 12 received $57,200 into their SCA FMA from Customer 3's SCA FMA.

Customer 12's risk profile during the relevant period

b. between 7 December 2016 and 11 July 2017, Customer 12 was a junket representative for ten junkets operated by Customer 3 at SCA;

Particulars

The total cumulative turnover for these junkets in the relevant period was $432,394,716.

c. designated services provided to Customer 12 lacked transparency as the services were provided through the channel of junket programs at SCA;

Particulars

See paragraph 392 above.

d. Customer 12 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs. Between 7 December 2016 and 24 July 2017, SCA recorded a high turnover estimated at $3,432,908 for Customer 12, with cumulative wins of $263,825;

Particulars

In 2016, Customer 12's recorded individual rated gambling activity at SCA was estimated as a buy-in of $46,400, and turnover of $312,303 with wins of $48,000 for table games.

In 2017, Customer 12's recorded individual rated gambling activity at SCA escalated to an estimated buy-in of $659,675 for table games, and for both table games and EGMs, a turnover of $3,120,606 with wins of $215,825.

e. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 12 by remitting large amounts of money into, out of and within the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

On 21 February 2017, Customer 12 deposited $202,424 into SCA's bank account. SCA made these funds available to Customer 12.

SCA accepted instructions to transfer funds from Customer 12's accounts for the following transactions:

a. On 27 April 2017, Customer 12 transferred $20,000 from their SCA FMA to their personal bank account.

b. On 17 June 2017, Customer 12 transferred $155,010 from their SCA FMA to Customer 3's bank account in Australia.

Remittances through the SkyCity New Zealand channel

SCA made money available to Customer 12 in the following transactions:

a. On 20 February 2017, SCA credited $198,638 to Customer 12's SCA FMA with funds originating from a SCEG New Zealand casino .

b. On 19 June 2017, SCA credited $3,051,563 to Customer 12's SCA FMA with funds originating from a SCEG New Zealand casino.

Remittances from SCA FMAs to SCEG New Zealand FMAs

SCA accepted instructions to transfer funds from Customer 12's accounts for the following transactions:

a. On 23 January 2017, SCA credited $1,800,000 to Customer 12's FMA held at a SCEG New Zealand casino from Customer 3's SCA FMA.

b. On 3 May 2017, SCA credited $2,000,000 to Customer 12's FMA held at a SCEG New Zealand casino from Customer 3's SCA FMA.

Remittances within the casino environment

SCA made money available to Customer 12 in the following transactions.

Between 23 January 2017 to 10 July 2017, Customer 12 received $2,194,928 into their SCA FMA from Customer 3's SCA FMA in seven transactions.

SCA accepted instructions to transfer funds from Customer 12's accounts for the following transactions.

Between 19 June 2017 and 4 July 2017, Customer 12 transferred $3,131,150 from their SCA FMA to Customer 3's SCA FMA in two transactions.

f. Customer 12 was connected to other customers at SCA, including junket operators, junket players, foreign PEPs, players who posed higher ML/TF risks, and players who SCA considered had acted suspiciously such as Customer 3, Customer 11, Customer 14 and Customer 15;

Particulars

Between 20 September 2016 and 11 July 2017, Customer 11 was the main player on ten junkets at SCA operated by Customer 3, for which Customer 12 was the junket representative. Customer 15 was also a player on these junkets.

SCA recorded that Customer 11 and Customer 12 were business partners.

Customer 3 and Customer 12 are siblings.

By July 2019, media reports identified Customer 12 as a business associate of Customer 14.

See *Customer 3's risk profile* above*, Customer 11's risk profile* above*, Customer 14's risk profile* above *and Customer 15's risk profile* above.

g. Customer 12 transacted using large amounts of cash and cash that appeared suspicious at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 15 December 2016 and 25 July 2017, SCA gave the AUSTRAC CEO 24 TTRs detailing incoming and outgoing payments made by Customer 12 totalling $4,043,397, which comprised:

a. nine TTRs totalling $233,560 in chip and cash exchanges;

b. six TTRs totalling $3,306,617 in account deposits;

c. eight TTRs totalling $458,322 in account withdrawals; and

d. one TTR totalling $44,896 for a premium player commission.

Large and suspicious cash transactions in 2017

Between 23 January 2017 and 11 July 2017, Customer 12 withdrew at least $153,860 in cash from their SCA FMA.

a. On 23 January 2017, Customer 12 withdrew $30,000 in cash from their SCA FMA.

b. On 15 April 2017, Customer 12 withdrew $5,000 in cash from their SCA FMA.

c. On 20 April 2017, Customer 12 withdrew $10,000 in cash from their SCA FMA.

d. On 6 June 2017, Customer 12 withdrew a total of $24,278 in cash from their SCA FMA across two transactions.

e. On 17 June 2017, Customer 12 withdrew $56,226 in cash from their SCA FMA.

f. On 19 June 2017, Customer 12 withdrew $1,470 in cash from their SCA FMA.

g. On 26 June 2017, Customer 12 withdrew $10,000 in cash from their SCA FMA.

h. On 11 July 2017, Customer 12 withdrew a total of $16,886 in cash from their SCA FMA across two transactions.

h. Customer 12 and persons associated with them engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose and appeared to be an attempt to disguise the source and beneficiary of funds;

Particulars

See paragraph 24 above.

On 14 December 2016, SCA recorded a transaction of $22,500 cashing out non-negotiable and commission chips as having been conducted by Customer 12, despite the transaction actually having been conducted by Customer 11. Customer 12 claimed the play was Customer 3's, but Customer 3 was not on site at SCA at the time and all play was confirmed to be Customer 11's.

On 15 April 2017, SCA recorded a $20,000 chip cash out as having been conducted by Customer 3, despite the transaction actually having been conducted by Customer 12. Customer 3 was not on site at SCA at the time and Customer 12 had taken the cash.

On 21 April 2017, SCA recorded a $20,000 cash deposit as having been conducted by Customer 3, despite the transaction actually having been conducted by Customer 12. Customer 3 was not on site at SCA at the time.

Between 7 December 2016 and 14 September, 2017 Customer 12 was included in an internal report titled 'Telegraphic Transfer – Third Party or Unusual' on six occasions.

On 2 May 2017, SCA received a deposit of $600,000 into its bank account from Company 5 for use by Customer 3's junket at a SCEG New Zealand casino. SCA conducted a company search on Company 5, which showed that it was owned by an overseas company, Company 6. SCA did not find a link between Customer 3's junket and Company 5. When questioned, Customer 12 claimed that Company 5 was a finance company of which Customer 3 was a customer: SMR dated 4 May 2017.

On 24 January 2018, Customer 12 carried out a number of chip redemptions on behalf of Customer 11 while Customer 11 was playing under an individual commission program. SCA did not have any records confirming that Customer 12 was physically present at SCA at the time.

i. Customer 12 had access to private gaming rooms at SCA;

Particulars

See paragraph 145(e) above.

Customer 12 had access to private gaming rooms at SCA, including the Grange Room and Horizon Salon.

j. by 28 July 2019, SCA was aware of media articles which reported that Customer 12 was associated with alleged money laundering, organised crime and foreign PEPs;

Particulars

From 2011, media reports linked the brothel owned by Customer 12 to alleged serious organised crime, including human trafficking and sex slavery.

In 2014, an Australian regulator commenced enforcement proceedings against Customer 12, alleging that Customer 12 was engaged in human trafficking.

From 2015, open court records relating to another proceeding reported that Customer 12's brothel had alleged links to organised crime and serious criminal activity, including money laundering, through the recruitment of women from a foreign region to work in the brothel for the material benefit of managers and staff, including Customer 12.

SCA's due diligence records did not contain details of these reports.

In July 2019, media reports connected Customer 12 to the brothel and to alleged organised crime and serious criminal activity, including money laundering and the recruitment of women from a foreign region to work in the brothel for the material benefit of Customer 12.

It was not until July 2019, following the publication of open source media articles which named Customer 12 in connection with an investigation into money laundering at another Australian casino, that SCA became aware that Customer 12 owned a brothel.

k. Customer 12 was a person of interest to Australian government agencies;

Particulars

SCA was aware that an Australian government agency was investigating Customer 12 in respect of their income and was concerned that Customer 11 may be assisting Customer 12 to move money and avoid detection: SMR dated 19 February 2018.

SCA also received a garnishee notice from the same Australian government agency in relation to Customer 12 in July 2020.

l. SCA did not have adequate reason to believe that Customer 12's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided by SCA to Customer 12.

Particulars

See paragraph 516 above.

At all times, SCA understood Customer 12's occupation to be as a Trade Manager and/or Managing Director.

SCA did not take steps to verify that information, nor did it take steps to obtain any source of wealth or source of funds information from Customer 12.

It was not until July 2019, when media reports were published linking Customer 12 with a brothel, that SCA became aware that Customer 12 owned the brothel.

Between late 2016 and mid-2017, Customer 12 was a junket representative for ten junkets which had a combined turnover exceeding $430,000,000. Customer 12 also had high turnover in their capacity as an individual player, with turnover of more than $3,400,000 in the same period.

From 2016, SCA's understanding of Customer 12's source of wealth and source of funds was not commensurate with the high value financial and gambling services provided by SCA to Customer 12.

SCA's determination of the ML/TF risks posed by Customer 12

721. On and from 15 December 2016, Customer 12 was rated by SCA as a high risk customer for the purpose of the Act and Rules

Particulars

On 15 December 2016, Customer 12 as high risk for the purpose of the Act and Rules.

722. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 12 appropriately on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by it with respect to Customer 12.

Monitoring of Customer 12's transactions

723. At no time did SCA apply appropriate transaction monitoring to Customer 12's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities;

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not make or keep appropriate records of designated services provided to junket representatives; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

c. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 12 through:

i. the junket channel; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

ii. the SCA customer account channel, which was a high risk remittance channel.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 12's KYC information

724. SCA did not review, update or verify Customer 12's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 12, including the nature, extent and purpose of Customer 12's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 12's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out above, there were higher ML/TF risks associated with Customer 12's source of wealth or source of funds: see *Customer 12's risk profile*.

d. to the extent that SCA reviewed Customer 12's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 12.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

ECDD triggers in respect of Customer 12

725. SCA was required to apply the ECDD program to Customer 12 following any ECDD triggers in respect of Customer 12.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

726. Customer 12 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 4 May 2017 and 19 February 2018, SCA gave the AUSTRAC CEO two SMRs pertaining to Customer 12.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 12* above.

727. Each matter pleaded at paragraph 726 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

728. SCA did not conduct appropriate risk-based ECDD with respect to Customer 12 following an ECDD trigger because:

a. on each occasion prior to 4 September 2020 that SCA conducted ECDD in respect of Customer 12 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 12 and failed to appropriately consider whether the ML/TF risks posed by Customer 12 were within SCA's ML/TF risk appetite; and

Particulars

Rule 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

No ECDD measures were taken in respect of Customer 12 until September 2019, months after Customer 12 had been named in media articles as being connected to alleged criminal conduct, including money laundering and human trafficking.

Customer 12 was closely associated with individuals, including foreign PEPs, known to SCA as posing higher ML/TF risks, including Customer 11.

However, it was not until 4 September 2020 that SCA issued a ban in respect of Customer 12.

The ECDD conducted by SCA did not have appropriate regard to Customer 12's higher ML/TF risks: see *Customer 12's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 12's source of funds or source of wealth.

By reason of the matters set out above, there were higher ML/TF risks associated with Customer 12's source of wealth or source of funds: see *Customer 12's risk profile* above.

b. on any occasion prior to 4 September 2020 that senior management considered the higher ML/TF risks posed by Customer 12 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 12 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

On 1 August 2019, the SCEG AML Compliance and Intelligence Manager sent an internal memorandum to the SCEG Group General Manager for Regulatory Affairs and AML, which was copied to the SCA Director, General Counsel and Company Secretary regarding allegations made in the media about another Australian casino and the customers of SCEG named in those reports, including Customer 12. The memorandum recommended that Customer 12 should be subject to ECDD as a result of the reported allegations that Customer 12's business interests involved criminal conduct, including human trafficking. Despite this, the memorandum acknowledged that such ECDD would be unlikely to advance SCA's understanding of Customer 12's source of funds or source of wealth.

On 8 August 2019, in an email from the SCEG General Manager Regulatory Affairs and AML to the SCEG AML Compliance and Intelligence Manager, which was copied to the SCEG General Counsel/Company Secretary and the SCEG General Manager Legal, Compliance & Regulatory Affairs, it was noted that Customer 12 was no longer considered a customer of SCEG and so did not require further action, but that an alert should be set up if Customer 12 was to return to a SCEG casino.

On 20 August 2019, in an email from the SCEG General Manager Regulatory Affairs and AML to the SCEG General Manager International Gaming, a SCEG Commercial Manager, the SCEG Chief Financial Officer, General Counsel and Company Secretary, SCEG General Manager Risk, General Manager Legal, Compliance & Regulatory Affairs and the SCEG AML Compliance and Intelligence Manager, it was confirmed that no further enquiries would be undertaken to determine Customer 12's ongoing suitability as a

customer of SCEG and that such enquiries would only be made if Customer 12 returned to a SCEG property in the future. SCEG reiterated this position in a memorandum from the SCEG General Manager Regulatory Affairs and AML to the SCEG Chief Financial Officer and the General Counsel/Company Secretary on 13 November 2019.

It was not until 4 September 2020 that SCA issued a ban in respect of Customer 12.

Contravention of s 36 of the Act in respect of Customer 12

729. By reason of the matters pleaded at paragraphs 717 to 728 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 12 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

730. By reason of the matters pleaded at paragraph 729, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 4 September 2020 with respect to Customer 12.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 13

731. Customer 13 was a customer of SCA during the relevant period. Between 16 December 2016 and 13 July 2019, junkets which Customer 13 played on had a total recorded turnover exceeding $16,500,000, however SCA failed to record Customer 13's individual gambling activity on those junkets.

Particulars

Customer 13 was a customer of SCA from at least 15 October 2016.

On 22 March 2022, SCA issued a ban in respect of Customer 13. Customer 13 was banned by the SCA AML team because they were a key player on the Suncity junket.

732. SCA provided Customer 13 with designated services within the meaning of table 3, s 6 of the Act during the relevant period including services connected to Customer 13's role as a junket player, facilitated through two different junket operators.

Particulars

On 15 October 2016, SCA opened an FMA for Customer 13 which was closed on 22 March 2022 (item 11, table 3, s 6 of the Act).

See *Customer 13's risk profile* below.

733. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 13.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 13's risk profile

734. On and from 7 December 2016, Customer 13, and the provision of designated services to Customer 13 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 13's risk profile prior to the relevant period

a. by 7 December 2016, Customer 13 had the following risk history:

   i. Customer 13 was a junket player and junket representative who received high value gambling services (table 3, s 6 of the Act) at SCA through junket programs; and

Particulars

Between 18 October 2016 and 21 October 2016, Customer 13 was a player on a junket at SCA operated by Person 1.

Customer 13 was also the junket representative for this junket program, which was run through the Suncity junket. Customer 1 held the line of credit for the junket program.

SCA did not record Customer 13's individual gambling activity on this junket program in its records for Customer 13. Instead, it recorded all of Customer 13's individual gambling activity on this junket program against Person 1. SCA recorded that Customer 13 won $262,415 on this junket program.

   ii. designated services provided to Customer 13 lacked transparency, as they were provided through the channel of junket programs at SCA;

Particulars

See paragraph 392 above.

Customer 13's risk profile during the relevant period

b. Customer 13 was a junket player who received high value gambling services (table 3, s 6 of the Act) at SCA through junket programs;

   i. between 16 December 2016 and 13 July 2019, Customer 13 was a junket player on seven Suncity junkets at SCA, and was a junket representative for four of those junkets. The junkets were operated by two junket operators, including Customer 1;

Particulars

On or around 1 February 2022, SCA recorded that Customer 13 appeared to be a high value player for Suncity. SCA also noted that Customer 13 appeared to have a close personal relationship with

Customer 1, who travelled to SCA with Customer 13 on two occasions, because Customer 13 was a key player on the Suncity junket.

ii. each of the seven Suncity junkets on which Customer 13 played were funded by lines of credit provided by SCA to Customer 1; and

Particulars

Each of the seven junket programs on which Customer 13 played were run through the Suncity junket. The credit holder for each junket was Customer 1.

iii. at no time did SCA record Customer 13's individual gambling activity on junket programs they attended as a junket player;

Particulars

All of Customer 13's individual gambling activity on junket programs at SCA was recorded against junket operators or junket representatives, including Customer 1.

The seven junkets which Customer 13 played on had a total recorded turnover exceeding $16,584,000.

SCA was not able to identify how much of that turnover was attributable to Customer 13's individual gambling activity on those junkets.

c. designated services provided to Customer 13 lacked transparency as the services were provided through the channel of junket programs at SCA;

Particulars

See paragraph 392 above.

d. Customer 13 received gambling services (table 3, s 6 of the Act) at SCA other than through junket programs. In 2017, Customer 13's recorded individual rated gambling activity for table games at SCA was estimated as a turnover of $5,400, and with wins of $2,000;

e. SCA was aware that Customer 13 frequently engaged in large buy-ins and cash outs, despite SCA not recording play for Customer 13 consistent with those buy-ins and cash outs;

Particulars

For example, on the following occasions Customer 13 transacted using large amounts of chips and cash at SCA without commensurate recorded play:

a. on 23 December 2016, Customer 13 cashed out $3,558,700;

b. on 12 January 2017, SCA issued Customer 13 with a CPV for $910,000;

c. on 14 March 2017, Customer 13 cashed out over $2,4,00,000 worth of chips, including non-negotiable chips;

d. on 3 April 2017, Customer 13 was issued with a CPV for $1,004,850 from their account. Customer 13 redeemed the CPV for CCF chips 10 minutes later;

e. on 27 April 2017, Customer 13 deposited $20,400 in cash into their SCA FMA. Customer 13 used the funds to purchase chips. Shortly after, Customer 13 cashed out $22,410 in chips;

f. on 14 December 2017, Customer 1 deposited $12,000 in cash into Customer 13's SCA FMA. Customer 13 then withdrew the funds from their FMA in cash;

g. on 11 July 2019, Customer 13 made a buy-in with a CPV for $1,600,000. Later that day, Customer 13 deposited $117,000 in non-negotiable chips into their SCA FMA; and

h. on 12 July 2019, Customer 13 deposited $137,705 in chips into the Suncity Group SCA FMA.

f. Customer 13, and persons from the Suncity junket associated with Customer 13, transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

See paragraph 734.e above.

TTRs

Between 7 April 2017 and 15 December 2017, SCA gave the AUSTRAC CEO four TTRs detailing incoming and outgoing transactions made by Customer 13 totalling $64,810, which comprised:

a. two TTRs totalling $32,410 in chip and cash exchanges;

b. one TTR totalling $12,000 for an account withdrawal; and

c. one TTR totalling $20,400 for an account deposit.

g. in 2018, Customer 13 was the subject of law enforcement enquiries at SCA; and

Particulars

For example, on 10 January 2018, SCA received a request from a law enforcement agency for Customer 13's gaming records, transactions and junket play. On 15 January 2018, SCA responded to the request.

h. SCA did not have adequate reason to believe that Customer 13's source of wealth or source of funds was sufficient to explain the gambling services (table 3, s 6 of the Act) provided to Customer 13 by SCA.

Particulars

See paragraph 516 above.

On and from 7 December 2016, SCA understood Customer 13's occupation to be as a restaurant franchisee entrepreneur.

At no time did SCA request source of wealth or source of funds information from Customer 13.

As SCA did not record Customer 13's individual gambling activity on junket programs they attended as a junket player, SCA was unable to determine whether Customer 13's gambling level was consistent with their source of wealth or source of funds.

SCA's determination of the ML/TF risks posed by Customer 13

735. SCA was unable to identify or assess the ML/TF risk posed by Customer 13 appropriately because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risk reasonably faced by SCA with respect to Customer 13.

a. On and from 7 December 2016, Customer 13 should have been recognised by SCA as a high risk customer for the purpose of the Act and Rules for the reasons pleaded above: see *Customer 13's risk profile.*

Particulars

Sections 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

b. At no time was Customer 13 rated high risk by SCA for the purpose of the Act and Rules.

Particulars

On 19 March 2017, Customer 13 was rated medium risk, which was not high risk for the purpose of the Act and Rules.

Monitoring of Customer 13's transactions

736. At no time did SCA apply appropriate transaction monitoring to Customer 13's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities;

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not make or keep appropriate records of designated services provided to junket representatives and junket players; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

SCA did not keep records of Customer 13's individual play on seven junkets.

Between 7 December 2016 and 2019, SCA recorded a total turnover of $5,400 for Customer 13, which was from their individual rated gambling activity only. During the same period, Customer 13 engaged in transactions totalling over $9,500,000 at SCA, including cash outs, buy-ins and account deposits and withdrawals.

See *Customer 13's risk profile* above.

c. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 13 through the junket channel.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

The review, update and verification of Customer 13's KYC information

737. SCA did not review, update or verify Customer 13's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 13, including the nature, extent and purpose of Customer 13's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 13's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out above, there were real risks that Customer 13's source of wealth and source of funds were not legitimate: see *Customer 13's risk profile*.

d. to the extent that SCA reviewed Customer 13's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 13.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

On 23 October 2021, SCA received an open source Dow Jones watchlist alert in respect to Customer 13, but resolved to close the alert.

There are no records of any further action taken in respect of reviewing Customer 13's KYC information that were appropriate having regard to the ML/TF risks pleaded above: see *Customer 13's risk profile* above.

On 22 March 2022, SCA issued a ban in respect of Customer 13 following investigations by the AML team and adverse open source media identified in respect of Customer 13.

Failure to apply appropriate due diligence suited to the high ML/TF risks

738. Had SCA conducted ongoing customer due diligence on and from 7 December 2016 by:

a. appropriately identifying and assessing the ML/TF risks posed by Customer 13;

b. applying appropriate risk-based transaction monitoring to Customer 13; and

c. appropriately reviewing and updating Customer 13's KYC information, having regard to the high ML/TF risks, SCA would likely have rated Customer 13 as a high risk customer for the purpose of the Act and Rules at a time before 22 March 2022 when Customer 13 was issued with a ban at SCA.

Particulars

Section 36(1)(a) of the Act, Rules 15.2 and 15.5 of the Rules.

739. Had SCA rated Customer 13 as a high risk customer for the purpose of the Act and Rules, it would have been required by the Act and Rules to apply the ECDD Program to Customer 13 at a time before 22 March 2022 when Customer 13 was issued with a ban at SCA.

Particulars

Rule 15.9 of the Rules.

Contravention of s 36 of the Act in respect of Customer 13

740. By reason of the matters pleaded at paragraphs 731 to 739 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 13 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2 and 15.5 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

741. By reason of the matters pleaded at paragraph 740, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 22 March 2022 with respect to Customer 13.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 14

742. Customer 14 was a customer of SCA during the relevant period.

Particulars

Customer 14 played on two junket programs at SCA in August 2017 and December 2018.

On 30 September 2020, SCA issued a ban in respect of Customer 14.

743. SCA provided Customer 14 with designated services within the meaning of table 1 and table 3, s 6 of the Act during the relevant period, including services connected to Customer 14's gambling as a junket player, facilitated through two different junket operators.

Particulars

SCA opened an FMA for Customer 14 (item 11, table 3, s 6 of the Act).

While a customer of SCA, Customer 14 remitted funds to their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 14's risk profile* below.

744. At all times from at least 16 August 2017, SCA was required to conduct ongoing customer due diligence in respect of Customer 14.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 14's risk profile

745. On and from at least 16 August 2017, Customer 14, and the provision of designated services by SCA to Customer 14, posed higher ML/TF risks because of the following red flags:

a. Customer 14 was a junket player who received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA through junket programs;

   i. between 16 August 2017 and 19 December 2018, Customer 14 was a player on two junket programs at SCA operated by two junket operators, being Customer 1 and Customer 9;

   ii. the combined total buy-in of these two junket programs was estimated at $5,947,305;

   iii. Customer 14 received a cheque for $1,350,000 from SCA authorised by Customer 1 following the junket program in December 2018; and

   iv. at no time did SCA record Customer 14's individual gambling activity on junket programs they attended as a junket player;

b. designated services provided to Customer 14 lacked transparency as the services were provided through the channel of junket programs at SCA;

Particulars

See paragraph 392 above.

c. at a time prior to August 2017, SCEG excluded Customer 14 from SCEG casinos due to Customer 14's behavioural issues at other Australian casinos;

Particulars

Due to this exclusion, Customer 14's visit as part of the 2017 junket program was personally approved by the President of International Business.

d. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 14 by remitting large amounts of money within the casino environment via their accounts;

Particulars

See paragraphs 232 to 312 above.

On 16 December 2018, Customer 14 received $700,000 into their SCA FMA from Customer 1's SCA FMA. SCA made these funds available to Customer 14.

e. Customer 14 was connected to other customers at SCA, including junket operators, junket players, foreign PEPs, players who posed higher ML/TF risks (such as Customer 1, Customer 9 and Customer 11) and players who SCA considered had acted suspiciously;

Particulars

In August 2017, Customer 14 played on a junket program operated by Customer 9 at SCA with Customer 11 (who was a foreign PEP).

In December 2018, Customer 14 played on a junket program at SCA operated by Customer 1.

From July 2019, SCA was aware of media reports that Customer 14 was a close associate and business partner of Customer 11.

By July 2019, SCA was aware that Customer 14 had been on board a private jet with Customer 11 which had been searched by a law enforcement agency in connection with suspicions of money laundering. By February 2022, SCA was aware that Customer 9 had also been on board the same private jet at the time it was searched.

See *Customer 1's risk profile,* above, *Customer 9's risk profile* above and *Customer 11's risk profile* above.

f. Customer 14 had access to private gaming rooms at SCA;

Particulars

See paragraph 145(e) above.

g. by 29 July 2019, open source media reports named Customer 14 as a person involved in serious organised and financial crime; and

Particulars

By October 2016, media reports named Customer 14 as the most lucrative private junket provider at another Australian casino.

On 29 July 2019, media reports from two major Australian newspapers named Customer 14 as an alleged international fugitive. The reports detailed that there had been law enforcement interest in Customer 14 from as early as 2016 in respect of international money laundering, and outlined Customer 14's role as a junket financier at another Australian casino. The reports revealed that in 2015, junkets operated by Customer 14 had turnover exceeding $1.45 billion at one Australian casino.

Media reports also identified Customer 14 as a business associate of Customer 11 (who was a foreign PEP) and Customer 12 (who was named as being involved in alleged human trafficking).

Media reports published between 31 July 2019 and 22 August 2019 detailed that Customer 14:

a. had been named in several civil and criminal cases in a foreign country, including for financial crimes since 2012;

b. was the subject of an international law enforcement agency red notice;

c. had links to organised crime;

d. set up a company to move large sums of money from a foreign country to Australia;

e. was suspected to be involved in foreign influence operations; and

f. was the subject of law enforcement probes by Australian law enforcement and government agencies.

In February 2020, it was reported that Customer 14 had been arrested overseas and deported to a foreign country for suspected money laundering and corruption offences.

h. SCA did not have adequate reason to believe that Customer 14's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 14 by SCA.

Particulars

See paragraph 516 above.

In August 2017, SCA recorded Customer 14's occupation as a 'property investor'. By December 2018, SCA recorded Customer 14's occupation as an 'Insurance Broker Manager'.

However, SCEG was aware from at least 2018 that Customer 14 was the guarantor and beneficial owner of a junket operating at SCEG New Zealand casinos.

SCEG did not take any steps to obtain or verify source of wealth and source of funds information from Customer 14 until after July 2019, following the publication of media reports alleging links between Customer 14 and organised crime.

SCA's determination of the ML/TF risks posed by Customer 14

746. On and from 13 September 2019 Customer 14 was rated by SCA as a high risk customer for the purpose of the Act and Rules.

747. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 14 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 14.

Monitoring of Customer 14's transactions

748. At no time did SCA apply appropriate transaction monitoring to Customer 14's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities;

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not make or keep appropriate records of designated services provided to junket players, including Customer 14; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

c. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 14 through the junket channel.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

The review, update and verification of Customer 14's KYC information

749. SCA did not review, update or verify Customer 14's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 14, including the nature, extent and purpose of Customer 14's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 14's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out above, there were higher ML/TF risks associated with Customer 14's source of wealth or source of funds: see *Customer 14's risk profile*.

d. to the extent that SCA reviewed Customer 14's KYC information, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 14.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

ECDD triggers in respect of Customer 14

750. SCA was required to apply the ECDD program to Customer 14 following any ECDD triggers in respect of Customer 14.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1) and 15.10 of the Rules.

751. Customer 14 was determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 14* above.

752. The matter pleaded at paragraph 751 was an ECDD trigger.

Particulars

See paragraphs 496 and 504 above.

753. SCA did not conduct appropriate risk-based ECDD with respect to Customer 14 following an ECDD trigger because:

a. on any occasion that SCA conducted ECDD in respect of Customer 14 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 14 and failed to appropriately consider whether the ML/TF risks posed by Customer 14 were within SCA's ML/TF risk appetite; and

Particulars

Rule 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

Following the 29 July 2019 media reports naming Customer 14 as a person involved in serious organised and financial crime, including in connection with other Australian casinos, SCEG drafted a series of memoranda about the media allegations and its relationship to SCEG customers: see paragraph 753.b below.

Following consideration of these memoranda, on 8 August 2019, SCEG determined that, 'in the absence of something more substantive' it was not necessary to conduct ECDD and that due diligence would be sufficient. It is not clear whether this was communicated to SCA.

It was not until 30 September 2020 that SCA issued a ban in respect of Customer 14.

The ECDD conducted by SCA did not have appropriate regard to Customer 14's higher ML/TF risks: see *Customer 14's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 14's source of funds and source of wealth.

By reason of the matters set out above, there were higher ML/TF risks associated with Customer 14's source of wealth or source of funds: see *Customer 14's risk profile*.

b. on any occasion prior to 30 September 2020 that senior management considered the higher ML/TF risks posed by Customer 14 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 14 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

On 1 August 2019, the SCEG AML Compliance and Intelligence Manager sent an internal memorandum to the SCEG Group General Manager for Regulatory Affairs and AML, which was copied to the SCA Director, General Counsel and Company Secretary about media

allegations regarding another Australian casino and the customers of SCEG named in those reports, including Customer 14.

The memorandum noted that SCEG had not supported Customer 14's application to be a junket operator due to Customer 14's undesirable behaviour at other Australian casinos.

On 2 August 2019, the SCEG General Manager of Regulatory Affairs and AML sent a memorandum to the SCEG General Counsel, which was copied to the AML Compliance and Intelligence Manager. The memorandum:

a. noted the allegations published in various media reports in July 2019; and

b. recommended that SCEG seek source of wealth and source of funds information from Customer 14 because:

    i. Customer 14 funded junkets at SCEG New Zealand casinos; and

    ii. the allegations of criminal activity were relevant to that junket operation and its risk profile.

On 8 August 2019, the SCEG General Manager of Regulatory Affairs advised the SCEG AML Compliance and Intelligence Manager, the SCEG General Counsel and the General Manager Legal, Compliance & Regulatory Affairs of their decision that:

a. Customer 14's risk profile should be elevated as a result of the media allegations, but that due diligence rather than ECDD should be conducted;

b. Customer 14 would be invited to comment on the allegations, and further consideration would be given to SCEG's business relationship with Customer 14 following their response; and

c. in the meantime, Customer 14's business relationship with SCEG could continue.

On 20 August 2019, the SCEG Group General Manager Regulatory Affairs and AML advised other SCEG and SCA personnel of their decision that:

a. the allegations in the media reports published in July 2019 were speculative and historical;

b. there was insufficient information in the media articles to suggest that Customer 14 or their junket operations at a SCEG New Zealand casino should be elevated to high risk and subject to ECDD before SCEG could continue to do business with them (this was despite the SCEG General Manager Regulatory Affairs and AML expressing the view on 8 August 2019 that Customer 14's risk profile should be elevated as a result of the media allegations, as noted above);

c. nevertheless, SCEG should ask Customer 14 about the allegations against them as part of SCEG's due diligence; and

d. notwithstanding the above, the due diligence should not have a bearing on SCEG's continued business relationship with either Customer 14 or their junket operations at a SCEG New Zealand casino at that point in time.

On 30 November 2019, a report by the SCEG Group General Manager Regulatory Affairs and AML noted that the operator of the junket funded by Customer 14 was suing SCEG over disputed costs relating to a jet charter used to bring the junket to a SCEG New Zealand casino. The report noted that there was no further appetite to conduct further business with the junket due to these proceedings. The decision to cease doing business with the junket funded by Customer 14 was due to commercial considerations. There is no evidence that in reaching this decision there was any consideration by SCEG or SCA of the higher ML/TF risks posed by Customer 14.

Customer 14 was arrested in a foreign country and deported to another foreign country in February 2020 in connection with money laundering and corruption offences.

However, it was not until 30 September 2020 that SCA issued a ban in respect of Customer 14.

Contravention of s 36 of the Act in respect of Customer 14

754. By reason of the matters pleaded at paragraphs 742 to 753 above, on and from 16 August 2017, SCA:

a. did not monitor Customer 14 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

755. By reason of the matters pleaded at paragraph 754, SCA contravened s 36(1) of the Act on and from 13 September 2019 to 30 September 2020 with respect to Customer 14.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 15

756. Customer 15 was a customer of SCA during the relevant period. SCA recorded turnover exceeding $400,000 for Customer 15, not including turnover as a junket player, which was not individually recorded.

Particulars

Customer 15 was a customer of SCA from at least 27 September 2016.

On 23 March 2022, SCA issued a ban in respect of Customer 15 following in-house investigations by the AML team and adverse open source media in respect of Customer 15.

757. SCA provided Customer 15 with designated services within the meaning of table 1 and table 3, s 6 of the Act during the relevant period including services connected to Customer 15's gambling as a junket player, facilitated through Customer 3's junket.

Particulars

On 27 September 2016, SCA opened an FMA for Customer 15 which was closed on 22 March 2022 (item 11, table 3, s 6 of the Act).

While a customer of SCA, Customer 15 remitted funds from their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 15's risk profile* below.

758. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 15.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 15's risk profile

759. On and from 7 December 2016, Customer 15, and the provision of designated services to Customer 15 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 15's risk profile during the relevant period

a. Customer 15 was a junket player who received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA through junket programs;

   i. between 7 December 2016 and 11 July 2017, Customer 15 was a player on 10 junkets at SCA operated by Customer 3 with Customer 12 as the junket representative;

   ii. at no time did SCA record Customer 15's individual gambling activity on junket programs they attended as a junket player;

b. designated services provided to Customer 15 lacked transparency as the services were provided through the channel of junket programs at SCA;

Particulars

See paragraph 392 above.

c. Customer 15 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs. Between 5 January 2017 and 26 April 2018, SCA recorded a high turnover estimated at $401,553 for Customer 15, with cumulative losses of $4,700;

Particulars

In 2017, Customer 15's recorded individual rated gambling activity at SCA was estimated as a buy-in of $35,500, turnover of $164,901 with losses of $4,300 for table games.

In 2018, Customer 15's recorded individual rated gambling activity at SCA was estimated as a buy-in of $131,400, turnover of $236,652 with losses of $400 for table games.

d. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 15 by remitting large amounts of money into and within the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCEG customer account channel and within the casino environment

On 18 January 2018, Company 7 acting on behalf of Customer 15 transferred AUD$626,792 to SCA through the SCEG Customer account channel. HKD$4,000,000 was transferred into an overseas SGEG account on behalf of Customer 15, which SCA deposited into Customer 15's FMA.

On 18 January 2018, Customer 15 transferred $626,792 from their SCA FMA to Customer 11's SCA FMA.

SCA determined the originator of funds was Customer 11, who used Company 7 to move funds out of a foreign country without government detection and Customer 15's account was used to further distance Customer 11 from the transaction.

e. Customer 15 was connected to other customers at SCA, including junket operators, junket players, foreign PEPs, players who posed higher ML/TF risks (such as Customer 2, Customer 3, Customer 11, Customer 12 and Customer 27) and players who SCA considered had acted suspiciously;

Particulars

Customer 15 was the personal assistant to Customer 11, and played on the junket operated by Customer 3, of which Customer 12 was the junket representative.

Customer 15 conducted chip exchanges involving Customer 2, Customer 11 and Customer 27.

See *Customer 2's risk profile* above*, Customer 3's risk profile* above*, Customer 11's risk profile* above*, Customer 12's risk profile* above and *Customer 27's risk profile* below.

f. Customer 15 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 22 January 2018 and 30 April 2018, SCA gave the AUSTRAC CEO three TTRs detailing incoming and outgoing payments made by Customer 15 totalling $1,263,584, which comprised:

a. one TTR totalling $10,000 for a chip and cash exchange;

b. one TTR totalling $626,792 for an account deposit; and

c. one TTR totalling $676,792 for an account withdrawal.

g. Customer 15 engaged in large and unusual transactions, which had no apparent economic or visible lawful purpose and appeared to be an attempt to disguise the source and beneficiary of funds;

Particulars

See paragraph 24 above.

For example, on 13 March 2018, Customer 15 was observed assisting in the exchange of $50,000 in chips between Customer 2, Customer 11 and Customer 27 and cashing those chips out on behalf of Customer 11.

Customer 15 was included in an internal report titled 'AML Unusual Changes in Betting – April' where SCA recorded Customer 15's turnover for April 2017.

h. Customer 15 had access to private gaming rooms at SCA;

Particulars

See paragraph 145(e) above.

Customer 15 had access to private gaming rooms at SCA, including the Grange Room and Horizon Suites.

i. by 30 July 2019, a media report named Customer 15 as a close friend of, and a director of a company registered by, Customer 11, who was alleged to be involved in organised crime and money laundering;

Particulars

The media report indicated that Customer 15 had no knowledge of what the company they were director of did and merely acted as a signatory for Customer 11. Customer 11, due to being a close relative of a high ranking foreign official, would not use their own name in some circumstances.

SCA's due diligence records suggest that SCA did not become aware of this report until 5 March 2020.

j. SCA did not have adequate reason to believe that Customer 15's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 15 by SCA.

Particulars

See paragraph 516 above.

At no time did SCA make enquiries regarding Customer 15's source of funds or source of wealth in circumstances where:

a. from at least 2018, SCA was aware that Customer 15 was Customer 11's personal assistant, even though Customer 15's occupation was listed as Assistant Trade Manager in SCA's records from 2016. SCA further suspected that Customer 11 used Customer 15 to distance Customer 11 from transactions through SCA; and

b. SCA was aware that Customer 15 was associated with a number of individuals who posed higher ML/TF risks including PEPs.

SCA's determination of the ML/TF risks posed by Customer 15

760. SCA was unable to appropriately identify or assess the ML/TF risks posed by Customer 15 because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 15.

a. On and from 18 January 2018, Customer 15 should have been recognised by SCA as a high risk customer for the purpose of the Act and Rules for the reasons pleaded above: see *Customer 15's risk profile.*

Particulars

Sections 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

b. At no time was Customer 15 rated high risk by SCA for the purpose of the Act and Rules.

Monitoring of Customer 15's transactions

761. At no time did SCA apply appropriate transaction monitoring to Customer 15's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities;

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not make or keep appropriate records of designated services provided to junket players; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

c. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 15 through:

i. the junket channel; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

ii. the SCEG customer account channel, which was a high risk remittance channel.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 15's KYC information

762. SCA did not review, update or verify Customer 15's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 15, including the nature, extent and purpose of Customer 15's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 15's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks;

Particulars

By reason of the matters set out above, there were real risks that Customer 15's source of wealth and source of funds were not legitimate: see *Customer 15's risk profile*.

d. to the extent that SCA reviewed Customer 15's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 15.

Particulars

Section 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

Failure to apply appropriate due diligence suited to the high ML/TF risks

763. Had SCA conducted ongoing customer due diligence on and from 7 December 2016 by:

a. appropriately identifying and assessing the ML/TF risks posed by Customer 15;

b. applying appropriate risk-based transaction monitoring to Customer 15; and

c. appropriately reviewing and updating Customer 15's KYC information, having regard to the high ML/TF risks,

SCA would have been required by the Act and Rules to apply the ECDD Program to Customer 15 at a time before the date of the ECDD triggers pleaded below: see *ECDD triggers in respect of Customer 15*.

ECDD triggers in respect of Customer 15

764. SCA was required to apply the ECDD program to Customer 15 following any ECDD triggers in respect of Customer 15.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(3) and 15.10 of the Rules.

765. Customer 15 was the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period.

Particulars

On 23 January 2018, SCA gave the AUSTRAC CEO an SMR with respect to Customer 15.

766. The matter pleaded at paragraph 765 was an ECDD trigger.

Particulars

See paragraphs 496 and 506 above.

767. SCA did not conduct appropriate risk-based ECDD with respect to Customer 15 following the ECDD trigger because:

a. on each occasion prior to March 2022 that SCA conducted ECDD in respect of Customer 15 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 15 and failed to appropriately consider whether the ML/TF risks posed by Customer 15 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501, 511 and 516 to 517 above.

On 27 February 2018 and 5 March 2020, SCA conducted ECDD in respect of Customer 15.

The ECDD report from March 2020 identified that Customer 15 had been reported in the media to be a director of a company registered by Customer 11, but that Customer 15 had no knowledge of what the company did and merely acted as a signatory for Customer 11.

The ECDD conducted by SCA did not have appropriate regard to Customer 15's higher ML/TF risks: see *Customer 15's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 15's source of funds or source of wealth.

By reason of the matters set out above, there were real risks that Customer 15's source of wealth and source of funds were not legitimate: see *Customer 15's risk profile*.

It was not until 23 March 2022 that SCA issued a ban in respect of Customer 15.

b. on any occasion prior to 23 March 2022 that senior management considered the higher ML/TF risks posed by Customer 15 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 15 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

It was not until September 2021 that an internal review recommended that SCA terminate the business relationship with Customer 15 and ban them from SCA.

It was not until February 2022 that SCA's AML team sent an email to the General Manager AML proposing to ban Customer 15 banned due to their association with Customer 11.

On 23 March 2022 SCA issued a ban in respect of Customer 15.

Contravention of s 36 of the Act in respect of Customer 15

768. By reason of the matters pleaded at paragraphs 756 to 767 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 15 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

769. By reason of the matters pleaded at paragraph 768, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 23 March 2022 with respect to Customer 15.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 16

770. Customer 16 was a customer of SCA during the relevant period. Between 7 December 2016 and 22 February 2018, SCA recorded turnover exceeding $162,000,000 for Customer 16.

Particulars

Customer 16 was a customer of SCA from at least 10 July 2015.

On 22 February 2018, SCA issued a three-month ban in respect of Customer 16 at the direction of the SCA AML team. SCA extended the ban for another six months on 22 May 2018 and a further 12 months on 22 November 2018.

On 22 November 2019, SCA issued a permanent ban in respect of Customer 16 at the direction of the SCA AML team.

771. SCA provided Customer 16 with designated services within the meaning of table 1 and table 3, s 6 of the Act during the relevant period including services connected to Customer 16's gambling as an individual commission player.

Particulars

Before 7 December 2016, SCA opened an FMA for Customer 16 which remained open as at 28 October 2022 (item 11, table 3, s 6 of the Act).

Between 4 November 2015 and 21 February 2018, SCA provided lines of credit for Customer 16 on 106 occasions, 105 of which had a limit of $20,000, and one of which had a limit of $25,000 (item 6, table 1, s 6 of the Act).

See *Customer 16's risk profile* below.

772. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 16.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 16's risk profile

773. On and from 7 December 2016, Customer 16, and the provision of designated services to Customer 16 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 16's risk profile prior to the relevant period

a. by 7 December 2016, Customer 16 had the following risk history:

i. Customer 16 had received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket or individual commission programs. Between 10 July 2015 and 6 December 2016, SCA recorded a high buy-in estimated at $16,060,050 for Customer 16, turnover of $3,012,437 and with losses of $719,505;

Particulars

In the 2016 financial year, Customer 16's recorded individual rated gambling activity for table games at SCA was estimated as a buy-in of $9,622,130, turnover of $2,386,265 with losses of $633,685; and

Between 1 July 2016 to 6 December 2016, Customer 16's recorded individual rated gambling activity for table games at SCA was estimated as a buy-in of $6,437,920, turnover of $626,173 with losses of $85,820.

ii. Customer 16 had received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA on individual commission programs, and an estimated commission of $5,624,852 was recorded as payable by SCA to Customer 16 on individual commission programs prior to 7 December 2016;

Particulars

In the 2016 financial year, Customer 16's recorded gambling activity from play on individual commission programs at SCA was estimated as a buy-in of $4,757,176, cash turnover of $70,200,489 with losses of $381,015.

In the 2016 financial year, a commission of $421,203 was payable by SCA to Customer 16 from play on individual commission programs.

Between 1 July 2016 and 6 December 2016, a commission of $5,203,649 was estimated as paid by SCA to Customer 16 from play on individual commission programs.

iii. Customer 16 frequently transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 7 May 2009 and 5 December 2016, SCA gave the AUSTRAC CEO 428 TTRs detailing incoming and outgoing payments made by Customer 16 totalling $16,085,090, which comprised:

a. 237 TTRs totalling $8,691,804 in chip and cash exchanges;

b. 101 TTRs totalling $3,755,933 in account deposits;

c. 53 TTRs totalling $2,006,214 in account withdrawals;

d. 12 TTRs totalling $280,000 in marker redemptions;

e. four TTRs totalling $44,886 in premium player commissions/rebates;

f. 11 TTRs totalling $831,787 in other cash transactions; and

g. 10 TTRs totalling $474,465 in international funds transfers out of Australia.

iv. SCA frequently provided Customer 16 with significant amounts of credit upon request, up to limits of $25,000;

Particulars

See paragraphs 321 to 323, and 342 above.

Between 4 November 2015 and 6 December 2016, SCA provided Customer 16 with at least $1,085,000 in credit, consisting of 53 lines of credit with limits of $20,000 each and one line of credit with a $25,000 limit.

v. between 3 September 2015 and 6 December 2016, Customer 16 made buy-ins for individual gaming and individual commission programs with 72 cheques totalling $1,540,000, one telegraphic transfer of $15,000 and one transfer from Customer 16's FMA in the amount of $5,000, and was paid out by SCA with 73 cheques totalling $1,560,000;

Particulars

In September 2015, SCA issued a cheque to Customer 16 in the amount of $30,000.

In November 2015, SCA issued four cheques to Customer 16, each in the amount of $20,000, totalling $80,000.

In December 2015, SCA issued seven cheques to Customer 16 each in the amount of $10,000, and eight cheques to Customer 16, each in the amount of $20,000. A total of 15 cheques were issued to

Customer 16 by SCA during this period, for a total amount of $230,000.

In January 2016, SCA issued three cheques to Customer 16 each in the amount of $20,000, and one cheque to Customer 16 in the amount of $50,000. A total of four cheques were issued to Customer 16 by SCA during this period, for a total amount of $110,000.

In February 2016, SCA issued six cheques to Customer 16 each in the amount of $20,000, and one cheque to Customer 16 in the amount of $50,000. A total of seven cheques were issued to Customer 16 by SCA during this period, for a total amount of $170,000.

In March 2016, SCA issued four cheques to Customer 16 each in the amount of $20,000, totalling of $80,000.

In April 2016, SCA issued one cheque to Customer 16 in the amount of $20,000 and one cheque to Customer 16 in the amount of $50,000, totalling $70,000.

In May 2016, SCA issued two cheques to Customer 16, each in the amount of $20,000, totalling $40,000.

In June 2016, SCA issued six cheques to Customer 16 each in the amount of $20,000, and one cheque to Customer 16 in the amount of $50,000. A total of seven cheques were issued to Customer 16 by SCA during this period, for a total amount of $170,000.

In July 2016, SCA issued two cheques to Customer 16, each in the amount of $20,000, and one cheque to Customer 16 in the amount of $40,000. A total of three cheques were issued to Customer 16 by SCA during this period, for a total amount of $80,000.

In August 2016, SCA issued eight cheques to Customer 16, each in the amount of $20,000, totalling $160,000.

In September 2016, SCA issued seven cheques to Customer 16, each in the amount of $20,000, totalling $140,000.

In October 2016, SCA issued three cheques to Customer 16, each in the amount of $20,000, totalling $60,000.

In November 2016, SCA issued five cheques to Customer 16, each in the amount of $20,000, totalling $100,000.

Between 1 December 2016 and 6 December 2016, SCA issued two cheques to Customer 16, each in the amount of $20,000, totalling $40,000.

Customer 16's risk profile during the relevant period

b. Customer 16 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs or individual commission programs. Between 7 December 2016 and 21 February 2018, SCA recorded a high buy-in

estimated at $13,461,215 for Customer 16, turnover of $184,297 and with losses of $1,527,735 for non-commission play;

Particulars

Between 7 December 2016 and 30 June 2017, Customer 16's recorded individual rated gambling activity for table games at SCA was estimated as a buy-in of $6,593,645, turnover of $120,556 with losses of $675,930.

In the 2018 financial year, Customer 16's recorded individual rated gambling activity for table games at SCA was estimated as a buy-in of $11,000, turnover of $24,002 with losses of $15,230.

c. Customer 16 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA from play on individual commission programs. Between 1 July 2016 and 30 June 2018, SCA recorded Customer 16's buy-in on individual commission programs as $8,758,108, with a cash turnover of $153,777,270, and with losses of $1,478,925. A commission of $898,680 was recorded as payable by SCA to Customer 16 on individual commission programs for this period;

Particulars

In the 2017 financial year, Customer 16's recorded play on individual commission programs at SCA was estimated as a buy-in of $5,544,200, cash turnover of $101,795,526, with losses of $642,350. A commission of $610,296 was payable by SCA to Customer 16 from play on individual commission programs for this period.

In the 2018 financial year, Customer 16's recorded play on individual commission programs at SCA was estimated as a buy-in of $3,213,908, cash turnover of $51,981,744, with losses of $836,575. A commission of $288,383 was payable by SCA to Customer 16 from play on individual commission programs for this period.

These figures only reflect gaming which took place up to February 2018, as Customer 16 was banned from SCA from 22 February 2018.

d. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 16 by remitting large amounts of money into, out of and within the casino environment via their accounts, including through high risk remittance channels:

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

SCA made money available to Customer 16 in the following transactions:

a. Between 7 December 2016 and 21 February 2018, Customer 16 transferred approximately $9,440,765 from their personal bank account in Australia to their SCA FMA in approximately 290 separate transactions.

b. In two transactions on 18 January 2017 and 11 September 2017, SCA accepted transfers totalling $85,469 from overseas casinos on Customer 16's behalf.

SCA accepted instructions to transfer funds from Customer 16's accounts for the following transactions:

a. Between 7 December 2016 and 23 February 2018, Customer 16 transferred $5,189,177 from their SCA FMA to their personal bank account in Australia in approximately 179 separate transactions.

b. In three transactions between 16 January 2017 and 6 September 2017, SCA transferred a total of $223,000 from its customer account to other overseas casinos on Customer 16's behalf.

Remittances within the casino environment

SCA made money available to Customer 16 in the following transactions:

a. On 21 September 2017, Customer 16 received $30,000 into their SCA FMA from Person 13's SCA FMA

b. On 18 November 2017, Customer 16 received $50,000 into their SCA FMA from Person 13's SCA FMA.

SCA accepted instructions to transfer funds from Customer 16's accounts for the following transactions:

a. On 21 September 2017, Customer 16 transferred $30,000 from their SCA FMA to Person 13's SCA FMA.

b. On 18 November 2017, Customer 16 transferred $20,000 from their SCA FMA to Person 13's SCA FMA.

c. On 18 November 2017, Customer 16 transferred $50,000 from their SCA FMA to Person 13's SCA FMA.

e. Customer 16 transacted using large amounts of cash;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 12 December 2016 and 27 February 2018, SCA gave the AUSTRAC CEO 69 TTRs detailing incoming and outgoing payments made by Customer 16 totalling $1,872,024, which comprised:

a. two TTRs totalling $49,500 in chip and cash exchanges;

b. 48 TTRs totalling $1,205,409 in account deposits;

c. 11 TTRs totalling $428,206 in account withdrawals;

d. five TTRs totalling $100,000 in marker redemptions;

e. one TTR totalling $44,460 for the purchase of foreign currency; and

f. two TTRs totalling $44,449 in premium player commissions/rebates.

f. between 7 December 2016 and 21 February 2018, SCA provided Customer 16 with significant amounts of credit upon request, up to limits of $20,000;

Particulars

See paragraphs 321 to 323, and 342 above.

Between 7 December 2016 and 21 February 2018, SCA provided Customer 16 with at least $1,000,000 in credit, consisting of 51 lines of credit with limits of $20,000 each.

g. between 7 December 2016 and 22 February 2018, Customer 16 made buy-ins for individual gaming and individual commission programs with 65 cheques totalling $1,364,000, and one transfer from Customer 16's FMA in the amount of $6,000, and was paid out by SCA with 65 cheques totalling $1,370,000;

Particulars

Between 7 December 2016 and 31 December 2016, SCA issued seven cheques to Customer 16 each in the amount of $20,000, totalling $140,000.

In January 2017, SCA issued one cheque to Customer 16 in the amount of $20,000.

In February 2017, SCA issued six cheques to Customer 16 each in the amount of $20,000, totalling $120,000.

In March 2017, SCA issued seven cheques to Customer 16 each in the amount of $20,000, totalling of $140,000.

In April 2017, SCA issued three cheques to Customer 16 each in the amount of $20,000, totalling $60,000.

In June 2017, SCA issued two cheques to Customer 16 each in the amount of $20,000, totalling $40,000.

In July 2017, SCA issued seven cheques to Customer 16 each in the amount of $20,000, and one cheque to Customer 16 in the amount of $50,000. A total of eight cheques were issued to Customer 16 by SCA during this period, totalling $190,000.

In September 2017, SCA issued five cheques to Customer 16 each in the amount of $20,000, totalling $100,000.

In October 2017, SCA issued four cheques to Customer 16 each in the amount of $20,000, and one cheque to Customer 16 in the amount of $100,000. A total of five cheques were issued to Customer 16 by SCA during this period, totalling $180,000.

In November 2017, SCA issued five cheques to Customer 16 each in the amount of $20,000, and one cheque to Customer 16 in the

amount of $50,000. A total of six cheques were issued to Customer 16 by SCA during this period, totalling $150,000.

In December 2017, SCA issued two cheques to Customer 16 each in the amount of $20,000, totalling $40,000.

In January 2018, SCA issued two cheques to Customer 16 each in the amount of $20,000, totalling $40,000.

In February 2018, SCA issued three cheques to Customer 16 each in the amount of $20,000, totalling $60,000.

h. in 2018, Customer 16 was the subject of law enforcement enquiries on five occasions at SCA;

Particulars

On 12 January 2018, a law enforcement agency informed SCA that Customer 16 was a person of interest in an investigation into suspected money laundering.

On 18 January 2018, 5 February 2018, 7 February 2018 and 21 February 2018, SCA received further requests for information from the law enforcement agency regarding Customer 16.

i. SCA did not have adequate reason to believe that Customer 16's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 16 by SCA.

Particulars

See paragraph 516 above.

On 2 September 2015, Customer 16 informed SCA that they ran an information technology company.

Between 2016 and 2018, Customer 16's buy-in exceeded $22,100,000.

At no time did SCA request source of wealth or source of funds information from Customer 16.

In January 2018, SCA received information from a law enforcement agency that Customer 16 was 'unemployed'.

At no time was SCA's understanding of Customer 16's source of wealth or source of funds commensurate with the high financial and gambling services that they received at SCA.

SCA's determination of the ML/TF risks posed by Customer 16

774. On and from 28 July 2016, Customer 16 was rated by SCA as a high risk customer for the purpose of the Act and Rules.

Particulars

On 14 October 2021, Customer 16 was rated significant risk by SCA, which was high risk for the purpose of the Act and Rules.

775. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 16 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 16.

Monitoring of Customer 16's transactions

776. At no time did SCA apply appropriate transaction monitoring to Customer 16's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 16 through the SCA customer account channel, which was a high risk remittance channel.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 16's KYC information

777. SCA did not review, update or verify Customer 16's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 16, including the nature, extent and purpose of their transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 16's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks;

Particulars

By reason of the matters set out above, there were higher ML/TF risks associated with Customer 16's source of wealth or source of funds: see *Customer 16's risk profile*.

d. to the extent that SCA reviewed Customer 16's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 16.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

ECDD triggers in respect of Customer 16

778. SCA was required to apply the ECDD program to Customer 16 following any ECDD triggers in respect of Customer 16.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

779. Customer 16 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period;

Particulars

On 12 February 2018, SCA gave the AUSTRAC CEO one SMR with respect to Customer 16.

b. determined by SCA to be high risk for the purpose of the Act and Rules prior to the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 16* above.

780. Each matter pleaded at paragraph 779 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

781. SCA did not conduct appropriate risk-based ECDD with respect to Customer 16 following an ECDD trigger because:

a. on each occasion prior to 22 February 2018 that SCA conducted ECDD in respect of Customer 16 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 16 and failed to appropriately consider whether the ML/TF risks posed by posed by Customer 16 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

On 22 February 2018, SCA issued a temporary ban in respect of Customer 16.

On 26 September 2019, some 18 months after SCA issued a ban in respect of Customer 16, SCA conducted an ECDD screening in respect of Customer 16 which identified that Customer 16 was a convicted drug trafficker: SMR dated 9 February 2018.

On 11 October 2021, SCA conducted an ECDD screening in respect of Customer 16 which recommended that SCA terminate its business relationship with Customer 16 and issue a permanent ban in respect of Customer 16.

On 14 October 2021, SCA raised Customer 16's risk rating to 'significant', which maintained their rating as a high risk customer for the purpose of the Act and Rules.

The ECDD conducted by SCA prior to Customer 16's ban in February 2018 did not have appropriate regard to Customer 16's higher ML/TF risks: see *Customer 16's risk profile* above.

The ECDD conducted by SCA prior to Customer 16's ban in February 2018 did not have appropriate regard to the higher ML/TF risks posed by Customer 16's source of funds or source of wealth.

By reason of the matters set out above, there were higher ML/TF risks associated with Customer 16's source of wealth or source of funds: see *Customer 16's risk profile*.

b. on any occasion prior to 22 February 2018 that senior management considered the higher ML/TF risks posed by Customer 16 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 16 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

Between 23 February 2017 and 1 May 2018, Customer 16 was mentioned in four 'Transaction Monitoring Overview' reports for the period 23 February 2017 to 1 May 2018. These reports were provided to SCA's AML/CTF Senior Management Group for discussion at their meeting.

It was not until 22 February 2018 that SCA issued a temporary ban in respect of Customer 16.

Contravention of s 36 of the Act in respect of Customer 16

782. By reason of the matters pleaded at paragraphs 770 to 781 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 16 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

783. By reason of the matters pleaded at paragraph 782, SCA contravened section 36(1) of the Act on and from 7 December 2016 to 22 February 2018 with respect to Customer 16.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 17

784. Customer 17 was a customer of SCA during the relevant period. Between 7 December 2016 and 9 August 2021, SCA recorded turnover exceeding $100,000,000 for Customer 17.

Particulars

Customer 17 was a customer of SCA from at least 2 October 2015.

On 9 August 2021, SCA issued a ban in respect of Customer 17 at the direction of the SCA AML team.

785. SCA provided Customer 17 with designated services within the meaning of tables 1 and 3, s 6 of the Act during the relevant period, including services connected to Customer 17's gambling as an individual commission player.

Particulars

Prior to the relevant period, SCA opened an FMA for Customer 17 which remained open as at 28 October 2022 (item 11, table 3, s 6 of the Act).

While a customer of SCA, Customer 17 remitted funds to and from their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 17's risk profile* below.

786. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 17.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 17's risk profile

787. On and from 7 December 2016, Customer 17, and the provision of designated services to Customer 17 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 17's risk profile prior to the relevant period

a. by 7 December 2016, Customer 17 had the following risk history:

i. SCA had formed suspicions for the purposes of s 41 of the Act with respect to Customer 17;

Particulars

SCA gave the AUSTRAC CEO an SMR on one occasion on 9 May 2015.

The SMR reported that on 8 May 2015, $150,000 was received from a third-party company account for Customer 17. The company had an Australian address.

ii. Customer 17 had received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket or individual commission programs. Between 2 October 2015 and 29 September 2016, SCA recorded a high buy-in estimated at $9,138,030 for Customer 17 on table games, with turnover of $1,270,749 and with losses of $1,555,970;

Particulars

In the 2016 financial year, Customer 17's recorded individual rated gambling activity for table games at SCA was estimated as a buy-in of $600,600, cash turnover of $425,358 and with losses of $87,300.

Between 1 July 2016 and 6 December 2016, Customer 17's recorded individual rated gambling activity for table games at SCA was estimated as a buy-in of $5,447,930, cash turnover of $1,206,822 and with losses of $1,156,030.

iii. Customer 17 had received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA from play on individual commission programs, and an estimated commission of $490,699 was recorded as payable by SCA to Customer 17;

Particulars

In the 2016 financial year, Customer 17's recorded gambling activity on individual commission program at SCA was estimated as a buy-in of $809,050, cash turnover of $31,650,650 with losses of $354,705. An estimated commission of $189,904 was payable by SCA to Customer 17 from play on individual commission programs.

Between 1 July 2016 and 6 December 2016, Customer 17's recorded gambling activity on individual commission programs was estimated as a buy-in of $809,050, cash turnover of $50,132,200 with losses of $1,083,865. An estimated commission of $300,795 was payable by SCA to Customer 17 from play on individual commission programs in this period.

iv. Customer 17 had engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose

Particulars

On 29 May 2016, SCA's CCTV cameras captured exchanges of chips used specifically in an individual commission program between Customer 17 and Customer 2:

a. Customer 17 twice handed $5,000 in chips to Customer 2 totalling $10,000.

b. A short time later, Customer 17 received chips from Customer 2 totalling $51,000, comprising 10 $5,000 chips and one $1,000 chip.

c. A short time after this, Customer 17 handed chips to Customer 2 totalling $20,000 comprising four $5,000 chips.

d. Less than 10 minutes later, Customer 17 received $100 in chips from Customer 2.

e. These exchanges happened within the space of 35 minutes.

v. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 17 by remitting large amounts of money into the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

SCA made money available to Customer 17 in the following transactions:

a. On 24 May 2016, Company 3 deposited $200,000 into an account held by SCA in Australia, which SCA made available to Customer 17 and deposited into Customer 17's FMA.

b. On 4 July 2016, Company 3 deposited $200,000 into an account held by SCA in Australia, which SCA made available to Customer 17 and deposited into Customer 17's FMA.

c. On 15 August 2016, Customer 17 transferred $500,000 from their personal bank account in Australia to their SCA FMA via an SCA bank account.

vi. Customer 17 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 11 August 2014 and 30 September 2016, SCA gave the AUSTRAC CEO 159 TTRs detailing incoming and outgoing payments made by Customer 17 totalling $5,944,632 which comprised:

a. 107 TTRs totalling $2,434,540 in chip and cash exchanges;

b. 29 TTRs totalling $2,399,162 in account deposits;

c. 19 TTRs totalling $1,013,930 in account withdrawals; and

d. four TTRs totalling $97,000 in premium player commissions/rebates.

Customer 17's risk profile during the relevant period

b. Customer 17 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket or individual commission programs. Between 7 December 2016 and 19 February 2020, SCA recorded a high buy-in estimated at $11,953,830 for Customer 17, turnover of $302,476 and with losses of $1,147,575 for non-commission play;

Particulars

Between 7 December 2016 and 30 June 2017, Customer 17's recorded individual rated gambling activity for table games at SCA was estimated as a buy-in of $2,405,650, turnover of $146,162 and with wins of $56,525.

In the 2018 financial year, Customer 17's recorded individual rated gambling activity at SCA was estimated as a buy-in of $77,700, turnover of $94,841 and with wins of $47,500.

In the 2019 financial year, Customer 17's recorded individual rated gambling activity at SCA was estimated as a buy-in of $67,000, turnover of $168 and with wins of $19,800.

In the 2020 financial year, despite closures related to the COVID-19 pandemic, Customer 17's recorded individual rated gambling activity at SCA was estimated as a buy-in of $8,200 with no recorded turnover or wins or losses.

c. Customer 17 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA from play on individual commission programs. Between 1 July 2016 and 30 June 2020, SCA recorded Customer 17's cumulative buy-in on individual commission programs as $5,775,309, cash turnover of $150,107,305 and with losses of $2,354,940. A commission of $873,634 was recorded as payable by SCA to Customer 17 through individual commission programs for this period;

Particulars

Between 7 December 2016 and 30 June 2017 SCA recorded that commissions of at least $115,204 were payable by SCA to Customer 17 from play on individual commission programs.

In the 2017 financial year, Customer 17's recorded play on individual commission programs at SCA was estimated as a buy-in of $2,182,000, cash turnover of $69,333,400 and with losses of $1,089,640. A commission of $416,000 was payable by SCA to Customer 17 from play on individual commission programs for this period.

In the 2018 financial year, Customer 17's recorded play on individual commission programs at SCA was estimated as a buy-in of

$1,704,100, cash turnover of $41,706,343 and with losses of $229,975. A commission of $232,818 was payable by SCA to Customer 17 from play on individual commission programs for this period.

In the 2019 financial year, Customer 17's recorded play on individual commission programs at SCA was estimated as a buy-in of $1,494,209, cash turnover of $27,740,718 and with losses of $1,223,720. A commission of $162,466 was payable by SCA to Customer 17 from play on individual commission programs for this period.

In the 2020 financial year, despite closures related to the COVID-19 pandemic, Customer 17's recorded play on individual commission programs at SCA was estimated as a buy-in of $395,000, cash turnover of $11,326,844 and with wins of $188,395. A commission of $62,350 was payable by SCA to Customer 17 from play on individual commission programs for this period.

d. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 17 by remitting large amounts of money into and within the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

SCA made money available to Customer 17 in the following transactions.

Between 23 December 2016 and 23 July 2019, third parties acting on behalf of Customer 17 transferred a total of $3,600,629 to SCA through the SCA Customer account channel.

On 18 August 2018, Customer 17 transferred $500,000 from their personal bank account in Australia to their SCA FMA.

Remittances within the casino environment

SCA made money available to Customer 17 in the following transactions.

On 4 August 2017, Customer 17 received $30,000 into their SCA account from another customer following settlement of that customer's program,

On 30 October 2017, Customer 17 received $139,861 into their SCA account from another customer's SCA FMA.

e. SCA was aware that Customer 17 had engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

Particulars

On 22 May 2017, Customer 17 exchanged 20 $1,000 CCF chips with Customer 2 in return for four $5,000 cash chips. Customer 17 then

attended the Platinum Cage and used the cash chips they had just obtained to make a $20,000 buy-in.

On 2 August 2017, Customer 17 handed cash to two associates, in the amounts of $20,000 and $25,000 respectively.

On 15 August 2017, Customer 17 handed $10,000 in cash to Person 3, who used the money for gambling. Later that evening, Customer 17 handed $10,000 in cash to Person 3, who again used the money for gambling.

On 20 February 2018, an SCA Gaming Operations Shift Manager reported that Customer 17 had been handing non-negotiable chips to Customer 2, which was in breach of both customers' individual program agreements. The shift manager stated that any further instances would result in SCA ceasing both customers' gaming, and that Customer 2 had been informed of this.

On 24 February 2018, Customer 17 removed $30,000 in non-negotiable chips from a gaming table and passed them under the table to Customer 2. Customer 2 then commenced play with the chips.

On 27 February 2018, Customer 17 made a buy-in for a $50,000 CPV at SCA. Immediately after the transaction was completed, Customer 17 handed the chips to Customer 2. Customer 2 then commenced gaming using the chips.

On 10 November 2018, Customer 17 transferred $200,000 to Customer 2's FMA. On the same day, Customer 2 withdrew the full amount and deposited the funds into their individual commission program account.

On 10 August 2019, Customer 17 transferred $100,000 to Customer 2's FMA. On the same day, Customer 2 withdrew the full amount and deposited the funds into their individual commission program account.

On 11 August 2019, Customer 17 transferred $70,000 to Customer 2's FMA. On the same day, Customer 2 withdrew the full amount.

On 29 January 2020, Customer 17 transferred $50,000 to Customer 2's FMA. On the same day, Customer 2 withdrew the full amount via a cash out in chips.

f. Customer 17 was connected to other customers at SCA, including players who posed higher ML/TF risks such as Customer 2 and players who SCA considered had acted suspiciously;

Particulars

On 13 January 2017, Customer 17 and Customer 2 approached the Grange Cage together with chips totalling $50,000. Customer 2 claimed that the chips were theirs. SCA approved a cash out of $25,000. Shortly afterwards, Customer 17 approached the Grange Cage with chips totalling $25,000 to cash out. When SCA staff asked

whether the chips were Customer 2's, Customer 17 claimed that the chips belonged to them. However, SCA staff noted that Customer 17 had settled their own program about 30 minutes before with a final payout of $609.

On 23 January 2017, SCA noted that Customer 17 and Customer 2 were close associates with suspected business ties to each other.

On 22 May 2017, Customer 17 and Customer 2 were playing on a commission program at SCA where CCF chips were used. Customer 2 also held cash chips of at least $50,000 on the day. Customer 2 exchanged their cash chips for the CCF chips held by Customer 17 in the amount of $20,000: SMR dated 24 May 2017.

On 23 May 2017, Customer 17 exchanged $30,000 in cash chips for cash and gave the cash to Customer 2: SMR dated 24 May 2017.

On 1 June 2017, Customer 17 was handed $20,000 in cash by Person 14.

See *Customer 2's risk profile*, above.

g. Customer 17 transacted using large amounts of cash and cash that appeared suspicious, including large volumes of cash in plastic bags at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 28 December 2016 and 31 January 2020, SCA gave the AUSTRAC CEO 152 TTRS detailing incoming and outgoing payments made by Customer 17 totalling $7,565,614, which comprised:

a. 84 TTRs totalling $1,739,470 in chip and cash exchanges;

b. 28 TTRs totalling $3,800,697 in account deposits;

c. 39 TTRs totalling $1,825,448 in account withdrawals; and

d. 13 TTRs totalling $20,646 in premium player commissions/rebates.

Large and suspicious cash transactions

On 2 August 2017, Customer 17 conducted a number of threshold transactions after a win of approximately $100,000: SMR dated 7 August 2017.

On 13 February 2020, Customer 17 attended SCA with $100,000 comprised of $50 notes in garbage bags, and attempted to buy-in to a program using the cash from the garbage bags. When SCA asked Customer 17 to complete a Source of Funds Declaration, Customer 17 then removed $3,000 in cash from garbage bags to deposit $97,000 in cash. Once Customer 17 was informed that SCA would not be accepting the cash until a completed Source of Funds

Declaration was provided, Customer 17 removed the cash and did not proceed with the deposit and instead left the premises with the cash: SMR dated 17 February 2020.

On 14 February 2020, Customer 17 attempted to buy-into a program with $80,000 in $50 notes in a garbage bag. SCA asked Customer 17 to complete a Source of Funds Declaration form. Customer 17 completed the Source of Funds Declaration stating that the source of the funds was previous winnings from an SCA program in March 2019. SCA considered the Source of Funds Declaration was not credible as the March 2019 settlement was paid in $100 notes: SMR dated 17 February 2020.

h. Customer 17 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including structuring with players who posed higher ML/TF risks (such as Customer 24) and other players in respect of whom SCA had formed suspicions;

Particulars

See paragraph 24 above.

On the following occasions, Customer 17 was involved in transactions indicative of the ML/TF typology of structuring:

a. on 3 August 2017, Customer 17 handed $19,800 in cash to another SCA customer. The other customer then conducted two buy-in transactions of $9,900 each.

b. on 10 August 2017, Customer 24 performed 18 cash outs of CCF chips on behalf of Customer 17. The 18 transactions were close in timing and each was below the reporting limit.

i. SCA did not have adequate reason to believe that Customer 17's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 17 by SCA.

Particulars

See paragraph 516 above.

On 10 March 2015, a note was recorded in SCA's Bally system stating that Customer 17's occupation was as a 'managing director'.

On 19 July 2016, a note was recorded in SCA's iTrak report that Customer 17 was a shareholder of a foreign company and in a business partnership with Customer 2.

On 16 January 2017, a note was recorded in SCA's iTrak report that Customer 17 was 'heavily involved in a construction machinery company' that was in a business partnership with Customer 2.

On 7 March 2019, a note was recorded in SCA's Bally system stating that SCA required a better occupation description for Customer 17 due to number of threshold transactions being conducted by Customer 17. The note also stated that Customer 17 was reluctant to provide details regarding their occupation.

On 14 February 2020, Customer 17 provided a Source of Funds Declaration to SCA. Customer 17 stated that they were a 'Construction Machinery Director' and their source of funds was "cash out from previous program".

On 15 August 2021, Customer 17 refused SCA's request to provide a Source of Wealth Declaration. SCA noted that Customer 17 was a key partner in Customer 2's company.

At no time was SCA's understanding of Customer 17's source of wealth or source of funds commensurate with the high value financial and gambling services that they received at SCA.

SCA's determination of the ML/TF risks posed by Customer 17

788. On and from 7 August 2016, Customer 17 was appropriately rated by SCA as a high risk customer for the purpose of the Act and Rules.

789. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 17 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 17.

Monitoring of Customer 17's transactions

790. At no time did SCA apply appropriate transaction monitoring to Customer 17's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities;

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not carry out adequate due diligence on source of funds in respect of third party deposits received for the benefit of Customer 17 into its bank accounts.

Particulars

See paragraph 227 above.

c. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 17 through SCA Customer account channel, which was a high risk remittance channel.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 17's KYC information

791. SCA did not review, update or verify Customer 17's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 17, including the nature, extent and purpose of Customer 17's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review and update Customer 17's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks;

Particulars

By reason of the matters set out above, there were higher ML/TF risks associated with Customer 17's source of wealth or source of funds: see *Customer 17's risk profile*.

d. to the extent that SCA reviewed Customer 17's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 17.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

ECDD triggers in respect of Customer 17

792. SCA was required to apply the ECDD program to Customer 17 following any ECDD triggers in respect of Customer 17.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

793. Customer 17 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period;

Particulars

Between 23 January 2017 and 17 February 2020, SCA gave the AUSTRAC CEO four SMRs with respect to Customer 17.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 17* above.

794. Each matter pleaded at paragraph 793 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

795. SCA did not conduct appropriate risk-based ECDD with respect to Customer 17 following an ECDD trigger because:

a. on each occasion prior to 9 August 2021 that SCA conducted ECDD in respect of Customer 17 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 17 and failed to appropriately consider whether the ML/TF risks posed by Customer 17 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501, 511 and 516 to 517 above.

On 8 May 2019, SCA conducted ECDD screening in respect of Customer 17. The ECDD screening recorded Customer 17's occupation, source of wealth and source of funds as a 'construction machinery director' but did not contain any known associates of Customer 17 or open source information about Customer 17.

On 1 August 2021, SCA conducted ECDD screening in respect of Customer 17 which was identical to the 8 May 2019 ECDD screening.

In April 2021, SCA conducted ECDD screening in respect of Customer 17. The ECDD screening recorded that Customer 17's occupation, source of wealth and source of funds was 'construction machinery director', but did not contain any reasons for the ECDD, known associates of Customer 17 or open source information about Customer 17.

On 9 August 2021, SCA issued a ban in respect of Customer 17.

The ECDD conducted by SCA did not have appropriate regard to Customer 17's higher ML/TF risks: see *Customer 17's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 17's source of funds or source of wealth.

By reason of the matters set out above, there were higher ML/TF risks associated with Customer 17's source of wealth or source of funds: see *Customer 17's risk profile*.

b. on any occasion prior to 9 August 2021 that senior management considered the higher ML/TF risks posed by Customer 17 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 17 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

Between 9 November 2017 and 13 February 2020, Customer 17 was mentioned in five 'Transaction Monitoring Overview' reports. These reports were provided to SCA's AML/CTF Senior Management Group for consideration at its meeting.

It was not until 9 August 2021 that SCA issued a ban in respect of Customer 17.

Contravention of s 36 of the Act in respect of Customer 17

796. By reason of the matters pleaded at paragraphs 784 to 796 above, from 7 December 2016, SCA:

a. did not monitor Customer 17 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

797. By reason of the matters pleaded at paragraph 796, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 9 August 2021 with respect to Customer 17.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 18

798. Customer 18 was a customer of SCA during the relevant period. Between February 2020 and March 2021, SCA recorded turnover exceeding $290,000,000 for Customer 18.

Particulars

Customer 18 was a customer of SCA from at least 18 February 2020.

As at 28 October 2022, Customer 18 remained a customer of SCA and had not been banned.

799. SCA provided Customer 18 with designated services within the meaning of table 1 and table 3, s 6 of the Act during the relevant period including services connected to Customer 18's gambling as an individual commission player.

Particulars

On 18 February 2020, SCA opened an FMA for Customer 18 which remained open as at 28 October 2022 (item 11, table 3, s 6 of the Act).

While a customer of SCA, Customer 18 remitted funds to and from their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 18's risk profile* below.

800. At all times from 18 February 2020, SCA was required to conduct ongoing customer due diligence in respect of Customer 18.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 18's risk profile

801. On and from 18 February 2020, Customer 18, and the provision of designated services to Customer 18 by SCA, posed higher ML/TF risks because of the following red flags:

a. Customer 18 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs or individual commission programs;

   i. between 2020 and 2021, SCA recorded turnover estimated at $1,363,494 for Customer 18, with cumulative wins of $14,400 on non-commission programs;

Particulars

In the 2021 financial year, Customer 18's individual rated gambling activity for non-commission play was an estimated buy-in of $49,300, turnover of $1,363,494 with wins of $14,400.

b. Customer 18 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA from play on individual commission programs, and a commission of $2,055,864 was recorded as payable by SCA to Customer 18 on individual commission programs;

Particulars

Between 10 October 2020 and 28 March 2021, Customer 18 played on eight individual commission programs at SCA.

In the 2021 financial year, Customer 18's individual rated gambling activity on individual commission programs was an estimated buy-in of $24,819,000, turnover of $289,256,570 with losses of $1,622,695. A commission of $2,055,864 was payable by SCA to Customer 18 from play on individual commission programs.

Between 10 October 2020 and 26 March 2021, Customer 18 was listed in SCA's 'Early Gaming Report' as a significant player on table games on at least 58 occasions.

c. Customer 18 received additional benefits from SCA in their capacity as an individual commission player;

Particulars

For example, during their individual commission program which ran from 10 October 2020 to 14 October 2020, Customer 18 received:

a. a bonus player chip worth $94,000;

b. products and services worth $42,001 free of charge;

c. complimentary value services worth $39,010; and

d. $38,000 in cash as a reimbursement for their jet expenses.

d. Customer 18:

i. had three different account numbers at SCA;

ii. in 2020, had turnover recorded by SCA against at least two different account numbers in circumstances where SCA had no means of automatically collating this data;

Particulars

On 10 October 2020, SCA merged Customer 18's two active account numbers. On the same day, SCA opened another account for Customer 18, with the result that Customer 18 still had two accounts with SCA. Customer 18 used the second account to buy-in on an EGM program. Customer 18 then transferred funds between their different FMAs: see particulars to paragraph 801.e below.

In 2020, SCA recorded turnover for Customer 18 against the two different account numbers.

e. Customer 18 facilitated the provision of high value financial and gambling services (tables 1 and 3, s 6 of the Act) for other customers at SCA, including in connection with junket programs;

Particulars

Junket programs

Customer 18 provided funding for junket programs at SCA, in circumstances where they were not a junket operator or junket representative on the junkets. For example:

a. on 15 November 2020, Customer 18 transferred $500,000 from their SCA FMA to a junket operator's SCA FMA;

b. these funds were used by the junket operator as an additional buy-in on their junket program; and

c. on 17 November 2020, following the settlement of the junket program, Customer 18 received $700,000 into their SCA FMA from the junket operator's SCA FMA.

Individual commission programs

Customer 18 provided funding to, and received funding from, other players to join individual commission programs at SCA. For example:

a. on 10 October 2020, Customer 18 transferred $50,000 from their SCA FMA to Person 15's SCA FMA. On 11 October 2020, Customer 18 and Person 15 each conducted a $50,000 buy-in for an EGM commission program. Later that day, Customer 18 and Person 15 settled their commission programs. Customer 18 then received $54,940 into their SCA FMA from Person 15's SCA FMA;

b. on 10 October 2020, Customer 18 also transferred $100,000 from their SCA FMA to their parent's SCA FMA. On 11 October 2020, Customer 18's parent used these funds to buy-in to an individual commission program. On 12 October 2020, Customer 18's parent settled their program. SCA recorded no gambling activity on the program. Customer 18's parent then transferred the $100,000 back from their SCA FMA to Customer 18's SCA FMA; and

c. on 23 March 2021, Customer 18 received a total of $250,000 from Person 15's SCA FMA into their SCA FMA in two transactions. Customer 18 was playing on an individual commission program at the time, and the customer was listed as part of Customer 18's entourage as their 'PA'.

f. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 18 by remitting large amounts of money into, out of and within the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCEG customer account channel

On 10 October 2020, Customer 18 transferred $1,000,000 to SCA through the SCEG Customer account channel. Customer 18 deposited the funds into an account held by SCEG in Australia, which SCA made available to Customer 18 and deposited into Customer 18's FMA on 15 October 2020.

Remittances through the SCA customer account channel

A report dated October 2021 prepared by Bank 1 identified that, between 1 September 2019 and 31 May 2021, Customer 18 was the top depositor by value into SCA's bank account. Bank 1 identified that during this period, Customer 18 made at least eight deposits totalling $14,813,000.

SCA made money available to Customer 18 in the following transactions:

a. In October 2020, Customer 18 transferred a total of $4,700,000 from their personal bank account in Australia to their SCA FMA in two separate transactions. These funds were used as buy-ins for Customer 18's individual commission programs.

b. In November 2020, Customer 18 transferred $2,000,000 from their personal bank account in Australia to their SCA FMA, for a buy-in on an individual commission program.

c. In December 2020, Customer 18 transferred a total of $2,263,000 from their personal bank account in Australia to their SCA FMA in two separate transactions.

d. In February 2021, Customer 18 transferred a total of $4,000,000 from their personal bank account in Australia to their SCA FMA in two separate transactions, to buy-into individual commission programs.

e. In March 2021, Customer 18 transferred a total of $1,938,000 from their personal bank account in Australia to their SCA FMA in three separate transactions.

SCA accepted instructions to transfer funds from Customer 18's accounts for the following transactions.

a. In October 2020, Customer 18 transferred a total of $6,000,000 from their SCA FMA to their personal bank account in Australia. These funds were winnings from Customer 18's individual commission programs.

b. In November 2020, Customer 18 transferred a total of $4,500,000 from their SCA FMA to their personal bank account in Australia in three separate transactions, following settlements of their individual commission programs.

c. On 9 December 2020, Customer 18 transferred $2,000,000 from their SCA FMA to their personal bank account in Australia.

d. In February 2021, Customer 18 transferred a total of $4,500,000 from their SCA FMA to their personal bank account in Australia.

Remittances within the casino environment

See particulars to paragraph 801.e above.

On 17 October 2020, Customer 18 made a request to transfer $100,000 from their SCA FMA to their mother's SCA FMA. However, later that day Customer 18 decided not to continue with the transfer.

g. Customer 18 was connected to other customers at SCA, including junket operators and junket players;

Particulars

By November 2020, SCA was aware that Customer 18's parent was a junket player on at least two junkets that were operated at SCA.

Customer 18 provided funds to at least one of these junket programs: see particulars to paragraph 801.e above.

h. Customer 18 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 20 October 2020 and 31 March 2021, SCA gave the AUSTRAC CEO 64 TTRs detailing incoming and outgoing payments made by Customer 18 totalling $30,856,401, which comprised:

a. 20 TTRs totalling $384,726 in chip and cash exchanges;

b. 24 TTRs totalling $16,658,575 in account deposits; and

c. 20 TTRs totalling $13,813,100 in account withdrawals.

i. in 2021, Customer 18 and a junket funded by them were the subject of law enforcement enquiries at SCA;

Particulars

In around February 2021, SCA received a request from a law enforcement agency with respect to a junket that Customer 18 partly funded.

On 22 July 2021, SCA received a request from a law enforcement agency with respect to Customer 18.

j. Customer 18 had access to private gaming rooms at SCA;

Particulars

See paragraph 145(e) above.

Customer 18 had access to private gaming rooms at SCA, including the Black Room and the Grange Room.

k. by October 2020, SCA was aware of media articles which reported that Customer 18 was involved in a private loan dispute overseas;

Particulars

On 16 October 2020, SCA became aware that Customer 18 was involved in a private loan dispute overseas and owed millions of dollars: see particulars to paragraph 805.d below. Media articles reported that in 2017, a foreign court ruled that Customer 18 had to repay a debt the equivalent of over $20,000,000 in a foreign currency. In 2018, Customer 18's company's assets were frozen after Customer 18 failed to repay the debt.

In May 2021, SCA became aware of further information relating to the civil dispute: see particulars to paragraph 809.a below. SCA found judgments of a foreign court which revealed that as at 2019, Customer 18 had not repaid the debt.

l. SCA did not have adequate reason to believe that Customer 18's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 18 by SCA.

Particulars

See paragraph 516 above.

At all times, SCA understood that Customer 18 was a real estate developer. In October 2020, SCA also recorded that Customer 18 was the legal representative of a foreign engineering company.

Between February 2020 and March 2021, SCA recorded turnover exceeding $290,000,000 for Customer 18.

By at least October 2020, SCA was aware that Customer 18 had been ordered by a foreign court to repay a debt the equivalent of over $20,000,000 in a foreign currency in 2017, and that Customer 18's company's assets had been frozen after Customer 18 failed to repay that debt.

Despite the above, at no time did SCA request source of wealth or source of funds information from Customer 18.

SCA's determination of the ML/TF risks posed by Customer 18

802. On and from 2 November 2020, Customer 18 was appropriately rated by SCA as a high risk customer for the purpose of the Act and Rules.

803. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 18 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 18.

Monitoring of Customer 18's transactions

804. At no time did SCA apply appropriate transaction monitoring to Customer 18's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 18 through the SCEG Customer account channel and the SCA customer account channel, which were high risk remittance channels.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 18's KYC information

805. SCA did not review, update or verify Customer 18's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 18, including the nature, extent and purpose of Customer 18's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 18's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks;

Particulars

By reason of the matters set out above, there were higher ML/TF risks associated with Customer 18's source of wealth or source of funds: see *Customer 18's risk profile*.

d. to the extent that SCA reviewed Customer 18's KYC information on and from 18 February 2020, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 18.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

On 16 October 2020, SCA conducted due diligence in respect of Customer 18 which identified that:

a. Customer 18's listed occupation was a real estate developer. Customer 18 was also listed as the legal representative of a foreign engineering company;

b. Customer 18 had known associates at SCA, including their parent; and

c. there was open source information available which revealed that Customer 18 was involved in a private loan dispute in a foreign country and owed the equivalent of over $20,000,000 in a foreign currency.

On 30 November 2020, the SCEG International Business Executive Operations Manager emailed an SCA AML Adviser a summary of the media articles relating to the foreign loan case, including the reports that:

a. in 2017, Customer 18 was taken to court in a foreign country and received a judgment that they had to repay a debt the equivalent of over $20,000,000 in a foreign currency within 10 days; and

b. in 2018, due to Customer 18's failure to repay the debt, their company's assets worth the equivalent of over $20,000,000 were frozen by the foreign court.

ECDD triggers in respect of Customer 18

806. SCA was required to apply the ECDD program to Customer 18 following any ECDD triggers in respect of Customer 18.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1) and 15.10 of the Rules

807. Customer 18 was determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 18* above.

808. The matter pleaded at paragraph 807 was an ECDD trigger.

Particulars

See paragraphs 496 and 504 above.

809. SCA did not conduct appropriate risk-based ECDD with respect to Customer 18 following an ECDD trigger because:

a. on each occasion that SCA conducted ECDD in respect of Customer 18 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 18 and failed to appropriately consider whether the ML/TF risks posed by Customer 18 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

On or around 20 May 2021, an SCA AML Compliance Manager conducted an open source search in respect of Customer 18 and identified documents relating to a foreign court judgment in respect of Customer 18.

On 21 May 2021, the SCEG Commercial Manager provided the foreign court judgments and gave the following summary:

a. since 2014, Customer 18 had been involved in the private lending dispute in a foreign country;

b. in December 2017, a foreign court held that Customer 18 and a related corporate defendant shared joint and several liability to the plaintiff for the debt the equivalent of over $20,000,000 in a foreign currency, and had to repay the debt within 10 days following the judgment;

c. the foreign court found that Customer 18 was the ultimate owner of the corporate defendant;

d. in 2018, Customer 18 did not repay the debt; and

e. in 2019, the foreign court ordered that Customer 18 must repay the total debt in three instalments by 31 December 2022.

SCEG staff noted that it was not known whether Customer 18 had partially or fully repaid the debt. SCEG stated that the best way to verify whether the documents related to Customer 18 would be to obtain Customer 18's foreign identification card, which was not currently on file with SCEG.

Based on this information, the AML Compliance Manager confirmed that they had no further queries regarding Customer 18.

On 12 August 2021, SCA conducted ECDD in respect of Customer 18.

The ECDD conducted by SCA did not have appropriate regard to Customer 18's higher ML/TF risks: see *Customer 18's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 18's source of funds or source of wealth.

By reason of the matters set out above, there were higher risks associated with Customer 18's source of wealth and source of funds: see *Customer 18's risk profile*.

b. on any occasion that senior management considered the higher ML/TF risks posed by Customer 18 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 18 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

Between November 2020 and May 2021, Customer 18 was mentioned in two 'Transaction Monitoring Overview' reports for the period August 2020 to May 2021 that were provided to the AML/CTF Senior Management Group for discussion at its meetings. The reports noted the current balance of Customer 18's SCA FMA, and the cheques that SCA issued to Customer 18.

Contravention of s 36 of the Act in respect of Customer 18

810. By reason of the matters pleaded at paragraphs 798 to 809 above, on and from 18 February 2020, SCA:

a. did not monitor Customer 18 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

811. By reason of the matters pleaded at paragraph 810, SCA contravened s 36(1) of the Act on and from 18 February 2020 with respect to Customer 18.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 19

812. Customer 19 was a customer of SCA during the relevant period. Between 17 May 2022 and 29 May 2022, SCA recorded cash turnover exceeding $93,000,000 for Customer 19.

Particulars

Customer 19 was a customer of SCA from at least 14 November 2015.

As at 28 October 2022, Customer 19 remained a customer of SCA and had not been banned.

813. SCA provided Customer 19 with designated services within the meaning of tables 1 and 3, s 6 of the Act tables 1 and 3 during the relevant period including services connected to Customer 19's role as a junket operator and as an individual commission player.

Particulars

On 14 November 2015, SCA opened an FMA for Customer 19 which remained open as at 28 October 2022 (item 11, table 3, s 6 of the Act).

While a customer of SCA, Customer 19 remitted funds to and from their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 19's risk profile* below.

814. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 19.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 19's risk profile

815. On and from 7 December 2016, Customer 19, and the provision of designated services to Customer 19 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 19's risk profile prior to the relevant period

a. by 7 December 2016, Customer 19 had the following risk history:

   i. SCA had formed suspicions for the purposes of s 41 of the Act with respect to Customer 19;

Particulars

SCA gave the AUSTRAC CEO an SMR on three occasions between 18 January 2016 and 22 May 2016.

The SMRs reported that:

a. Customer 19 had made outgoing payments from their SCA FMA to a third party on two occasions totalling $210,000. Customer 19 claimed that the recipient of those funds was

their child: SMRs dated 18 January 2016 and 12 February 2016; and

b. $500,000 in cash was delivered to Customer 19 at SCA by their personal assistant who had just arrived from a foreign country with the money: SMR dated 22 May 2016.

ii. Customer 19 was a junket operator who received and facilitated the provision of high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA;

a. between 15 January 2016 and 29 April 2016, Customer 19 operated four junkets at SCA;

Particulars

Between 15 January 2016 and 20 January 2016, Customer 19 operated a junket at SCA.

Between 4 February 2016 and 15 February 2016, Customer 19 operated a junket at SCA.

Between 15 March 2016 and 19 March 2016, Customer 19 operated a junket at SCA.

Between 27 April 2016 and 29 April 2016, Customer 19 operated a junket at SCA.

b. between 15 January 2016 and 29 April 2016, SCA recorded that the total cumulative turnover of junkets operated by Customer 19 was at least $75,084,600 with buy-ins of at least $16,935,345 and cumulative wins of at least $4,521,220;

Particulars

See paragraphs 399 to 401 above.

The junket that Customer 19 operated in January 2016 had a recorded turnover of at least $10,053,400 with wins of at least $2,068,135.

The junket that Customer 19 operated in February 2016 had a recorded turnover of at least $49,899,900 with losses of at least $47,420.

The junket that Customer 19 operated in March 2016 had a recorded turnover of at least $12,356,300 with wins of at least $1,015,215.

The junket that Customer 19 operated in April 2016 had a recorded turnover of at least $2,775,000 with wins of at least $1,390,450.

c. between 15 January 2016 and 29 April 2016, total benefits of $1,180,926 were payable to Customer 19 by SCA in their capacity as a junket operator;

Particulars

On 20 January 2016, total benefits of $140,747 were payable to Customer 19 in their capacity as a junket operator which included a commission on their junket program's turnover.

In February 2016, total benefits of $798,078 were payable to Customer 19 in their capacity as a junket operator which included a commission on their junket program's turnover.

In March 2016, total benefits of $197,701 were payable to Customer 19 in their capacity as a junket operator which included a commission on their junket program's turnover.

In April 2016, total benefits of $44,400 were payable to Customer 19 in their capacity as a junket operator which included a commission on their junket program's turnover.

d. Customer 19 operated junkets in private gaming rooms at SCA;

Particulars

See paragraph 145(e) above.

Customer 19 operated junkets in private gaming rooms at SCA, including the Opal Room, the Barossa Room, the McLaren Room and the Horizon Room.

e. Customer 19 had three junket representatives at SCA; and

Particulars

The junkets that Customer 19 operated in January 2016, February 2016 and March 2016 had one junket representative.

The junket that Customer 19 operated in April 2016 had two junket representatives.

f. Customer 19 and their junket representatives facilitated the provision of high value designated services to junket players at SCA.

Particulars

See paragraphs 388 and 389 above.

i. designated services provided to Customer 19 lacked transparency as the services were provided through the channel of junket programs at SCA;

Particulars

See paragraph 392 above.

ii. between 15 May 2016 and 25 May 2016, Customer 19 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA through an individual commission program, and a commission of $1,315,149 was recorded as payable by SCA to Customer 19 on the individual commission program;

Particulars

In the 2016 financial year, Customer 19's recorded individual rated gambling activity on the individual commission program at SCA was estimated as a buy-in of $8,103,811, cash turnover of $179,189,024, and with losses of $7,289,020. A commission of $1,315,149 was payable by SCA to Customer 19 through the individual commission program for this period.

iii. Customer 19 received additional benefits from SCA in their capacity as an individual commission player;

Particulars

For example, Customer 19 received benefits of $21,349 in relation to the individual commission program on which they played from 15 May 2016 to 25 May 2016.

iv. Customer 19 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 18 January 2016 and 22 June 2016, SCA gave the AUSTRAC CEO 46 TTRs detailing incoming and outgoing payments made by Customer 19 totalling $19,441,099, which comprised:

a. 21 TTRs totalling $609,830 in chip and cash exchanges;

b. 12 TTRs totalling $9,330,069 in account deposits;

c. 10 TTRs totalling $8,661,301 in account withdrawals; and

d. three TTRs totalling $839,900 in foreign currency exchanges.

v. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 19 by remitting large amounts of money into and out of the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

SCA made money available to Customer 19 in the following transactions:

a. Between 15 March 2016 and 20 May 2016, SCA received 3 telegraphic transfers totalling $6,200,000 from Customer 19 through the SCA customer account channel, each of which it made available to Customer 19's FMA.

SCA accepted instructions to transfer funds from Customer 19's accounts for the following transactions:

a. On 17 January 2016, Customer 19 transferred $100,000 from their SCA FMA to a third party account in Australia: SMR dated 18 January 2016.

b. On 12 February 2016, Customer 19 transferred $110,000 from their SCA FMA to a third party account in Australia: SMR dated 12 February 2016.

c. On 18 June 2016, Customer 19 transferred $15,135 from their SCA FMA to their personal bank account in Australia.

Remittances through the SkyCity New Zealand channel

On 20 May 2016, Customer 19 received $246,710 into their SCA FMA from a SCEG New Zealand casino. SCA made these funds available to Customer 19.

Customer 19's risk profile during the relevant period

b. between 17 May 2022 and 29 May 2022, Customer 19 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA through an individual commission program, and a commission of $640,460 was recorded as payable by SCA to Customer 19 on the individual commission program;

Particulars

In the 2022 financial year, Customer 19's recorded individual rated gambling activity on their individual commission program at SCA was estimated as a buy-in of $4,438,866, cash turnover of $93,080,114 with losses of $3,506,155. A commission of $640,460 was payable by SCA to Customer 19 through the individual commission program.

c. Customer 19 received additional benefits from SCA in their capacity as an individual commission player;

Particulars

For example, Customer 19 received benefits of $57,024 in relation to the individual commission program that they played on from 17 May 2022 to 29 May 2022. These benefits included management compensation of $35,675 for non-gaming complimentary services such as hotel accommodation, airfares and food and beverage expenses.

d. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 19 by remitting large amounts of money into the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

SCA made money available to Customer 19 in the following transactions.

a. In May 2022, Customer 19 transferred a total of $2,890,000 from their personal bank account in Australia to their SCA FMA in five separate transfers.

b. In June 2022 and July 2022, SCA received two telegraphic transfers totalling $210,134, both of which were made available to Customer 19's FMA.

Remittances through the SkyCity New Zealand channel

SCA made money available to Customer 19 in the following transactions.

On 17 May 2022, Customer 19 received $500,000 into their SCA FMA from a SCEG New Zealand casino.

On 25 May 2022, Customer 19 received $400,000 into their SCA FMA from a SCEG New Zealand casino.

e. SCA was aware that Customer 19 had engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

Particulars

On 19 May 2022, Customer 19 and their associates passed large amounts of cash and chips between one another in a series of covert exchanges. Customer 19 and their associates used items such as envelopes, bags and their clothing to conceal the exchanges of cash and chips. SCA recorded that Customer 19 and their associates worked together to conduct cash buy-ins totalling $51,900: SMR dated 4 July 2022.

On 21 May 2022, Customer 19 conducted a cash out of $50,000 at 3:50pm and an equal cash buy-in of $50,000 at 11:36pm. Similarly, on 26 May 2022, Customer 19 conducted a cash out of $9,500 at 5:40pm and an equal cash buy-in of $9,500 at 11:49pm. In a report dated 14 June 2022, SCA's Financial Crime Team recorded that these transactions did not have an apparent economic purpose.

On 23 May 2022, SCA donated money on behalf of Customer 19 to a religious association. SCA's Financial Crime Team observed that the transaction posed risks of concealing bribery, terrorism financing, political influence and kickbacks.

f. Customer 19 transacted using large amounts of cash and cash that appeared suspicious, including large volumes of cash separated into bundles that SCA recorded was inconsistent with SCA's cash bundling procedure;

Particulars

See paragraphs 376 to 381 above.

See paragraph 815.e above.

TTRs

Between 20 May 2022 and 3 June 2022, SCA gave the AUSTRAC CEO 14 TTRs detailing incoming and outgoing payments made by Customer 19 totalling $742,835, which comprised:

a. five TTRs totalling $88,815 in chip and cash exchanges;

b. four TTRs totalling $415,440 in account deposits; and

c. five TTRs totalling $238,580 in account withdrawals.

Large cash and CVI transactions in May 2022

In May 2022, SCA frequently recorded that Customer 19 conducted significant transactions involving cash and CVIs at SCA, including on the following occasions:

a. on 17 May 2022, Customer 19 made a buy-in using a $500,000 CPV;

b. on 18 May 2022, Customer 19 deposited $100,100 in chips into their FMA and subsequently withdrew $60,000 in cash from their FMA in two transactions;

c. on 19 May 2022, Customer 19 deposited $86,600 in cash into their FMA. Later that day, Customer 19 made a buy-in using a total of $560,000 in CPVs;

d. on 20 May 2022, Customer 19 deposited $198,840 in cash into their FMA. Later that day, Customer 19 made a buy-in using a total of $899,800 in CPVs before cashing out $422,050 in chips;

e. on 21 May 2022, Customer 19 made a buy-in using a $300,000 CPV;

f. on 23 May 2022, Customer 19 made a buy-in using a $500,000 CPV, and later deposited $595,000 in chips into their FMA;

g. on 25 May 2022, Customer 19 made a using a total of $1,200,000 in CPVs, and later deposited $450,000 in chips into their FMA; and

h. on 26 May 2022, Customer 19 made a buy-in using a total of $1,050,000 in CPVs, and later deposited $440,000 in chips into their FMA. The same day, Customer 19 conducted a cash buy-in of $79,900. The cash was separated into bundles of $2,500 with ‘count team’ written on the straps. SCA staff reported that the packaging was inconsistent with SCA’s cash bundling procedure: SMR dated 4 July 2022.

g. Customer 19 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including utilising third parties to conduct transactions and transferring money from their FMA to a third party;

Particulars

See paragraph 24 above.

Customer 19 was involved in transactions indicative of the ML/TF typology of utilising third parties to conduct transactions: see paragraph 815.e above.

In a report dated 14 June 2022, the SCA Financial Crime Team identified the following ML/TF vulnerabilities faced by SCA based on Customer 19’s activity on an individual commission program in May 2022:

a. SCA customers sharing cash as a private group, which could be perceived as 'quasi junket' type activity: see paragraph 815.e above;

b. individual commission program players conducting recurrent large cash outs, which increased the difficulty in tracking cash: see paragraph 815.f above.

c. SCA accepting incomplete customer Source of Funds Declarations, which posed risks that SCA could receive cash funds from unknown sources and contravene standard procedures: see paragraph 815.i below;

d. SCA relying on online banking screenshots for processing incoming customer telegraphic transfers which could pose the risk of accepting payments from third parties: see paragraph 815.i below; and

e. charitable donations made by SCA on behalf of a customer which had the potential to pose a bribery, terrorism financing or political risk: see paragraph 815.e above.

h. Customer 19 had access to private gaming rooms at SCA; and

Particulars

See paragraph 145(e) above.

Customer 19 had access to private gaming rooms at SCA, including the Horizon Room and the Salon 88 Gaming Room.

i. SCA did not have adequate reason to believe that Customer 19's source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 19 by SCA.

Particulars

See paragraph 516 above.

In January 2016, SCA recorded Customer 19's occupation as assistant to the chairperson of an overseas company, Company 8.

In November 2021, Customer 19 updated their occupation status to unemployed. Customer 19 declared that the source of their wealth was income from their shareholdings in Company 8, investment in stock trading and real estate ownership.

In May 2022, Customer 19's use of gambling and financial services at SCA escalated significantly. For example, between 17 May 2022 and 29 May 2022, SCA recorded that Customer 19 had an estimated buy-in of $4,438,866 on their individual commission program at SCA. During this time, Customer 19 transacted using large amounts of cash at SCA. Between 20 May 2022 and 3 June 2022, SCA gave the AUSTRAC CEO 14 TTRs detailing incoming and outgoing payments made by Customer 19 totalling $742,835.

SCA determined that it was unable to satisfactorily confirm the source of cash transacted by Customer 19 at SCA: SMR dated 4 July 2022.

Inconsistent and incomplete information regarding Customer 19's occupation and source of funds

An external report prepared on 18 May 2022 found that the income derived by Customer 19 from their stated occupation as the director of a company and their real estate assets could not be verified. The report found that Customer 19 had an estimated verified net worth of $12,630,912 based on their interest in shares held in Company 8.

On 19 May 2022, 20 May 2022, 21 May 2022 and 26 May 2022, Customer 19 completed four Source of Funds Declaration Forms at SCA containing inconsistent and incomplete information. For example, on 19 May 2022, Customer 19 declared their occupation as the Chief Executive Officer of Company 8 and their main source of income as business earnings. On the following, day Customer 19 declared their occupation as the owner of a different company and their main source of income as rent, real estate and dividends.

In addition, the Source of Funds Declarations provided by Customer 19 on 20 May 2022, 21 May 2022 and 26 May 2022 did not provide any information regarding the bank, company or trust, individual, proceeds from sale or casino winnings from which Customer 19's funds were sourced. In Customer 19's Source of Funds Declaration Form dated 19 May 2022, they declared their casino winnings as their source of cash. However, SCA staff observed that the amount of cash declared in the form was not commensurate with Customer 19's purported casino winnings: SMR dated 4 July 2022.

At no time was SCA's understanding of Customer 19's source of funds commensurate with the high value financial and gambling services that they received at SCA.

Source of funds risks arising from unverified remittances

In May 2022, Customer 19 transferred a total of $2,890,000 from their personal bank account to SCA in five separate transfers. Customer 19 provided online banking screenshots, which SCA relied on to process telegraphic transfers from Customer 19's personal bank account. SCA later observed that this practice posed the risk of accepting payments from third parties.

SCA's determination of the ML/TF risks posed by Customer 19

816. On and from 23 May 2016, Customer 19 was appropriately rated by SCA as a high risk customer for the purpose of the Act and Rules.

817. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 19 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by it with respect to Customer 19.

Monitoring of Customer 19's transactions

818. At no time did SCA apply appropriate transaction monitoring to Customer 19's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities;

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not make or keep appropriate records of designated services provided to junket operators; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

c. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 19 through:

i. the junket channel; and

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

ii. the SCA Customer account channel and the SkyCity New Zealand channel, which were high risk remittance channels.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 19's KYC information

819. SCA did not review, update or verify Customer 19's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 19, including the nature, extent and purpose of Customer 19's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 19's source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 19's risk profile* above, there were higher ML/TF risks associated with Customer 19's source of wealth or source of funds.

d. to the extent that SCA reviewed Customer 19's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 19.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

ECDD triggers in respect of Customer 19

820. SCA was required to apply the ECDD program to Customer 19 following any ECDD triggers in respect of Customer 19.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1) and 15.10 of the Rules.

821. Customer 19 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

On 4 July 2022, SCA gave the AUSTRAC CEO an SMR with respect to Customer 19.

b. determined by SCA to be high risk for the purpose of the Act and Rules prior to the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 19* above.

822. Each matter pleaded in paragraph 821 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

823. SCA did not conduct appropriate risk-based ECDD with respect to Customer 19 following an ECDD trigger because:

a. on each occasion that SCA conducted ECDD in respect of Customer 19 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 19 and failed to appropriately consider whether the ML/TF risks posed by Customer 19 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501, 511 and 516 to 517 above.

On 20 June 2019, SCA conducted ECDD in respect of Customer 19 but did not have appropriate regard to Customer 19's higher ML/TF risks: see *Customer 19's risk profile* above.

The ECDD screening in respect of Customer 19 identified:

a. the SMRs dated 18 January 2016, 12 February 2016 and 21 May 2016 as the reasons for elevating Customer 19 to high risk;

b. Customer 19's occupation as an assistant to the executive chairman of Company 8. The ECDD report noted that the executive chairman of Company 8 was Customer 19's spouse; and

c. Customer 19's junket representative as their known associate.

SCEG International Business ECDD

On 6 December 2021, the SCEG International Business team conducted ECDD and assessed certain source of funds and source of wealth information for Customer 19. The report verified Customer 19's income from shareholdings in Company 8, investment in another company and payments of rent from a tenancy agreement. The report also verified Customer 19's bank account balance and equity in three companies including Company 8. Based on those sources, the SCEG International Business team concluded that Customer 19's income was approximately NZD$2,800,000 and the value of their assets was approximately NZD$35,600,000. The ECDD report did not verify any employment information for Customer 19. The ECDD report classified Customer 19's player tier as 'AML thresholds'. It is not known from SCA's records whether this ECDD report was provided to SCA: see paragraph 528 above.

External ECDD report

SCA received an external report prepared on 18 May 2022 assessing Customer 19's source of wealth and source of funds information: see paragraph 815.i above.

Post-Visit Review

The SCA Financial Crime Team recorded a number of ML/TF risks posed by Customer 19 during their individual commission program in May 2022: see paragraph 815.g above.

At the end of the report, the SCA Financial Crime Team recommended that Customer 19's post-visit review be provided to relevant stakeholders for comment and that the SCA business units, such as International Business and the Cage, collaborate with the SCA Financial Crime Team to identify and implement risk mitigation controls for the ML/TF vulnerabilities identified.

At no time was SCA's understanding of Customer 19's source of funds commensurate with the extremely high value financial and gambling services that they received at SCA.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 19's source of funds: see *Customer 19's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 19's source of funds or source of wealth.

By reason of the matters set out in *Customer 19's risk profile* above, there were higher ML/TF risks associated with Customer 19's source of wealth or source of funds.

b. on any occasion that senior management considered the higher ML/TF risks posed by Customer 19 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 19 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

Knowledge of significant additional buy-ins

Between 17 May 2022 and 29 May 2022, SCA recorded that Customer 19 had an estimated buy-in of $4,438,866 on their individual commission program at SCA.

Throughout the course of Customer 19's individual commission program in May 2022, senior management including the President of International Business Group and the General Manager of International Gaming were provided with frequent updates detailing Customer 19's significant additional buy-ins at SCA.

Knowledge of inconsistent and incomplete source of funds declarations

On 22 May 2022, Customer 19's Source of Funds Declaration Form dated 21 May 2022 was circulated to senior management including the President of International Business Group and General Manager

of International Gaming. The declaration form was incomplete as it did not provide any information regarding the bank, company or trust, individual, proceeds from sale or casino winnings from which Customer 19's funds were sourced. The declaration form also contained information that was inconsistent with SCA's records of Customer 19's occupation and source of funds.

As at 1 September 2022, SCA's due diligence records in respect of Customer 19 did not include any evidence that senior management took any further action to respond to the ML/TF risks posed by Customer 19's significant additional buy-ins in May 2022 or their inconsistent and incomplete Source of Funds Declaration Form.

Contravention of s 36 of the Act in respect of Customer 19

824. By reason of the matters pleaded from paragraphs 812 to 823 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 19 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

825. By reason of the matters pleaded at paragraph 824, SCA contravened s 36(1) of the Act on and from 7 December 2016 with respect to Customer 19.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 20

826. Customer 20 was a customer of SCA during the relevant period. Between 7 December 2016 and November 2017, SCA recorded turnover exceeding $19,000,000 for Customer 20.

Particulars

Customer 20 was a customer of SCA from at least 27 June 2015.

As at 28 October 2022, Customer 20 remained a customer of SCA and had not been banned.

827. SCA provided Customer 20 with designated services within the meaning of tables 1 and 3, s 6 of the Act tables 1 and 3, s 6 of the Act during the relevant period including services connected with Customer 20's role as a junket player and as an individual commission player.

Particulars

On 27 June 2015, SCA opened an FMA for Customer 20 which remained open as at 28 October 2022 (item 11, table 3, s 6 of the Act).

While a customer of SCA, Customer 20 remitted funds to and from their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 20's risk profile* below.

828. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 20.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 20's risk profile

829. On and from 7 December 2016, Customer 20, and the provision of designated services to Customer 20 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 20's risk profile prior to the relevant period

a. by 7 December 2016 Customer 20 had the following risk history:

i. Customer 20 was associated with persons involved in criminal activity;

Particulars

By August 2015, SCA was aware that Customer 20's immediate family member had been found guilty of carrying guns and ammunition, and deliberately destroying property.

ii. Customer 20's bank accounts had been frozen by a foreign government;

Particulars

By June 2016, SCEG was aware that Customer 20's accounts had been frozen by a foreign government in relation to Customer 20's alleged relationship with a junket operator. It is not known whether SCEG provided this information to SCA: see paragraph 528 above.

iii. Customer 20 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA;

Particulars

In 2015, Customer 20's recorded individual rated gambling activity at SCA was estimated as a buy-in of $17,972,100.

In the 2016 financial year, Customer 20's recorded individual rated gambling activity on individual commission programs at SCA was estimated as a buy-in of $5,111,006, cash turnover of $215,243,700, and with losses of $5,383,870. A commission of $1,291,462 was payable by SCA to Customer 20 from play on individual commission programs.

Between October 2015 and November 2015, SCA provided four lines of credit for Customer 20 totalling $2,000,000.

See paragraphs 321 to 323, and 342 above.

iv. SCA provided designated services (items 31 and 32, table 1, s6 of the Act) to Customer 20 by remitting large amounts of money into the casino environment via their accounts, including through high risk remittance channels; and

Particulars

Remittances through the SCEG Customer account channel

On 13 November 2015, a third party company transferred $321,983 for Customer 20 through the SCEG Customer account channel. SCA made these funds available to Customer 20's FMA.

v. Customer 20 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 1 July 2015 and 22 December 2015, SCA gave the AUSTRAC CEO 43 TTRs detailing incoming and outcoming payments made by Customer 20 totalling $4,957,261, which comprised:

a. six TTRs totalling $145,200 in chip and cash exchanges;

b. 33 TTRs totalling $4,544,420 in account deposits;

c. two TTRs totalling $67,641 in account withdrawals; and

d. two TTRs totalling $200,000 in marker redemptions.

Customer 20's risk profile during the relevant period

b. Customer 20 was a junket player who received gambling services (table 3, s 6 of the Act) at SCA through junket programs;

i. between 25 July 2019 and 27 July 2019, Customer 20 was a player on two junket programs at SCA operated by a junket operator; and

ii. at no time did SCA record Customer 20's individual gambling activity on junket programs they attended as a junket player;

c. designated services provided to Customer 20 lacked transparency as the services were provided through the channel of junket programs at SCA;

Particulars

See paragraph 392 above.

d. Customer 20 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA from play on individual commission programs, with a commission of $115,875 recorded as payable to Customer 20;

Particulars

In the 2017 financial year, Customer 20's recorded individual rated gambling activity on individual commission programs at SCA was estimated as a buy-in of $500,668, cash turnover of $15,369,200 with losses of $503,505. A commission of $92,215 was payable by SCA to Customer 20 from play on individual commission programs.

In the 2018 financial year, Customer 20's recorded individual rated gambling activity on individual commission programs at SCA was estimated as a buy-in of $685,830, cash turnover of $3,967,600 with losses of $685,000. A commission of $23,660 was payable by SCA to Customer 20 from play on individual commission programs.

e. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 20 by remitting large amounts of money into, out of and within the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

SCA made money available to Customer 20 in the following transactions:

a. On or around 5 July 2017, Customer 20 received $233,962 into their SCA FMA from a third party company account overseas to settle Customer 20's outstanding debt.

b. On or around 4 November 2017, Customer 20 received $457,236 into their SCA FMA from a third party company account overseas.

c. On or around 1 December 2017, Customer 20 received $186,332 into their SCA FMA from the same third party company account overseas.

Remittances through the SkyCity New Zealand channel

SCA made money available to Customer 20 in the following transactions:

a. Between 28 December 2018 and 25 January 2019, SCA credited at least $4,707,820 to Customer 20's FMA with these funds originating from Customer 20's FMA held at a SCEG New Zealand casino: see paragraph 829.f below.

Remittances within the casino environment

SCA remitted funds for Customer 20 through their associate, Person 16's FMA: see paragraph 829.f below.

f. SCA was aware that Customer 20 had engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

Particulars

On 28 December 2018, at Customer 20's request, SCA facilitated the inter-company transfer of approximately NZD$1,000,000 from a SCEG New Zealand casino to SCA. The funds were part of Customer 20's winnings made as the main player on Customer 8's junket program at the SCEG New Zealand casino. The funds were then transferred to Person 16's SCA FMA. The same day, Person 16 travelled from Melbourne to SCA, purchased a suitcase nearby, withdrew the funds from their FMA in cash and flew back to Melbourne carrying the $1,000,000 in cash: SMR dated 11 January 2019.

Between around 9 January 2019 and 25 January 2019, SCA facilitated inter-company transfers totalling over $4,700,000 from Customer 20's FMA at a SCEG New Zealand casino to Person 16's SCA FMA, via Customer 20's SCA FMA, despite neither Customer 20 nor Person 16 gaming at SCA during this period:

a. On 9 January 2019 or 10 January 2019, SCA facilitated an inter-company transfer of AUD$908,832 from Customer 20's FMA at a SCEG New Zealand casino to Customer 20's SCA FMA. Once the funds had been credited to Customer 20's FMA, SCA transferred the full amount to Person 16's SCA FMA. On 10 January 2019, Person 16 flew into Adelaide and withdrew the entire $908,832 in cash. The same day, Person 16 deposited a total of $585,482 back into Customer 20's FMA in three separate transactions. At Customer 20's request, these funds were returned to a SCEG New Zealand casino to another junket, for Customer 20 to use for gaming there. At the time of the transaction, Person 16 had never gamed at SCA, and Customer 20 had not gamed at SCA since November 2017: SMR dated 11 January 2019.

b. On 11 January 2019, SCA facilitated four inter-company transfers totalling $889,898 from Customer 20's FMA at a SCEG New Zealand casino to their FMA at SCA. Customer 20 then instructed SCA to transfer the funds to Person 16's SCA FMA. Person 16 withdrew the funds in one lump sum as cash without any play, put the cash into a suitcase, left SCA and boarded a flight to Sydney. Person 16 did not engage in any gaming at SCA: SMR dated 14 January 2019.

c. On 25 January 2019, SCA facilitated an inter-company transfer of $2,766,020 from Customer 20's FMA at a SCEG New Zealand casino to their SCA FMA. The same day, SCA facilitated an inter-company transfer of an additional $143,070 from Customer 20's FMA at a SCEG New Zealand casino to their SCA FMA. On Customer 20's instructions, SCA then transferred both amounts as one lump sum totalling $2,909,090 to Person 16's SCA FMA. SCA then permitted Person 16 to withdraw $909,909 of the funds in cash. SCA

also transferred $300,000 and $1,700,000 from Person 16's SCA FMA to another Australian casino. The bank transfers were for the benefit of a third party. Neither Customer 20 nor Person 16 engaged in any gaming at SCA on this occasion. SCA was unaware of the relationship between Customer 20, Person 16, and the third party: SMR dated 31 January 2019.

g. Customer 20 was connected to other customers at SCA, including junket operators who posed higher ML/TF risks such as Customer 8;

Particulars

SCA recorded that Customer 20 was known to be an associate of Customer 8.

h. Customer 20, and persons associated with them, transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 9 February 2017 and 30 January 2019, SCA gave the AUSTRAC CEO 16 TTRs detailing incoming and outcoming payments made by Customer 20 totalling $10,955,035, which comprised:

a. 11 TTRs totalling $6,003,528 in account deposits;

b. four TTRs totalling $4,859,292 in account withdrawals; and

c. one TTR totalling $92,215 in a premium player commission/rebate.

Large cash transactions

On 25 January 2019, Customer 20 engaged in cash transactions at SCA totalling $5,818,180.

i. Customer 20 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including the use of third parties to conduct transactions;

Particulars

See paragraph 24 above.

See paragraph 829.f above.

j. Customer 20 had access to private gaming rooms at SCA;

Particulars

See paragraph 145(e) above.

Customer 28 had access to private gaming rooms at SCA, including Suite 88, the Grange Room and the Horizon Room.

k. by January 2019, SCA was aware of a media article which reported that Customer 20 was involved in legal proceedings relating to an alleged debt owed to an overseas casino; and

Particulars

On 24 June 2018, an online article alleged that Customer 20 owed a debt of over $8,000,000 to an overseas casino.

Despite SCEG being aware of this article by 2 July 2018, it was not until 11 January 2019 that SCA became aware of this information: see paragraph 528 above.

l. SCA did not have adequate reason to believe that Customer 20's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 20 by SCA.

Particulars

See paragraph 516 above.

From 27 June 2015, SCA understood Customer 20's occupation to be as a property developer.

In August 2021, Customer 20 provided SCA with a letter stating that they had been employed by an overseas company, and had an annual salary in a foreign currency equal to approximately AUD$762,000 from 1993**.**

At no time during the relevant period was SCA's understanding of Customer 20's source of wealth or source of funds commensurate with the high value financial and gambling services Customer 20 received at SCA.

Between 7 December 2016 and November 2017, SCA recorded turnover exceeding $19,000,000 for Customer 20.

SCA's determination of the ML/TF risks posed by Customer 20

830. SCA was unable to appropriately identify or assess the ML/TF risks posed by Customer 20 because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 20.

a. On and from 7 December 2016, Customer 20 should have been recognised by SCA as a high risk customer for the purpose of the Act and Rules for the reasons pleaded above: see *Customer 20's risk profile* above*.*

Particulars

Sections 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

b. It was not until 11 January 2019 that Customer 20 was rated high risk by SCA for the purpose of the Act and Rules.

Monitoring of Customer 20's transactions

831. At no time did SCA apply appropriate transaction monitoring to Customer 20's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities;

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not make or keep appropriate records of designated services provided to junket players;

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

c. SCA did not carry out adequate due diligence on source of funds in respect of third party deposits received for the benefit of Customer 20 into its bank accounts; and

Particulars

See paragraph 227 above.

d. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 20 through:

i. the junket channel; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 490 to 494 above.

ii. the SCA Customer account channel, which was a high risk remittance channel.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 20's KYC information

832. SCA did not review, update or verify Customer 20's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 20, including the nature, extent and purpose of Customer 20's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 20's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 20's risk profile* above, there were higher ML/TF risks associated with Customer 20's source of wealth or source of funds.

d. to the extent that SCA reviewed Customer 20's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 20.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

In October 2017, SCA performed open source searches on Customer 20 and Customer 20's family members.

Failure to apply appropriate due diligence suited to the high ML/TF risks

833. Had SCA conducted ongoing customer due diligence on and from 7 December 2016 by:

a. appropriately identifying and assessing the ML/TF risks posed by Customer 20;

b. applying appropriate risk-based transaction monitoring to Customer 20; and

c. appropriately reviewing and updating Customer 20's KYC information, having regard to the high ML/TF risks,

SCA would have been required by the Act and Rules to apply the ECDD Program to Customer 20 at a time before the date of the ECDD triggers pleaded below: see *ECDD triggers in respect of Customer 20*.

ECDD triggers in respect of Customer 20

834. SCA was required to apply the ECDD program to Customer 20 following any ECDD triggers in respect of Customer 20.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

835. Customer 20 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 11 January 2019 and 31 January 2019, SCA gave the AUSTRAC CEO three SMRs with respect to Customer 20.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 20* above.

836. Each matter pleaded in paragraph 835 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

837. SCA did not conduct appropriate risk-based ECDD with respect to Customer 20 following an ECDD trigger because:

a. on each occasion that SCA conducted ECDD in respect of Customer 20 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 20 and failed to appropriately consider whether the ML/TF risks posed by Customer 20 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501, 511 and 516 to 517 above.

In September 2019, SCA conducted ECDD in respect of Customer 20. The ECDD screening identified adverse open source media about Customer 20 including three articles reporting that Customer 20 was involved in a lawsuit with an overseas casino regarding an alleged outstanding debt incurred when Customer 20 gambled at that casino. One of the articles dated 26 June 2018 reported that Customer 20 gave the overseas casino a false address on their casino credit application. The article noted that the overseas casino had sought to issue a subpoena to Customer 20 in Australia.

In or around December 2019, SCEG conducted a review of Customer 20's KYC information because Customer 20 was one of SCEG's top six individual international customers (based on their turnover in the 2019 financial year). This review found gaps in the source of wealth information SCEG had for Customer 20, including that there were limited details of Customer 20's involvement in the real estate sector in a foreign country, and limited details regarding Customer 20's business interests in real estate (for example, SCEG did not have any company names for real estate businesses operated by Customer 20). It is not known whether SCEG provided this review to SCA: see paragraph 528 above.

In 2020, the International Business team considered Customer 20's source of wealth as part of a credit application by Customer 20. The

information was obtained through open source searches, property searches and information provided by the Sales team. It is not known whether SCEG provided this information to SCA: see paragraph 528 above.

In January 2020, SCA conducted searches on Customer 20 including a title search on a property belonging to Customer 20, and Dow Jones Risk & Compliance searches on Customer 20 and companies to which Customer 20 was connected.

On 30 August 2021, Customer 20 completed a Source of Wealth Declaration Form. Around the same time, SCA obtained a letter dated 27 August 2021 stating that since 1993, Customer 20 had been employed by a foreign company, with an annual salary in a foreign currency equal to approximately AUD$762,000.

On 3 December 2021, Customer 20 completed a patron credentials disclosure form, stating that they were the chairman of a foreign real estate company.

On 14 December 2021, an International Business Enhanced Due Diligence Application was completed by SCEG for SCEG New Zealand casinos and SCA with respect to Customer 20. The ECDD noted no red flags with respect to Customer 20, and that Customer 20's occupation, asset ownership and business were all verified with no adverse findings. It is not clear if this information was provided to SCA: see paragraph 528 above.

On 16 December 2021, SCA conducted a Jade watchlist screening on a company that Customer 20 was employed by. This search produced no results.

In February 2022, SCA conducted ECDD in respect of Customer 20 and obtained an intelligence report in respect of Customer 20.

The ECDD conducted by SCA did not have appropriate regard to Customer 20's higher ML/TF risks: see *Customer 20's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 20's source of funds or source of wealth.

By reason of the matters set out in *Customer 20's risk profile* above, there were higher risks associated with Customer 20's source of wealth and source of funds.

b. at no time did senior management consider the higher ML/TF risks posed by Customer 20 in response to an ECDD trigger, or appropriately consider whether the ML/TF risks posed by Customer 20 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

Contravention of s 36 of the Act in respect of Customer 20

838. By reason of the matters pleaded from paragraphs 826 to 837 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 20 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

839. By reason of the matters pleaded at paragraph 838, SCA contravened s 36(1) of the Act on and from 7 December 2016 with respect to Customer 20.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 21

840. Customer 21 was a customer of SCA during the relevant period. Between 2016 and 2020, SCA recorded turnover exceeding $18,000,000 for Customer 21.

Particulars

Customer 21 was a customer of SCA from at least 3 July 2015.

On 22 March 2022, SCA issued a ban in respect of Customer 21.

841. SCA provided Customer 21 with designated services within the meaning of table 3, s 6 of the Act during the relevant period including services as an individual commission player.

Particulars

On 26 February 2021, SCA opened an FMA for Customer 21 which was closed on 22 March 2022 (item 11, table 3, s 6 of the Act).

See *Customer 21's risk profile* below.

842. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 21.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 21's risk profile

843. On and from 7 December 2016, Customer 21, and the provision of designated services to Customer 21 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 21's risk profile prior to the relevant period

a. by 7 December 2016, Customer 21 had the following risk history:

   i. SCA recorded high turnover of $11,723,184 for Customer 21, with cumulative losses of $79,655;

Particulars

In the 2016 financial year, Customer 21's non-commission play at SCA was estimated as a buy-in of $708,000, turnover of $11,723,184 with losses of $79,655.

   ii. Customer 21 transacted using large amounts of cash and cash that appeared suspicious at SCA; and

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 19 May 2013 and 14 November 2016, SCA gave the AUSTRAC CEO 89 TTRs detailing incoming and outcoming payments made by Customer 21 totalling $1,480,993, which comprised:

a. 57 TTRs totalling $1,003,600 in account deposits; and

b. 32 TTRs totalling $477,393 in chip and cash exchanges.

Large cash transactions

Between 11 September 2015 and 7 November 2016, Customer 21 deposited $178,276 in cash into their SCA FMA in 26 transactions below the transaction reporting threshold.

Between 11 September 2015 and 7 November 2016, Customer 21 withdrew $185,000 in CPVs from their SCA FMA in 25 transactions below the transaction reporting threshold.

   iii. Customer 21 and their associates engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including structuring;

Particulars

See paragraph 24 above.

Between 11 November 2015 and 7 November 2016, Customer 21 was involved in 20 transactions indicative of the ML/TF typology of structuring. The total value of these transactions was $148,000: see particulars to paragraph 843.a.ii above.

Customer 21's risk profile during the relevant period

b. Customer 21 received high value gambling services (table 3, s 6 of the Act) at SCA other than through junket or individual commission programs. Between 2016 and 2020, SCA recorded a high turnover for non-commission play of $14,545,486 for Customer 21, with cumulative losses of $524,080;

Particulars

In the 2017 financial year, Customer 21's non-commission play at SCA was estimated as a buy-in of $608,250, turnover of $8,798,604 with losses of $372,080.

In the 2018 financial year, Customer 21's non-commission play at SCA was estimated as a buy-in of $9,000, turnover of $529,256 with losses of $33,600.

In the 2019 financial year, Customer 21's non-commission play at SCA was estimated as a buy-in of $30,900, turnover of $777,300 with losses of $31,500.

In the 2020 financial year, despite closures related to the COVID-19 pandemic, Customer 21's non-commission play at SCA remained high, with an estimated buy-in of $42,800, turnover of $4,440,326 with losses of $86,900. The COVID-19 border closures meant Customer 21 was unable to attend SCA between 14 March 2020 and 28 December 2020.

c. Customer 21 received high value gambling services (tables 3, s 6 of the Act) at SCA from play on individual commission programs. Customer 21 recorded a high turnover of $3,601,796 with losses of $164,050 on individual commission programs at SCA, with a commission of $19,826 recorded as payable by SCA to Customer 21;

Particulars

Between April 2019 and May 2019, Customer 21 played on two individual commission programs at SCA.

During this period, Customer 21's play on individual commission programs was estimated as a buy-in of $233,000, turnover of $3,601,796 with losses of $164,050.

SCA estimated the commission payable to Customer 21 from play on individual commission programs this period at $19,826.

d. SCA was aware that Customer 21 and their associates had engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

Particulars

From at least 21 April 2017, SCA was aware that Customer 21 was associated with a number of customers, including Customer 2, that conducted transactions involving the receipt and movement of significant amounts of cash with no apparent economic or visible purpose and were related to loan sharking activities.

On 22 December 2016, Customer 21 exchanged approximately $100,000 in CPVs for chips at SCA and received 20 stacks of chips each with a value of $5,000. Over the next hour, SCA staff observed that Customer 21 progressively transferred all of these chips to Customer 27 over a number of transactions:

a. Customer 21 immediately placed $50,000 of the chips into their own jacket pocket.

b. Customer 21 sat down at a gaming table alongside Customer 27 with the remaining $50,000 in chips and slid these $50,000 in chips across to Customer 27. Customer 21 then produced the $50,000 in chips from their jacket pocket and commenced play, placing only a few small bets.

c. Customer 21 left the table to exchange $5,000 of the chips for a different denomination.

d. While Customer 21 was away from the table, Customer 27 reached across the table and took the $45,000 in chips that Customer 21 had left on the table into their possession.

e. Customer 27 left the table with the $95,000 in chips that they had received from Customer 21 and commenced play at another table.

f. Shortly after this transaction, Customer 21 approached Customer 27 and gave them the remaining $5,000 in chips. Customer 27 placed the $5,000 in chips into their pocket.

g. At the conclusion of these transactions, Customer 27 was in possession of all of the $100,000 in chips that Customer 21 had originally received.

SCA considered that these transactions were unusual. It noted that the recorded play for Customer 21 for the day was minimal and not at all consistent with the expected level of play for their buy-in. SCA also noted that the recorded play for Customer 27 for the day was significant and that they recorded losses of $50,000 for the day. SCA noted that it had previously reported Customer 27 for structuring and money lending. It noted that Customer 27 appeared to be actively trying to avoid reporting obligations by having other players conduct transactions on their behalf. SCA noted that Customer 27 had previously been subtly taking photos of other players including Customer 21: SMR dated 23 December 2016.

On 19 April 2017, Customer 21 was engaged in a number of suspicious cash and chip exchanges at SCA alongside Customer 2, Customer 27 and Person 18. SCA concluded that Customer 21 had assisted the customers to engage in prohibited money lending:

a. Customer 27 gave $9,000 in chips to Customer 2. Customer 27 and Customer 2 then attended an SCA gaming table and Customer 2 commenced play while Customer 27 stood behind the table. Customer 21 was also standing behind the table.

b. Customer 27 then handed another $5,000 in chips to Customer 21.

c. Customer 21 then left the table area, exchanged the chips for chips of another denomination at the Cashier, and returned the $5,000 in chips to Customer 27.

d. Customer 2 then continued to play at the gaming table and lost the original $9,000 in chips that they received from Customer 27.

e. Customer 27 then passed $27,000 in chips to Customer 2. Customer 2 then passed these chips to Customer 21.

f. Customer 21 then left the room and deposited the chips into Customer 2's account with the assistance of a VIP host at the Grange Room desk. SCA issued a $27,000 CPV for Customer 2 which Customer 21 and the VIP Host then took into their possession.

g. The VIP Host then presented the CPV to Customer 2. Customer 2 then presented the CPV for redemption at a gaming table.

h. During this time, Customer 21 was at a gaming table.

i. Shortly after, Customer 27 joined Customer 21 at the gaming table. Customer 27 then removed an item from the pocket of their pants and placed it in Customer 21's jacket pocket.

j. Customer 27 then left the Grange Room. Moments later, Customer 27 returned and joined Customer 21 at the gaming table. Customer 21 then removed the items from their jacket pocket and handed them to Customer 27.

k. During this time, Customer 2 recorded a significant win of $97,000 at a gaming table and exchanged their winning chips for different denominations at an SCA Cashier.

l. Customer 2 then joined Customer 21 and Customer 27 at the gaming table.

m. After a short period, Customer 2 and Customer 27 left the gaming table and attended the Cashier. At the Cashier, Customer 2 presented $105,800 in chips and exchanged $75,800 of the chips for cash. Customer 2 placed $50,000 of the cash into an envelope and the remaining $25,800 of the cash into their personal bag.

n. Customer 2 then handed the envelope containing $50,000 in cash to Customer 21.

o. Customer 21 then exchanged the $50,000 in cash within the envelope for a CPV and moved through multiple areas of SCA. SCA considered that Customer 21 appeared to be searching for someone.

p. Eventually, Customer 21 found Person 18, spoke with them briefly, and then attended an SCA Cashier and exchanged the $50,000 CPV for chips.

q. Customer 21 then attended the VIP Balcony and handed the $50,000 in chips to Person 18.

SCA considered that this activity was unusual. It considered that Customer 2 had borrowed money from Customer 27 and repaid this debt, using Customer 21 to disguise this transaction. SCA also considered that Customer 27 had loaned or repaid money to Person 18, using Customer 21 to disguise this transaction: SMR dated 21 April 2017.

On 28 August 2019, Customer 21 attended the Cashier in the Premium Gaming Area at SCA alongside an associate, Person 17. Person 17 then exchanged $30,000 of cash for chips. While this transaction was being processed, Customer 27 approached the Cashier and placed an unknown amount of cash into Person 17's bag. After the cash buy-in transaction was processed, Person 17 received $30,000 in chips and gave $10,000 of the chips to Customer 21. Over the next hour, Person 17 did not use the remaining $20,000 of the chips in play, and Customer 21 gave Person 17 at least an additional $12,350 in chips. Person 17 then exchanged the total of $32,350 in chips that were now in their possession for cash at an SCA Cashier. Person 17, Customer 21 and Customer 27 then departed SCA together.

SCA considered that this activity was suspicious. It noted that Person 17 was a student with minimal recorded play and that Customer 21 and Customer 27 had previously used Person 17 to conduct deceptive transactions. SCA suspected that this transaction was related to the loan sharking business that it suspected Customer 27 operated: SMR dated 30 August 2019.

On 4 February 2021, Customer 21 engaged in a number of suspicious cash and chip exchanges at SCA alongside Person 17 and two other associates, including Person 6:

a. Shortly after midnight on 4 February 2021, Person 17 exchanged $10,000 in cash for chips at an SCA Cashier.

b. Person 17 then handed the $10,000 in chips to Customer 21, who commenced play at a gaming table.

c. Customer 21 then handed $10,000 in chips back to Person 17.

d. Soon after, Person 17 returned to an SCA Cashier and exchanged the $10,000 in chips for chips of different denominations. Customer 21 also left the gaming table and joined Person 17 at the Cashier. Person 17 then handed $1,000 in chips to Customer 21.

e. Shortly after this transaction, Person 17 handed the remaining $9,000 in chips to Customer 21.

f. Subsequently, Customer 21 handed $12,350 in chips to Person 6. The other associate then exchanged these chips for cash at an SCA Cashier.

g. Shortly after this transaction, the other associate handed the $12,350 in cash to Person 17. Person 17 then placed the cash into their bag.

h. Soon after that exchange, Customer 21, Person 17 and the two other associates, including Person 6, departed the Grange Room and departed the SCA premises.

SCA considered that these transactions were suspicious. It concluded that Customer 21 was using Person 17 and the two other associates to conduct threshold transactions on behalf of Customer 21 in order to avoid reporting requirements. It noted that Person 17 appeared to be in a relationship with Customer 21. It also noted that the other two associates shared a residential address and had previously entered VIP premises at SCA as guests of Customer 21: SMR dated 9 February 2021.

e. Customer 21 was connected to other customers at SCA, including high-risk players such as Customer 2 and Customer 27, and customers in respect of whom SCA had formed suspicions, such as Person 17;

Particulars

See particulars to paragraphs 843.d and 843.f.

SCA suspected that Customer 21 was acting in concert with Customer 2, Customer 27 and their associates, including Person 17, to:

a. deliberately structure transactions to avoid reporting obligations; and

b. engage in prohibited money lending.

f. Customer 21 transacted using large amounts of cash and cash that appeared suspicious at SCA;

Particulars

See paragraphs 376 to 381 above.

See particulars to paragraph 843.d above.

TTRs

Between 9 December 2016 and 31 March 2021, SCA gave the AUSTRAC CEO 71 TTRs detailing incoming and outgoing payments made by Customer 21 totalling $2,376,820, which comprised:

a. 43 TTRs totalling $961,940 in cash and chips exchanges;

b. 24 TTRs totalling $1,280,000 in account deposits; and

c. four TTRs totalling $134,880 in account withdrawals.

Large cash transactions

Between 23 December 2016 and 30 January 2021, Customer 21 deposited $121,454 in cash into their SCA FMA in 31 transactions in amounts below the transaction reporting threshold.

Between 9 January 2017 and 14 March 2021, Customer 21 withdrew $45,353 in cash from their SCA FMA in 23 transactions in amounts below the transaction reporting threshold.

Between 3 June 2019 and 14 March 2021, Customer 21 exchanged $39,200 in cash for chips at SCA in nine transactions in amounts below the transaction reporting threshold.

On 10 June 2017, Customer 27 handed a shopping bag to Customer 21 containing $60,000 in cash on SCA premises. Customer 21 then exchanged this cash for a $60,000 CPV at an SCA Cashier. Customer 21 then exchanged this $60,000 CPV for chips at a gaming table. After this transaction was completed, Customer 21 immediately left the gaming table, met Customer 27 and gave the $60,000 in chips to Customer 27. SCA later observed Customer 27 standing by a Cashier counting a handful of $5,000 chips in their hand. SCA considered that these transactions were unusual as Customer 21 did not typically participate in gambling activity anywhere near this level of buy-in whereas Customer 27 recorded substantial play with no cash buy-in: SMR dated 13 June 2017.

On 30 June 2017, Customer 21 deposited $180,000 in cash into their SCA FMA. SCA issued two CPVs of $90,000 each to Customer 21. Customer 21 then attended two different gaming tables in the Grange Room and exchanged one CPV for cash at each table. Customer 21 then covertly passed the $180,000 in cash to Customer 27.

SCA noted that Customer 21 had attempted to hide the exchange by passing the money under a table with the assistance of Person 17 who placed the cash into the vest pocket of Customer 27's jacket. SCA considered that these transactions were suspicious. It noted that Customer 27 subsequently played and recorded a loss of $142,000, which was their largest loss recorded at SCA. By contrast, it noted that Customer 21 only recorded a loss of $3,600 for the day, which was not at the level expected from their FMA deposit, and Person 17 did not have any recorded play on table games. SCA also noted that Customer 27 routinely used associates to avoid recording significant transactions against their name: SMR dated 3 July 2017.

On 8 March 2021, Customer 21 withdrew approximately $80,000 in chips from their SCA account. Customer 21 then gambled with some of these chips but gave the majority to Customer 2. SCA suspected that, sometime later, Customer 2 arranged for an unknown third party to give $80,000 in cash to Customer 21 outside of CCTV coverage, likely as repayment for the $80,000 in chips.

SCA then observed Customer 21 give an unknown amount of cash to Person 6. Customer 21 and Person 6 then attended an SCA Cashier and attempted to use the cash to purchase chips. However, Customer 21 advised that they were not willing to have their details recorded against the transaction. SCA considered that this activity was unusual. It considered that Customer 21 was deliberately attempting to avoid the reporting requirements. It also noted that Customer 21 had previously used Person 6 for this purpose: SMR dated 15 March 2021.

g. Customer 21 and their associates engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including structuring and cashing-in large value chips with no evidence of play;

Particulars

See paragraph 24 above.

Between 13 December 2016 and 14 May 2019, Customer 21 withdrew $100,000 in CPVs from their SCA FMA in 15 transactions in amounts below the transaction reporting threshold.

Between 14 April 2019 and 27 May 2019, Customer 21 withdrew $24,900 in chips from their SCA FMA in eight transactions in amounts below the transaction reporting threshold.

The above transactions were indicative of the ML/TF typology of structuring.

Between 22 December 2016 and 8 March 2021, Customer 21 and their associates were involved in at least 10 transactions indicative of the ML/TF typology of cashing-in large value chips with no evidence of play. The total value of these transactions was at least $479,350.

See paragraphs 843.d and 843.f above.

h. Customer 21 had access to private gaming rooms at SCA; and

Particulars

See paragraph 145(e) above.

Customer 21 had access to private gaming rooms at SCA, including the Black Room, the Grange Room and the Platinum Room.

i. SCA did not have adequate reason to believe that Customer 21's source of wealth or source of funds was sufficient to explain the high value gambling services (table 3, s 6 of the Act) provided to Customer 21 by SCA.

Particulars

See paragraph 516 above.

By 7 December 2016, SCA understood that Customer 21 was a restaurant entrepreneur. Between 23 September 2015 and 6 May 2016, SCA had previously understood that Customer 21 was a property developer and contractor.

By 23 December 2016, SCA understood that Customer 21 owned two restaurants in South Australia and possibly more in Victoria.

From 2017, SCA suspected that Customer 21 and their associates were engaging in loan sharking and other activities indicative of ML/TF typologies: see paragraph 843.d above. SCA identified a number of suspicious transactions in which Customer 21 and multiple third parties exchanged chips and cash.

Between 2016 and 2020, SCA recorded turnover exceeding $18,000,000 for Customer 21.

On 22 September 2021, SCA noted that it still needed to confirm Customer 21's source of wealth.

At no time was SCA's understanding of Customer 21's source of wealth or source of funds commensurate with the high value gambling services that they received at SCA.

SCA's determination of the ML/TF risks posed by Customer 21

844. On and from 23 December 2016, Customer 21 was appropriately rated by SCA as a high risk customer for the purpose of the Act and Rules.

845. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 21 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by it with respect to Customer 21.

Monitoring of Customer 21's transactions

846. At no time did SCA apply appropriate transaction monitoring to Customer 21's transactions because SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

The review, update and verification of Customer 21's KYC information

847. SCA did not review, update or verify Customer 21's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 21, including the nature, extent and purpose of Customer 21's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 21's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 21's risk profile* above, there were higher ML/TF risks associated with Customer 21's source of wealth or source of funds.

On and from 2017, SCA suspected that Customer 21 and their associates were engaging in loan sharking and other behaviour indicative of ML/TF typologies, suggesting that there were real ML/TF risks as to Customer 21's source of funds (see paragraph 843.d above).

d. to the extent that SCA reviewed Customer 21's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 21.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

In April 2019, SCA reviewed Customer 21's place of residence and obtained an updated scan of their driver's licence. SCA also reviewed Customer 21's individual gambling activity.

On 19 September 2019, SCA asked Customer 21 to provide evidence of current personal identification.

ECDD triggers in respect of Customer 21

848. SCA was required to apply the ECDD program to Customer 21 following any ECDD triggers in respect of Customer 21.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1),15.9(3) and 15.10 of the Rules.

849. Customer 21 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 23 December 2016 and 15 March 2021, SCA gave the AUSTRAC CEO seven SMRs with respect to Customer 21.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer* 21 above.

850. Each matter pleaded in paragraph 849 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

851. SCA did not conduct appropriate risk-based ECDD with respect to Customer 21 following an ECDD trigger because.

a. on each occasion prior to 22 March 2022 that SCA conducted ECDD in respect of Customer 21 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 21 and failed to appropriately consider whether the ML/TF risks posed by Customer 21 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501, 511 and 516 to 517 above.

Between 7 December 2016 and 19 January 2022, SCA conducted ECDD in respect of Customer 21.

Database alerts

Between 7 December 2016 and 19 January 2022, SCA received six open source Dow Jones watchlist alerts and 26 transaction alerts in respect of Customer 21, which triggered a manual review of Customer 21's transactions which was conducted by SCA's AML team.

Transaction reviews

In April 2017, June 2017, July 2017, August 2019, February 2021 and March 2021, SCA surveillance operators reviewed SCA's surveillance records of Customer 21's transactions. On each occasion, the review confirmed that Customer 21 had engaged in suspicious transactions, including with Customer 2, Customer 27, Person 6, Person 17 and Person 18.

In March 2021, an SCA surveillance operator commented that Customer 21's conduct had always been a bit "iffy".

In March 2021, an SCA AML Analyst conducted a compliance investigation and concluded that Customer 21's conduct appeared to be relatively harmless. The AML Analyst reached this conclusion despite the fact that, by this date, SCA had:

a. given the AUSTRAC CEO seven SMRs in respect of Customer 21 reporting large and suspicious cash transactions with a value of more than $554,700; and

b. observed on at least four occasions that Customer 21 was engaged in loan sharking with large amounts of cash in concert with other high risk customers including Customer 2 and Customer 27.

ECDD screening

On 12 September 2019, SCA conducted ECDD in respect of Customer 21. This ECDD screening consisted of reviews of:

a. historical SMRs submitted in respect of Customer 21;

b. Customer 21's source of wealth, which recorded their occupation as a restaurant owner;

c. Customer 21's associates; and

d. open source media in respect of Customer 21, which identified no adverse information.

There are no records of any further steps taken by SCA to conduct ECDD in respect of Customer 21, having regard to the ML/TF risks pleaded in *Customer 21's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to Customer 21's higher ML/TF risks: see *Customer 21's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 21's source of funds or source of wealth.

By reason of the matters set out in *Customer's 21's risk profile* above, there were higher ML/TF risks associated with Customer 21's source of wealth or source of funds.

However, it was not until 22 March 2022 that SCA issued a ban in respect of Customer 21 following in-house investigations by the AML team and adverse open source media in respect of Customer 21.

b. at no time prior to 22 March 2022 did senior management consider the higher ML/TF risks posed by Customer 21 in response to an ECDD trigger, or appropriately consider whether the ML/TF risks posed by Customer 20 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

It was not until 22 March 2022 that SCA issued a ban in respect of Customer 21.

Contravention of s 36 of the Act in respect of Customer 21

852. By reason of the matters pleaded from paragraphs 840 to 851, on and from 7 December 2016, SCA:

a. did not monitor Customer 21 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

853. By reason of the matters pleaded at paragraph 852, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 22 March 2022 with respect to Customer 21.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 22

854. Customer 22 was a customer of SCA during the relevant period. Between 2017 and 2022, SCA recorded turnover exceeding $58,000,000 for Customer 22.

Particulars

Customer 22 was a customer of SCA from at least 7 January 2016.

As at 28 October 2022, Customer 22 remained a customer of SCA and had not been banned.

855. SCA provided Customer 22 with designated services within the meaning of table 1 and table 3, s 6 of the Act during the relevant period including services as an individual commission player.

Particulars

On 7 January 2016, SCA opened an FMA for Customer 22 which remained open as at 28 October 2022 (item 11, table 3, s 6 of the Act).

While a customer of SCA, Customer 22 remitted funds to and from their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 22's risk profile* below.

856. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 22.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 22's risk profile

857. On and from 7 December 2016, Customer 22, and the provision of designated services to Customer 22 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 22's risk profile prior to the relevant period

a. by 7 December 2016, Customer 22 had the following risk history:

i. Customer 22 received financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs or individual commission programs;

Particulars

In the 2016 financial year, Customer 22's recorded individual rated gambling activity for non-commission play on EGMs at SCA was estimated as turnover of $15,350 with losses of $865.

ii. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 22 by remitting money into the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

For example, on 7 January 2016, Customer 22 received $20,000 into their SCA FMA via telegraphic transfer. SCA made these funds available to Customer 22.

Remittances from SCA FMAs to SCEG New Zealand FMAs

On 14 January 2016, SCA accepted instructions to transfer $19,135 from Customer 22's SCA FMA to Customer 22's FMA at a SCEG New Zealand casino.

iii. Customer 22 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 8 January 2016 and 18 January 2016, SCA gave the AUSTRAC CEO two TTRs detailing incoming and outgoing payments made by Customer 22 totalling $39,135, which comprised:

a. one TTR totalling $20,000 for an account deposit; and

b. one TTR totalling $19,135 for an account withdrawal.

Customer 22's risk profile during the relevant period

b. Customer 22 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs or individual commission programs. Between 2017 and 2020, SCA recorded escalating turnover estimated at $1,731,639 for Customer 22, with cumulative losses of $282,875 on non-commission programs;

Particulars

In the 2018 financial year, Customer 22's recorded individual rated gambling activity for non-commission play on EGMs at SCA escalated to an estimated turnover of $260,870 with losses of $57,814.

In the 2019 financial year, Customer 22's recorded individual rated gambling activity for non-commission play on EGMs at SCA escalated to an estimated turnover of $827,794 with losses of $91,065.

In the 2020 financial year, despite closures due to the COVID-19 pandemic, Customer 22's recorded individual rated gambling activity for non-commission play on EGMs at SCA escalated to an estimated turnover of $6,429,375 with losses of $133,996.

c. Customer 22 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA from play on individual commission programs, and a commission of $585,107 was recorded as payable by SCA to Customer 22;

Particulars

Between 17 December 2020 and 9 February 2022, Customer 22 played on 14 individual commission programs at SCA.

In the 2021 financial year, Customer 22's individual rated gambling activity on individual commission programs at SCA was an estimated buy-in of $1,109,800, turnover of $15,499,086 with losses of $1,699,540. A commission of $143,189 was payable by SCA to Customer 22 from play on individual commission programs.

In the 2022 financial year, Customer 22's individual rated gambling activity on individual commission programs at SCA escalated to an estimated buy-in of $2,208,000, turnover of $27,553,126 with losses of $945,341. A commission of $334,900 was payable by SCA to Customer 22 from play on individual commission programs.

In the first half of the 2023 financial year, Customer 22's individual rated gambling activity on individual commission programs at SCA was an estimated buy-in of $817,000, turnover of $8,261,187 with losses of $712,731. A commission of $107,018 was payable by SCA to Customer 22 from play on individual commission programs.

d. Customer 22 received additional benefits from SCA in their capacity as an individual commission player;

Particulars

Customer 22 received additional benefits in their capacity as an individual commission program player, including non-gaming complimentary services. For example, during their individual commission program which ran between 12 March 2021 and 14 March 2021, Customer 22 received $2,745 in complimentary deductions on hotel rooms and food and beverages.

e. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 22 by remitting large amounts of money into, out of and within the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCEG customer account channel

On 26 July 2018, $15,000 was deposited into an account held by SCEG in Australia on behalf of Customer 22, which SCA made available to Customer 22 and which was deposited into Customer 22's FMA.

Remittances through the SCA customer account channel

A report dated October 2021 prepared by Bank 1 identified that between 1 September 2019 and 31 May 2021, Customer 22 was a top depositor by value and volume into SCA's bank account. Bank 1 identified that during this period, Customer 22 made at least 72 deposits totalling $1,672,000.

SCA made money available to Customer 22 in the following transactions:

a. Between 14 December 2017 and 27 May 2022, Customer 22 received $4,326,000 into their SCA FMA via telegraphic transfer in 179 separate transactions. On several occasions, Customer 22 received multiple transfers in one day. Some of these transfers were from Customer 22's personal bank account in Australia.

SCA accepted instructions to transfer funds from Customer 22's accounts for the following transactions:

a. Between 19 February 2020 and 4 August 2022, Customer 22 transferred $2,779,103 in 21 separate transactions from their SCA FMA to their personal bank account in Australia.

Remittances through the SkyCity New Zealand channel

On 10 August 2019, SCA credited $2,501 to Customer 22's FMA with the funds originating from Customer 22's FMA held at a SCEG New Zealand casino. SCA made the funds available to Customer 22.

Remittances from SCA FMAs to SCEG New Zealand FMAs

On 7 February 2019, SCA transferred $2,501 from Customer 22's SCA FMA to Customer 22's FMA held at a SCEG New Zealand casino.

f. designated services provided to Customer 22 included substantial EGM activity at SCA;

Particulars

See paragraphs 352 and 353 above.

See particulars to paragraphs 857.b and 857.c above.

On 21 January 2022, the SCEG General Manager Finance for SCA noted that Customer 22 was probably SCA's largest EGM customer.

g. SCA was aware that Customer 22 frequently engaged in large buy-ins and cash outs, including with cash, telegraphic transfers and cheques;

Particulars

SCA frequently recorded that Customer 22 made significant buy-ins or cash outs at SCA. For example:

a. on 27 July 2018, Customer 22 received $16,462 in cash from an EGM payout;

b. on 19 February 2020, Customer 22 received $13,979 in cash following a jackpot win;

c. on 11 March 2020, Customer 22 made a buy-in using $55,000 they had telegraphically transferred to their FMA;

d. on 26 December 2020, Customer 22 withdrew $350,000 from their FMA, comprising a cheque for $300,000 and $50,000 in cash; and

e. on 8 July 2021, Customer 22 transferred $145,000 to their SCA FMA over six transactions and made a buy-in on an EGM commission program.

h. Customer 22 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 19 December 2017 and 14 January 2022, SCA gave the AUSTRAC CEO 79 TTRs detailing incoming and outgoing payments made by Customer 22 totalling $3,117,191, which comprised:

a. four TTRs totalling $156,106 in EGM payouts;

b. one TTR totalling $29,777 in premium player commissions;

c. 68 TTRs totalling $1,690,000 in account deposits; and

d. six TTRs totalling $962,307 in account withdrawals.

i. Customer 22 had access to private gaming rooms at SCA; and

Particulars

See paragraph 145(e) above.

Customer 22 had access to private gaming rooms at SCA, including the Black Room and the Platinum Room.

j. SCA did not have adequate reason to believe that Customer 22's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 22 by SCA.

Particulars

See paragraph 516 above.

By 7 December 2016, SCA understood that Customer 22 was the Managing Director of a construction company.

On 25 November 2021, Customer 22 provided SCA with a completed Patron Credentials Disclosure Form. Based on information in the form and open source searches conducted by SCA, SCA estimated that Customer 22's annual salary was around $220,000.

Despite this, at no time did SCA request adequate source of wealth or source of funds information from Customer 22. On 10 May 2022, the SCEG AML/CTF Compliance & Intelligence Manager noted that formal source of wealth information was needed for Customer 22. On 3 June 2022, SCA noted that the completion of a financial profile for Customer 22 was a priority. There are no records of either item being completed.

At no time was SCA's understanding of Customer 22's source of wealth or source of funds commensurate with the high value financial and gambling services that Customer 22 received at SCA.

Between 2017 and 2022, SCA recorded turnover exceeding $58,000,000 for Customer 22.

SCA's determination of the ML/TF risks posed by Customer 22

858. SCA was unable to appropriately identify or assess the ML/TF risks posed by Customer 22 because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 22.

a. On and from late 2019, Customer 22 should have been recognised by SCA as a high risk customer for the purpose of the Act and Rules for the reasons pleaded above: see *Customer 22's risk profile* above.

Particulars

Sections 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

b. It was not until 4 January 2021 that Customer 22 was rated high risk by SCA for the purpose of the Act and Rules.

Monitoring of Customer 22's transactions

859. At no time did SCA apply appropriate transaction monitoring to Customer 22's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities;

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 22 through the SCEG customer account channel, the SCA Customer account channel and the SkyCity New Zealand channel, which were high risk remittance channels;

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 22's KYC information

860. SCA did not review, update or verify Customer 22's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 22, including the nature, extent and purpose of Customer 22's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 22's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 22's risk profile* above, there were higher ML/TF risks associated with Customer 22's source of wealth or source of funds.

d. to the extent that SCA reviewed Customer 22's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 22.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

On 5 March 2017 and 23 January 2020, SCA received open source Dow Jones watchlist alerts in respect of Customer 22.

KYC screening

Following a request from the AML team, on 25 November 2021 Customer 22 provided SCA with a completed Patron Credentials Disclosure Form. In the form, Customer 22 stated that they were the owner of a construction company. On the same day, SCA completed an International Business Enhanced Know Your Customer Application for Customer 22. As part of the application, SCA conducted an open source review with respect to Customer 22. The review identified that:

a. Customer 22's occupation had been verified as the Managing Director of a construction firm and a property investment firm. SCA estimated Customer 22's income from both roles to be a total of $220,000 a year; and

b. No adverse open source information with respect to Customer 22 was found.

Based on the above, the SCA Compliance Manager determined that Customer 22 should be approved to continue playing at SCA. SCA relied on the fact that Customer 22's gaming transactions (generally a $150,000 buy-in) did not exceed their estimated income level ($200,000 per year). This decision was made despite the fact that in the 2020 financial year, despite closures due to the COVID-19 pandemic, Customer 22's recorded individual rated gambling activity on EGMs at SCA escalated to over $6,400,000 from around $800,000 in the previous financial year.

Customer 22 subsequently commenced a new individual commission program on 26 November 2021.

Failure to apply appropriate due diligence suited to the high ML/TF risks

861. Had SCA conducted ongoing customer due diligence on and from 7 December 2016 by:

a. appropriately identifying and assessing the ML/TF risks posed by Customer 22;

b. applying appropriate risk-based transaction monitoring to Customer 22; and

c. appropriately reviewing and updating Customer 22's KYC information, having regard to the high ML/TF risks,

SCA would have been required by the Act and Rules to apply the ECDD Program to Customer 22 at a time before the date of the ECDD trigger pleaded below: see *ECDD triggers in respect of Customer 22*.

ECDD triggers in respect of Customer 22

862. SCA was required to apply the ECDD program to Customer 22 following any ECDD triggers in respect of Customer 22.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1) and 15.10 of the Rules.

863. Customer 22 was determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 22* above.

864. The matter pleaded in paragraph 863 was an ECDD trigger.

Particulars

See paragraphs 496 and 504 above.

865. SCA did not conduct appropriate risk-based ECDD with respect to Customer 22 following an ECDD trigger because:

a. on each occasion that SCA conducted ECDD in respect of Customer 22 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 22 and failed to appropriately consider whether the ML/TF risks posed by Customer 22 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501, 511 and 516 to 517 above.

Watchlist alerts

Between 22 November 2021 and 24 November 2021, SCA conducted Jade watchlist screenings with respect to Customer 22 and companies with which they were associated.

ECDD screenings

On or around 16 August 2021 and 18 October 2021, SCA conducted ECDD screening in respect of Customer 22. The screenings identified that Customer 22 was a Managing Director at a construction company and at a property company, and identified an open source media article which reported on Customer 22's work at their construction company.

The ECDD conducted by SCA did not have appropriate regard to Customer 22's higher ML/TF risks: see *Customer 22's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 22's source of funds or source of wealth.

By reason of the matters set out in *Customer 22's risk profile* above, there were real risks that Customer 22's source of wealth and source of funds were not legitimate.

b. on any occasion that senior management considered the higher ML/TF risks posed by Customer 22 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 22 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

Transaction Monitoring Overview reports

Between February 2020 and February 2021, Customer 22 was mentioned in three 'Transaction Monitoring Overview' reports for the period November 2019 to February 2021, which were provided to the AML/CTF Senior Management Group for discussion at their meetings.

Senior management consideration of KYC information

On 25 November 2021, the results of the open source review with respect to Customer 22, and Customer 22's completed Patron Credentials Disclosure Form, were provided to SCA's General Manager AML and the SCEG Group Manager International Gaming. The SCEG Group Manager International Gaming responded that the form should be processed as per the KYC Standard, but that Customer 22 could be allowed to play immediately if the SCA Compliance Manager confirmed they were comfortable with the historical checks conducted with respect to Customer 22. The SCA Compliance Manager confirmed that they had no concerns with respect to Customer 22.

Senior management consideration of Customer 22's telegraphic transfers

On 21 January 2022, Bank 1 informed SCA that a telegraphic transfer from Customer 22 to SCA's bank account for $100,000 had been held pending review. The SCEG General Manager of Finance for SCA responded that Customer 22 was a regular interstate visitor who was probably SCA's largest EGM player. The General Manager also stated that the funds were for Customer 22's use when they arrived at SCA and that SCA had made two large payments to Customer 22 in January totalling $603,000. Bank 1 then approved the release of the funds.

On 8 February 2022, Bank 1 again asked SCA for further information regarding a telegraphic transfer from Customer 22 to SCA's bank account for $110,000. The SCEG General Manager of Finance for

SCA directed Bank 1 to the previous correspondence in relation to the transfer on 21 January 2022, and stated that the funds were for gaming. The SCEG General Manager of Finance stated that they could not be sure how often Customer 22 would attend SCA, but noted that Customer 22 was a fairly regular visitor. The funds were then released.

Contravention of s 36 of the Act in respect of Customer 22

866. By reason of the matters pleaded from paragraphs 854 to 865 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 22 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

867. By reason of the matters pleaded at paragraph 866, SCA contravened s 36(1) of the Act on and from 7 December 2016 with respect to Customer 22.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 23

868. Customer 23 was a customer of SCA during the relevant period. Between the 1 July 2016 and 30 June 2021, SCA recorded turnover exceeding $4,700,000 for Customer 23 on individual commission programs and non-commission gambling.

Particulars

Customer 23 was a customer of SCA from at least 12 June 2014.

On 1 June 2022, SCA issued a ban in respect of Customer 23.

869. SCA provided Customer 23 with designated services within the meaning of tables 1 and 3, s 6 of the Act during the relevant period including services as an individual commission player.

Particulars

Prior to 7 December 2016, SCA opened an FMA for Customer 23 which was closed on 11 June 2022 (item 11, table 3, s 6 of the Act).

While a customer of SCA, Customer 23 remitted funds to and from their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 23's risk profile* below.

870. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 23.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 23's risk profile

871. On and from 7 December 2016, Customer 23, and the provision of designated services to Customer 23 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 23's risk profile prior to the relevant period

a. by 7 December 2016, Customer 23 had the following risk history:

i. SCA had formed suspicions for the purposes of s 41 of the Act with respect to Customer 23;

Particulars

SCA gave the AUSTRAC CEO an SMR on one occasion, on 12 June 2014.

The SMR reported that Customer 23 cashed in $7,000 worth of chips, and then tried to cash in a further $8,400 worth of chips. When asked for identification in relation to the second transaction, Customer 23 and took back the chips. When Customer 23 was asked why they were unwilling to provide identification they responded that they did not like to be reported on.

ii. Customer 23 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 15 April 2014 and 28 July 2016, SCA gave the AUSTRAC CEO 11 TTRs detailing incoming and outgoing payments made by Customer 23 totalling $1,134,401, which comprised:

a. three TTRs totalling $60,000 in the issue of chips or tokens;

b. two TTRs totalling $48,474 in account deposits;

c. one TTR totalling $751,645 in an international funds transfer; and

d. seven TTRs totalling $1,089,268 in account withdrawals.

iii. Customer 23 had received financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket or individual commission programs;

Particulars

In the 2016 financial year, Customer 23's recorded individual rated gambling activity on table games at SCA was estimated as a buy-in of $5,600, turnover of $95,076 with losses of $33,900.

iv. Customer 23 had received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA from play on individual commission programs, and a commission of $36,731 was recorded as payable by SCA to Customer 23 on individual commission programs;

Particulars

In the 2016 financial year, Customer 23's recorded individual rated gambling activity on individual commission programs at SCA was estimated as a buy-in of $150,000, cash turnover of $6,121,800 with losses of $315,915. A commission of $36,731 was payable by SCA to Customer 23 from play on individual commission programs.

v. on 27 May 2016, SCA provided Customer 23 with a significant amount of credit upon request, up to a limit of $50,000; and

Particulars

See paragraphs 321 to 323, and 342 above.

vi. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 23 by remitting money from overseas;

Particulars

See paragraphs 232 to 312 above.

In 2014, SCA reported an incoming IFTI from a SCEG New Zealand casino totalling $751,645 where Customer 23 was named as the beneficiary customer.

In 2016, SCA reported an incoming IFTI from the SCEG New Zealand casino account totalling $28,474 where Customer 23 was named as the beneficiary customer.

Customer 23's risk profile during the relevant period

b. Customer 23 received financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket or individual commission programs;

i. between 1 July 2016 and 30 June 2021, SCA recorded a turnover for non-commission play of $1,440,068 for Customer 23, with cumulative losses of $6,550;

Particulars

In the 2017 financial year, Customer 23's recorded individual rated gambling activity for non-commission play at SCA was estimated as a buy-in of $0, cash turnover of $43,000, and with wins of $6,200.

In the 2019 financial year, Customer 23's recorded individual rated gambling activity for non-commission play at SCA was estimated as a buy-in of $1,200, cash turnover of $668, and with losses of $600.

In the 2020 financial year, despite closures related to the COVID-19 pandemic, Customer 23's recorded individual rated gambling activity for non-commission play at SCA escalated to an estimated buy-in of $12,000, cash turnover of $826,150, and with losses of $450.

In the 2021 financial year, Customer 23's recorded individual rated gambling activity for non-commission play at SCA was estimated as a buy-in of $35,400, cash turnover of $570,250, and with losses of $11,700.

c. Customer 23 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA from play on individual commission programs, and a commission of $440,715 was recorded as payable by SCA to Customer 23 on individual commission programs;

Particulars

In the 2019 financial year, Customer 23's recorded individual rated gambling activity on individual commission programs at SCA was estimated as a buy-in of $54,100, cash turnover of $199,034, and with losses of $54,300. A commission of $1,096 was payable by SCA to Customer 23 from play on individual commission programs.

In the 2021 financial year, Customer 23's recorded individual rated gambling activity on individual commission programs at SCA escalated to an estimated buy-in of $3,300,800, cash turnover of $74,757,432, and with wins of $185,175. A commission of $439,619 was payable by SCA to Customer 23 from play on individual commission programs.

In February 2021, Customer 23 was named as a significant player in an SCA 'Early Gaming Report'.

d. Customer 23 received additional benefits from SCA in their capacity as an individual commission player;

Particulars

For example, Customer 23 received benefits of $2,273 in relation to an individual commission program on which they played from 20 February 2021 to 21 February 2021. These benefits included non-gaming complimentary services such as hotel accommodation, airfares and food and beverage expenses.

Customer 23 received benefits of $3,496 in relation to an individual commission program on which they played from 27 February 2021 to 1 March 2021. These benefits included non-gaming complimentary services such as hotel accommodation and food and beverage expenses.

e. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 23 by remitting large amounts of money into and out of the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

SCA made money available to Customer 23 in the following transactions:

a. Between 27 February 2021 and 17 April 2021 Customer 23 received $136,000 into their SCA FMA via telegraphic transfer in five separate transactions.

SCA accepted instructions to transfer funds from Customer 23's accounts for the following transactions:

a. Between 21 February and 10 March 2021 Customer 23 was refunded $283,242 from their SCA FMA via telegraphic transfer in three separate transactions.

b. In February 2021, Customer 23 received a telegraphic transfer from SCA of $619,726 which represented a part settlement for their play on an individual commission program.

c. In March 2021, Customer 23 received a telegraphic transfer from SCA of $190,000 which represented a part settlement for their play on an individual commission program.

f. Customer 23 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 5 November 2018 and 29 April 2021, SCA gave the AUSTRAC CEO 27 TTRs detailing incoming and outgoing payments made by Customer 23 totalling $1,810,243, which comprised:

a. 10 TTRs totalling $273,175 in chip and cash exchanges;

b. nine TTRs totalling $375,800 in account deposits;

c. seven TTRs totalling $1,089,268 in account withdrawals; and

d. one TTR totalling $72,000 in a premium player commission.

Other cash transactions

An SCA spreadsheet titled 'Player AML data' noted that on 27 February 2020, Customer 23 made two transactions exchanging chips for cash, in the amounts of $7,000 and $8,000 respectively.

g. Customer 23 had access to private gaming rooms at SCA; and

Particulars

See paragraph 145(e) above.

Customer 23 had access to private gaming rooms at SCA, including the Grange Room and the Platinum Room.

h. SCA did not have adequate reason to believe that Customer 23's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 23 by SCA.

Particulars

See paragraph 516 above.

SCA recorded Customer 23's occupation as 'Rail Manager' from May 2016.

In the 2021 financial year Customer 23's buy-in on individual commission programs escalated to over $3,300,000, from just over $54,000 the previous financial year. Customer 23's gambling activity was inconsistent with SCA's understanding of their source of funds and source of wealth.

Despite this inconsistency, SCA did not take appropriate steps to review and verify Customer 23's source of wealth or source of funds.

At no time was SCA's understanding of Customer 23's source of wealth or source of funds commensurate with Customer 23's gambling and transactional activity.

SCA's determination of the ML/TF risks posed by Customer 23

872. By 7 December 2016, Customer 23 was appropriately rated by SCA as a high risk customer for the purpose of the Act and Rules.

873. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 23 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by it with respect to Customer 23.

Monitoring of Customer 23's transactions

874. At no time did SCA apply appropriate transaction monitoring to Customer 23's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 23 through the SCA Customer account channel, which was a high risk remittance channel.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 23's KYC information

875. SCA did not review, update or verify Customer 23's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 23, including the nature, extent and purpose of Customer 23's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 23's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 23's risk profile* above, there were higher ML/TF risks associated with Customer 23's source of wealth or source of funds.

d. to the extent that SCA reviewed Customer 23's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 23.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

ECDD triggers in respect of Customer 23

876. SCA was required to apply the ECDD program to Customer 23 following any ECDD triggers in respect of Customer 23.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1) and 15.10 of the Rules.

877. Customer 23 was determined by SCA to be high risk for the purpose of the Act and Rules prior to the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 23* above.

878. The matter pleaded in paragraph 877 was an ECDD trigger.

Particulars

See paragraphs 496 and 504 above.

879. SCA did not conduct appropriate risk-based ECDD with respect to Customer 23 following an ECDD trigger because:

a. on each occasion prior to 1 June 2022 that SCA conducted ECDD in respect of Customer 23 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 23 and failed to appropriately consider whether the ML/TF risks posed by Customer 23 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501, 511 and 516 to 517 above.

On 8 May 2019, SCA conducted an ECDD screening in respect of Customer 23. The ECDD screening included information from the SMR given to the AUSTRAC CEO on 12 June 2014; stated that Customer 23's occupation, source of wealth and source of funds was as a Rail Manager; and listed the URLs for Customer 23's LinkedIn and Facebook pages.

On 20 May 2021 and 9 March 2022, SCA conducted a PEP screening in respect of Customer 23. The screenings did not return a result.

In September 2021, the SCEG International Business team performed watchlist checks in relation to Customer 23, with no derogatory information found. The International Business team also performed a Google search which revealed that Customer 23's LinkedIn page listed that they were self-employed, and that they had been registered as an individual/sole trader since February 2016. However, it is unclear if this information was provided to SCA by the International Business team.

The ECDD conducted by SCA did not have appropriate regard to Customer 23's higher ML/TF risks: see *Customer 23's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 23's source of funds or source of wealth.

By reason of the matters set out in *Customer 23's risk profile* above, there were higher ML/TF risks associated with Customer 23's source of wealth or source of funds.

It was not until 1 June 2022 that SCA issued a ban in respect of Customer 23.

b. on any occasion prior to 1 June 2022 that senior management considered the higher ML/TF risks posed by Customer 23 in response to an ECDD trigger, senior

management failed to appropriately consider whether the ML/TF risks posed by Customer 23 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

Customer 23 was mentioned in a 'Transaction Monitoring Overview' report for the period 1 February 2021 to 1 May 2021, which was provided to the AML/CTF Senior Management Group for discussion at their meeting.

The report noted that in February 2021, SCA had provided Customer 23 with three cheques (a cheque for $100,000 on 22 February 2021, and two cheques for $200,000 and $700,000 respectively on 28 February 2021). The report noted that these cheques related to commission play and tables wins.

It was not until 1 June 2022 that SCA issued a ban in respect of Customer 23.

Contravention of s 36 of the Act in respect of Customer 23

880. By reason of the matters pleaded from paragraphs 868 to 879 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 23 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

881. By reason of the matters pleaded at paragraph 880, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 1 June 2022 with respect to Customer 23.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 24

882. Customer 24 was a customer of SCA during the relevant period. Between 7 December 2016 and 13 December 2021, SCA recorded turnover exceeding $730,000,000 for Customer 24.

Particulars

Customer 24 was a customer of SCA from at least 10 November 2012.

On 3 February 2022, SCA issued a ban in respect of Customer 24 at the direction of the SCA AML team.

883. SCA provided Customer 24 with designated services within the meaning of tables 1 and 3, s 6 of the Act during the relevant period.

Particulars

On 10 November 2012, SCA opened an FMA for Customer 24 which was closed on 3 February 2022 (item 11, table 3, s 6 of the Act).

While a customer of SCA, Customer 24 remitted funds to and from their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 24's risk profile* below.

884. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 24.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 24's risk profile

885. On and from 7 December 2016, Customer 24, and the provision of designated services to Customer 24 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 24's risk profile prior to the relevant period

a. by 7 December 2016, Customer 24 had the following risk history:

i. SCA had formed suspicions for the purposes of s 41 of the Act with respect to Customer 24;

Particulars

SCA gave the AUSTRAC CEO an SMR on three occasions between 20 May 2016 and 6 September 2016. The SMRs reported concerns that Customer 24 had engaged in transactions that were indicative of money laundering, high value gambling activity, and had access to large amounts of cash which did not align to their source of funds.

ii. Customer 24 received designated services through the SCA Customer account channel, which was a high risk channel;

Particulars

Between 20 July 2016 and 15 November 2016, Customer 24 remitted a total of $265,000 to SCA through the SCA Customer account channel in 12 separate transactions.

On 15 November 2016, Customer 24 remitted $1,000 to SCA through the SCA Customer account channel. Ten minutes later, Customer 24 remitted another $9,000 to SCA through the same channel. SCA approved an early release of both transactions despite an SCA AML Analyst noting that:

a. these transactions could be seen as attempts to avoid a threshold transaction report;

b. Customer 24 was known for attempting to avoid threshold transactions; and

c. SCA had previously given the AUSTRAC CEO two SMRs describing suspicious transactions involving Customer 24.

iii. Customer 24 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs;

Particulars

Between 11 April 2016 and 18 November 2016, Customer 24's recorded individual rated gambling activity for table games at SCA was estimated as a buy-in of $5,958,900, turnover of $28,167,483, and with losses of $314,770.

On 10 September 2016, SCA recorded that Customer 24 was a high value player with a very high turnover to buy-in factor, and large recorded wins and losses.

iv. designated services provided to Customer 24 included substantial EGM activity at SCA;

Particulars

See paragraphs 352 and 353 above.

Between 12 April 2016 and 14 November 2016, Customer 24's recorded individual rated gambling activity for EGMs at SCA was estimated as turnover of $60,471 with losses of $825.

v. Customer 24 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 15 April 2016 and 17 November 2016, SCA gave the AUSTRAC CEO 86 TTRs detailing incoming and outgoing payments made by Customer 24 totalling $1,954,839, which comprised:

a. 54 TTRs totalling $1,080,295 in cash and chip exchanges;

b. 22 TTRs totalling $706,000 in account deposits;

c. seven TTRs totalling $130,000 in account withdrawals; and

d. three TTRs totalling $38,544 in foreign currency exchanges.

Large cash transactions

See paragraph 885.a.vii below.

Between July 2016 and November 2016, Customer 24 conducted 11 cash withdrawals from their SCA FMA beneath the reporting threshold totalling $34,805.

vi. Customer 24 and their associates engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including structuring and cashing-in large value chips with no evidence of play;

Particulars

See paragraph 24 above.

In November 2016, Customer 24 and their associates engaged in at least two transactions indicative of the ML/TF typology of structuring with a total value of at least $10,000.

In August 2016 and September 2016, Customer 24 and their associates engaged in at least three transactions indicative of the ML/TF typology of cashing in large value chips with no evidence of play with a total value of $49,000.

vii. Customer 24 engaged in large and unusual transactions, and patterns of transactions, which had no apparent economic or visible lawful purpose; and

Particulars

For example, on 16 August 2016, Customer 24 requested to transfer $20,000 from their SCA account to Person 3. After SCA refused the request because Person 3 was not on site, Customer 24 withdrew $20,000 in cash from their SCA account and purchased chips at a gaming table. Customer 24 intended to give the chips to Person 3 but, because Person 3 was on a program that used a different type of chip, Person 3 could not use them. Instead, Customer 24 gave the chips to a second SCA customer, who then gave the chips to an SCA VIP Host. The VIP host presented the chips at an SCA Cage and the funds were deposited into Person 3's account: SMR dated 17 August 2016.

Following this incident, on 10 September 2016, SCA recorded that Customer 24 may have engaged in chip lending activities.

viii. by April 2016, SCA became concerned that Customer 24's gambling activity was not commensurate with their source of wealth or source of funds;

Particulars

Between 12 April 2016 and 19 April 2016, SCA gave the AUSTRAC CEO seven TTRs detailing cash transactions made by Customer 24 totalling $86,000.

On 19 April 2016, SCA raised concerns that Customer 24's occupation was recorded as "unemployed" despite gaming at levels that could not be sustained by someone with no source of income.

On 21 April 2016, Customer 24 signed a Source of Wealth Declaration stating that they were unemployed, their funds were sourced from "family support", and their family had connections to a foreign company.

By May 2016, SCA reported that Customer 24's explanation as to their source of funds was "questionable": SMR dated 20 May 2016.

Customer 24's risk profile during the relevant period

b. Customer 24 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs. Between 7 December 2016 and 13 December 2021, SCA recorded an estimated buy-in of $72,598,350, a turnover estimated at $735,999,856 for Customer 24, with cumulative losses of $9,081,365;

Particulars

Between 16 December 2016 and 31 December 2017, Customer 24's recorded individual rated gambling activity for table games at SCA was estimated as a buy-in of $3,261,690, turnover of $12,890,106, and with losses of $405,645.

Between 11 July 2017 and 11 August 2017, SCA recorded that Customer 24 was very active in the Grange Room alongside Customer 2 and Customer 17: SMR dated 11 August 2017.

In 2018, Customer 24's recorded individual rated gambling activity for table games at SCA was estimated as a buy-in of $961,935, turnover of $3,006,810, and with losses of $121,835.

In 2019, Customer 24's recorded individual rated gambling activity for table games at SCA was estimated as a buy-in of $469,860, turnover of $1,950,032 with wins of $100,740.

In 2020, despite closures related to the COVID-19 pandemic, Customer 24's recorded individual rated gambling activity for table games at SCA escalated to an estimated buy-in of $8,201,845, turnover of $24,264,119, and with losses of $2,165,290.

Between 1 January 2021 and 13 December 2021, Customer 24's recorded individual rated gambling activity for table games at SCA escalated significantly to an estimated buy-in of $59,703,020, turnover of $709,951,063, and with losses of $6,489,335.

c. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 24 by remitting large amounts of money into, out of, and within the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

See paragraph 885.d below.

SCA made money available to Customer 24 in the following transactions:

a. Between 6 January 2017 and 23 August 2021, SCA received 48 telegraphic transfers totalling $13,108,690 which was made available to Customer 24.

b. On 26 February 2021, Customer 24 remitted $4,440,000 to SCA. While these funds cleared, SCA permitted an early release of $100,000 to enable Customer 24 to play.

d. SCA was aware that Customer 24 had engaged in large and unusual transactions, and patterns of transactions, which had no apparent economic or visible lawful purpose;

Particulars

For example, on 2 January 2017 Customer 24 presented $36,500 in chips at the Grange Room Cashier. Customer 24 advised that the chips belonged to Customer 2 and requested that they be deposited into Customer 2's account. Following a discussion with a VIP Host at the Cashier, Customer 24 retained $11,500 of the chips and exchanged $25,000 in chips for cash before departing with the VIP Host. Customer 24 then gave the cash to Customer 2. Shortly afterwards, Customer 2 reclaimed the commission chips from Customer 24 and exchanged them for cash.

SCA recorded that Customer 24 had conducted a number of cash buy-ins on 19 and 20 January 2017 for $9,900, and considered that Customer 24 was structuring transactions to avoid reporting obligations.

On 12 March 2021, Customer 24 deposited $250,000 in cash into their SCA FMA. Customer 24 then immediately transferred the funds to their personal bank account via telegraphic transfer. Customer 24 advised SCA cash handling staff that they did not intend to play with the funds but instead just wanted the funds transferred.

On 18 September 2021, Customer 24 engaged in table play and recorded a total loss of $410,000 for the day. At the conclusion of play, SCA staff observed that Customer 24 tore up scorecards and gambling help line cards, throwing the pieces over the table.

e. Customer 24 was connected to other customers at SCA, including players who posed higher ML/TF risks such as Customer 2, Customer 17 and Customer 25 and customers in respect of whom SCA had formed suspicions;

Particulars

From 23 January 2017 onwards, SCA understood that:

a. Customer 24 frequently conducted transactions in concert with, and on behalf of, Customer 2, Customer 17 and Customer 25, including buy-ins and cash-outs that were structured so as to avoid reporting obligations;

b. Customer 24 had acted as a personal assistant to Customer 2 and Customer 17, particularly in the Grange Room;

c. Customer 2 and Customer 17 were themselves close associates with suspected business ties, and SCA was concerned about Customer 24's involvement in their relationship;

d. Customer 24 had acted as a “runner” for these customers alongside other customers in respect of whom SCA had formed suspicions; and

e. two other SCA customers acted as runners for Customer 24 and performed buy-ins and cash-outs on Customer 24’s behalf: SMRs dated 23 January 2017, 20 February 2017, 11 August 2017 and 16 August 2018.

On 23 February 2021, SCA staff observed that Customer 24 was associating with another SCA customer in respect of whom it had formed suspicions. SCA noted that the customer was attempting to exchanged $170,000 in cash for chips and that they claimed that their wealth was partially sourced from their parents, which mirrored Customer 24’s claimed source of wealth.

f. designated services provided to Customer 24 included substantial EGM activity at SCA;

Particulars

See paragraphs 352 and 353 above.

Between 16 January 2017 and 11 December 2021, Customer 24's recorded individual rated gambling activity for EGMs at SCA was estimated as turnover of $2,778,691 with losses of $187,206. Customer 24’s turnover escalated significantly from June 2021.

Between 1 August 2021 and 2 August 2021, SCA gave the AUSTRAC CEO four TTRs detailing EGM payouts conducted by Customer 24 at SCA totalling $86,512.

Between 8 January 2017 and 26 September 2021, Customer 24 exchanged at least $96,644 in EGM tickets for cash at SCA in at least 39 transactions below the reporting threshold.

Between 18 July 2017 and 1 September 2021, SCA issued at least $12,510 in EGM tickets to Customer 24 in at least 11 transactions below the reporting threshold.

Between 17 May 2021 and 1 December 2021, Customer 24 transferred over $1,200,000 from EGMs to their cashless gaming card, often conducting multiple transactions on a single day. For example, on 7 August 2021, Customer 24 made 14 ‘cashless out’ transfers totalling $88,136 and ranging between $5,000 and $7,035.

Customer 24 received incentive benefits from SCA due to their substantial EGM activity, including incentives based on their EGM turnover. For example, in December 2021, Customer 24 received incentives worth $84,393 based on EGM play.

g. Customer 24 engaged in transactions:

i. using large amounts of cash and cash that appeared suspicious, including cash presented in a briefcase, at SCA; and

ii. indicative of ML/TF typologies and vulnerabilities, including structuring, cashing-in large value chips with no evidence of play, and quick turnover of money (without betting);

Particulars

See paragraphs 24, and 376 to 381 above.

See paragraph 885.d above.

TTRs

Between 9 January 2017 and 16 December 2021, SCA gave the AUSTRAC CEO 232 TTRs detailing incoming and outgoing payments made by Customer 24 totalling $24,124,165, which comprised:

a. 162 TTRs totalling $5,722,982 in cash and chip exchanges;

b. 53 TTRs totalling $12,398,600 in account deposits;

c. 13 TTRs totalling $6,002,583 in account withdrawals; and

d. four TTRs totalling $86,512 in EGM payouts.

Large and suspicious cash transactions in 2017

Between 19 January 2017 and 20 January 2017, Customer 24 exchanged $59,400 in cash for chips at SCA in six separate transactions of $9,900 each. SCA considered that these transactions were suspicious and noted that Customer 24 had previously been structuring their buy-ins to avoid AML reporting obligations. SCA suspected that Customer 24 conducted these transactions on behalf of Customer 2 and Customer 17: SMR dated 23 January 2017.

On 28 July 2017, Person 14 exchanged $10,000 in cash for chips at an SCA gaming table. The customer then walked with Customer 25 to a second gaming table and passed the $10,000 to Customer 24 in two transactions. Customer 24 then played at the gaming table and lost the chips. Shortly afterwards, Customer 25 exchanged a $20,000 CPV for chips at the second gaming table. Customer 25 then walked over to Customer 24 who was at another location in the Grange Room. Customer 24 then returned to the second gaming table with $20,000 in chips and commenced play. SCA's records showed that Customer 24 had not completed a cash or chip purchase voucher transaction in the interim.

In July 2017, SCA’s AML/CTF Senior Management Group considered that Customer 24 was structuring transactions so as to fall under the reporting threshold, but it did not take any further action.

On 10 August 2017, Customer 24 exchanged $79,805 in chips for cash at SCA in 18 separate transactions. SCA suspected that Customer 24 was attempting to avoid the threshold reporting obligation. Later that day, Customer 24 won a significant amount of cash chips playing baccarat. Customer 24 handed $60,000 in cash chips to Person 14 whom SCA considered to be Customer 24’s

runner. Customer 24 and Person 14 then attended the Grange Room Cashier. Person 14 exchanged the $60,000 in cash chips for cash. Customer 24 exchanged a separate $21,840 in cash chips for cash: SMR dated 11 August 2017.

Large and suspicious cash transactions in 2018

On 15 August 2018, Customer 24 engaged in a series of suspicious cash and chip transactions in concert with Customer 25:

a. On 15 August 2018, Customer 25 deposited $20,000 in cash into their FMA.

b. Customer 24 and Customer 25 then attended the Grange Room Cashier and Customer 25 withdrew a $20,000 chip purchase voucher.

c. Customer 24 and Customer 25 then immediately attended a gaming table and Customer 25 redeemed the voucher for $20,000 in chips.

d. Customer 24 and Customer 25 then exited the Grange Room and Customer 25 handed the $20,000 in chips to Customer 24.

e. Customer 25 then exited the premises and Customer 24 commenced play on the main gaming floor with the chips.

Customer 24 recorded a loss of approximately $68,000 for the day. Customer 25 did not record any gambling activity for the day. SCA considered that Customer 25 attended SCA for the sole reason of conducting a $20,000 transaction on behalf of Customer 24: SMR dated 16 August 2018.

Large and suspicious cash transactions in 2021

On 23 September 2021, Customer 24 presented $1,000,000 in cash in a suitcase and requested that SCA exchange the cash for chips. Due to the substantial amount of cash involved, SCA requested that Customer 24 complete a Source of Funds Declaration to explain and verify where the funds originated from. Customer 24 declared that the cash was comprised of casino winnings from SCA for the month of August 2021. After reviewing this declaration, SCA concluded that Customer 24's recorded gambling activity for August 2021 did not support the substantial amount of cash presented, and therefore declined the transaction: SMR dated 18 October 2021.

On 4 December 2021, Customer 24 withdrew a $200,000 chip purchase voucher from their FMA at SCA. Two days later, Customer 24 exchanged a $200,000 chip purchase voucher for chips at SCA.

h. Customer 24 had access to private gaming rooms at SCA;

Particulars

See paragraph 145(e) above.

Customer 24 had access to private gaming rooms at SCA, including the Grange Room, Platinum Room and Black Room.

i. by 16 July 2020, media reports named Customer 24 as a person involved in criminal conduct;

Particulars

On 16 July 2020, a media report recorded that a criminal matter concerning Customer 24 was listed for hearing at an Australian court.

SCA's due diligence records did not contain details of this report.

j. between 2021 and 2022, Customer 24 was the subject of law enforcement enquiries at SCA;

Particulars

On 4 May 2021, a state government agency requested information in respect of Customer 24.

In October 2021, SCA corresponded with a law enforcement agency regarding Customer 24 and responded to requests for information. In the course of its correspondence, the law enforcement agency advised SCA that law enforcement officers had attended Customer 24's home, seized $1,000,000 in cash and questioned them about a $310,000 cash buy-in on 18 September 2021: SMR dated 18 October 2021.

Between 4 January 2022 and 7 January 2022, the law enforcement agency informed SCA that:

a. its enquiries into Customer 24 had revealed that Customer 24 more than likely did not receive and had never received any salary from the company of which they claimed to be a director and the statements as to their annual salary provided in their Source of Wealth Declarations of February 2021 and July 2021 were false;

b. it was investigating Customer 24 in relation to money laundering; and

c. its officers had seized cash from Customer 24's property: SMR dated 18 February 2022.

k. SCA did not have adequate reason to believe that Customer 24's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 24 by SCA; and

Particulars

See paragraph 516 above.

By 7 December 2016, SCA held concerns that Customer 24's gambling activity was not commensurate with their occupation, source of wealth or source of funds, and that Customer 24's

explanation as to their source of funds was "questionable": see particulars to paragraph 885.a.viii.

By 3 February 2022, SCA considered that Customer 24 had failed to adequately explain their source of wealth, was unable to provide any documentation that supported their standard of living, and had been unwilling to provide information that reflected the source of wealth used to support the level of gambling activity that they engaged in: SMR dated 18 February 2022. SCA issued a ban in respect of Customer 24 on 3 February 2022.

Between 7 December 2016 and 3 February 2022:

a. SCA recorded turnover exceeding $730,000,000 for Customer 24;

b. Customer 24 engaged in at least 28 transactions indicative of structuring with a total value of at least $160,000;

c. SCA was aware that Customer 24 was conducting large cash transactions on behalf of Customer 2, Customer 17 and Customer 25; and

d. SCA was aware that Customer 24 had presented $1,000,000 in cash for which SCA could not entirely account and that was subsequently seized by law enforcement.

At no time was SCA's understanding of Customer 24's source of funds and source of wealth commensurate with the high value financial and gambling services that they received at SCA.

SCA's determination of the ML/TF risks posed by Customer 24

886. On and from 28 May 2016, Customer 24 was appropriately rated by SCA as a high risk customer for the purpose of the Act and Rules.

Particulars

On 6 October 2021, SCA rated Customer 24 as a significant risk customer, which maintained their rating as high risk for the purpose of the Act and Rules.

887. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 24 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by it with respect to Customer 24.

Monitoring of Customer 24's transactions

888. At no time did SCA apply appropriate transaction monitoring to Customer 24's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

On 11 August 2017, SCA gave the AUSTRAC CEO an SMR in which it reported its concern that:

a. Customer 24's transactional behaviour, as both a player in their own right and an assistant performing buy-ins and cash-outs on behalf of Customer 17 and Customer 2, was adding to the winning buy-in and cash-out inflation in the Grange Room; and

b. this made it very difficult to track all the chip and cash exchanges occurring in the Grange Room: SMR dated 11 August 2017.

By October 2021, the AML General Manager was aware that SCA had not performed a transaction analysis in respect of Customer 24's flow of funds so that SCA could understand whether Customer 24's source of wealth was plausible.

b. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 24 through the SCA Customer account channel, which was a high risk remittance channel.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 24's KYC information

889. SCA did not review, update or verify Customer 24's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 24, including the nature, extent and purpose of Customer 24's transactions, having regard to the high ML/TF risks; and

c. SCA did not appropriately review, update or verify Customer 24's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks;

Particulars

By reason of the matters set out in *Customer 24's risk profile* above, there were higher ML/TF risks associated with Customer 24's source of wealth or source of funds.

d. to the extent that SCA reviewed Customer 24's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 24.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

ECDD triggers in respect of Customer 24

890. SCA was required to apply the ECDD program to Customer 24 following any ECDD triggers in respect of Customer 24.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

891. Customer 24 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 20 February 2017 and 18 February 2022, SCA gave the AUSTRAC CEO six SMRs with respect to Customer 24.

b. determined by SCA to be high risk for the purpose of the Act and Rules prior to the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 24* above.

892. Each matter pleaded in paragraph 891 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

893. SCA did not conduct appropriate risk-based ECDD with respect to Customer 24 following an ECDD trigger because:

a. on each occasion prior to late 2021 that SCA conducted ECDD in respect of Customer 24 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 24 and failed to appropriately consider whether the ML/TF risks posed by Customer 24 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501, 511 and 516 to 517 above.

SCA undertook ECDD regarding Customer 24 on a number of occasions, but failed to perform ECDD which was suited to the ML/TF risks presented by Customer 24's behaviour at SCA: see *Customer 24's risk profile* above.

Customer 24's source of wealth and source of funds

At various times during the relevant period, Customer 24 advised SCA that their gambling activity was funded by:

a. family support;

b. their occupation as a personal assistant;

c. their annual salary of $100,000 as the Managing Director of an Australian company;

d. their annual salary of $30,000 as an executive officer of an overseas company;

e. their annual income of over $200,000 from ownership of Australian equity instruments; and

f. their winnings at SCA and other Australian casinos.

Between 2020 and 2021, on multiple occasions, SCA sought information from Customer 24 in respect of their source of wealth and source of funds.

However, by February 2022, SCA had failed to take appropriate steps to verify that Customer 24's claims as to their source of wealth and source of funds were legitimate: see paragraph 885.k above.

SCA failed to identify that the Source of Wealth and Source of Funds Declarations completed by Customer 24 more than likely contained false information until it received a notification to this effect from a law enforcement agency.

In January 2022, SCA received an ECDD report concerning Customer 24 which confirmed that the incomes they claimed to derive from their corporate positions were unverified.

ECDD screenings

Between September 2018 and January 2022, SCA conducted ECDD screenings in respect of Customer 24 on three occasions, but it did not appropriately consider the real risks that Customer 24's declared sources of wealth and sources of funds were not legitimate, nor did it take steps to verify these declared sources of wealth and sources of funds: see *Customer 24's risk profile* above.

Measures adopted in 2021 and 2022

Between 1 January 2021 and 31 August 2021, SCA recorded turnover exceeding $340,000,000 for Customer 24.

In around September 2021, SCA determined that it would not accept further cash transactions from Customer 24 until it received source of wealth documentation, but that Customer 24 could continue to game at SCA, access their FMA and remit funds to SCA.

Between 1 September 2021 and 3 February 2022, SCA recorded turnover exceeding $360,000,000 for Customer 24.

In February 2022, after a law enforcement agency reported to SCA that Customer 24's statutory declarations as to their source of funds contained information that was most likely false, SCA issued a ban in respect of Customer 24: SMR dated 18 February 2022.

The ECDD conducted by SCA did not have appropriate regard to Customer 24's higher ML/TF risks: see *Customer 24's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 24's source of funds or source of wealth.

By reason of the matters set out in *Customer 24's risk profile* above, there were higher ML/TF risks associated with Customer 24]'s source of wealth or source of funds.

b. on any occasion prior to 3 February 2022 that senior management considered the higher ML/TF risks posed by Customer 24 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 24 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

In each of May 2021, July 2021 and September 2021 Customer 24 was named in an internal report titled 'Transaction Monitoring Overview' report, which was provided to the SCA's AML/CTF Senior Management Group for consideration at their meetings. Each of these reports noted that Customer 24's FMA had a very high balance.

Despite the higher ML/TF risks associated with Customer 24's source of wealth and source of funds (see *Customer 24's risk profile* above), senior management failed to consider the higher ML/TF risks posed by Customer 24 until September 2021.

On 24 September 2021, the General Manager granted their approval for SCA to accept $1,000,000 in cash that Customer 24 presented on the basis that Customer 24 complete a Source of Wealth Declaration. This was despite the General Manager acknowledging that they could not see any reason why Customer 24 would have possession of that

much cash, and despite being advised by the AML Compliance Manager that:

a. SCA could not entirely account for Customer 24 being in possession of $1,000,000 in cash from their play records;

b. SCA had no explanation as to why Customer 24 attempted to perform this large cash buy-in without adequate documentation;

c. the AML Compliance Manager was “uncomfortable” with the transaction; and

d. there was no reasonable explanation as to why Customer 24 retained such a large amount of physical currency outside of the casino.

On 1 October 2021, the SCA AML Compliance Manager escalated Customer 24 to the SCEG International Gaming General Manager and the SCEG General Counsel. The AML Compliance Manager noted that Customer 24 represented a significant level of risk to SCA’s business and highlighted that:

a. Customer 24 was attempting to use $1,000,000 in cash for gaming;

b. Customer 24 had recorded turnover of over $780,000,000 since 11 April 2016;

c. Customer 24 was the subject of a warrant served on SCA by a law enforcement agency;

d. Customer 24 was the subject of six SMRs; and

e. SCA suspected that Customer 24 had previously acted as a runner for other SCA customers to structure their transactions to avoid reporting requirements.

The International Gaming General Manager and the General Counsel granted their approval for SCA to continue its business relationship with Customer 24, noting that:

a. the law enforcement agency did not hold any position in relation to whether SCA should continue its business relationship with Customer 24;

b. SCEG was not aware of any adverse information in respect of Customer 24; and

c. SCA had no reason to suggest Customer 24 had done anything to warrant a banning order and it should trust the AML/CTF information collated to that point.

The International Gaming General Manager and the General Counsel also noted that SCA should seek further information from the law enforcement agency.

On 4 October 2021, after SCA received a request from a law enforcement agency for information in respect of Customer 24, the SCEG International Gaming General Manager, the SCEG General Counsel, and the SCA Chief Operating Officer determined that SCA should still continue its business relationship with Customer 24 on the basis that the law enforcement agency's investigation was only preliminary in nature, but noted that SCA should not accept further large cash deposits from Customer 24.

However, throughout October 2021, SCA's AML team recorded that they were not aware of the nature of the law enforcement agency's interest in Customer 24 or the agency's specific concerns.

On 6 October 2021, after SCA became aware that a law enforcement agency had seized $1,000,000 in cash from Customer 24's home, the SCA AML Compliance Manager advised the SCEG International Gaming General Manager that the law enforcement agency had requested further information in respect of Customer 24. The SCEG International Gaming General Manager determined that SCA should continue with its current position in relation to Customer 24 until it received further information.

It was not until 3 February 2022 that SCA issued a ban in respect of Customer 24, after a law enforcement agency advised that Customer 24's statutory declarations as to their source of wealth and source of funds more than likely contained false information.

Contravention of s 36 of the Act in respect of Customer 24

894. By reason of the matters pleaded from paragraphs 882 to 893 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 24 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

895. By reason of the matters pleaded at paragraph 894, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 3 February 2022 with respect to Customer 24.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 25

896. Customer 25 was a customer of SCA during the relevant period. Between March 2017 and March 2020, SCA recorded turnover exceeding $1,900,000 for Customer 25.

Particulars

Customer 25 was a customer of SCA from at least 12 March 2017.

On 29 March 2022, SCA issued a ban in respect of Customer 25 at the direction of the SCA AML team.

897. SCA provided Customer 25 with designated services within the meaning of table 1 and table 3, s 6 of the Act during the relevant period.

Particulars

On 12 March 2017, SCA opened an FMA for Customer 25 which was closed on 22 March 2022 (item 11, table 3, s 6 of the Act).

While a customer of SCA, Customer 25 remitted funds to and from their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 25's risk profile* below.

898. At all times from 12 March 2017, SCA was required to conduct ongoing customer due diligence in respect of Customer 25.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 25's risk profile

899. On and from 12 March 2017, Customer 25, and the provision of designated services to Customer 25 by SCA, posed higher ML/TF risks because of the following red flags:

a. Customer 25 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs. Between 13 March 2017 and 26 December 2020, SCA recorded an estimated buy-in of $670,700, a high turnover estimated at $1,917,107 for Customer 25, with cumulative losses of $40,038;

Particulars

In 2017, Customer 25's recorded individual rated gambling activity at SCA was estimated as a buy-in of $637,200 for table games, and for both table games and EGMs turnover of $1,833,923 with losses of $40,038.

In 2018, Customer 25's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $20,000.

In 2020, despite closures related to the COVID-19 pandemic, Customer 25's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $13,500, turnover of $83,183 and no recorded wins or losses.

b. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 25 by remitting large amounts of money into the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

Between 20 April 2017 and 14 August 2018, SCA received 15 telegraphic transfers totalling $223,010 from unknown accounts, each of which was made available to Customer 25's FMA.

c. SCA was aware that:

   i. Customer 25 had engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose; and

   ii. Customer 25 was connected to other customers at SCA, including players who posed higher ML/TF risks such as Customer 24 and players who SCA considered had acted suspiciously.

Particulars

From mid-2017, SCA identified that Customer 25 was associated with Customer 24 and had engaged in a number of suspicious transactions involving Customer 24 or which appeared to be conducted on Customer 24's behalf:

   a. on 28 July 2017, Person 14 made a buy-in for $10,000 in chips at a gaming table and then moved to a second gaming table with Customer 25 and Customer 24. Person 14 and Customer 25 passed the $10,000 in chips to Customer 24, who played and lost the money. Shortly after, Customer 25 exchanged $20,000 for a chip purchase voucher and was seen with Customer 24. Customer 24 then went to a gaming table with $20,000 in chips;

   b. on 11 August 2017, SCA identified that Customer 25 was a runner for Customer 24 and performed buy-ins and cash outs on Customer 24's behalf; and

   c. on 15 August 2018, Customer 25 deposited $20,000 in cash into their FMA and then redeemed this for $20,000 in chips. Without undertaking any gaming, Customer 25 handed $20,000 worth of chips to Customer 24 and then the premises. SCA noted that this was Customer 25's first visit to SCA in 2018 and that it appeared that the sole reason for their visit was to conduct the transaction on Customer 24's behalf: SMR dated 16 August 2018.

d. designated services provided to Customer 25 included EGM activity at SCA;

Particulars

See paragraphs 352 and 353 above.

In 2017, Customer 25's recorded individual rated gambling activity at SCA was estimated as a turnover of $7,174 for EGMs.

e. Customer 25 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

Between 24 April 2017 and 15 August 2018, SCA gave the AUSTRAC CEO 14 TTRs detailing transactions made by Customer 25 totalling $235,000, which comprised:

a. two TTRs totalling $21,000 in chip and token transactions; and

b. 12 TTRs totalling $214,000 in account deposits.

f. Customer 25 had access to a private gaming room at SCA; and

Particulars

See paragraph 145(e) above.

Customer 25 had access to the Platinum Room.

g. SCA did not have adequate reason to believe that Customer 25's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 25 by SCA.

Particulars

See paragraph 516 above.

From at least 12 March 2017, SCA recorded Customer 25's occupation as a student.

On 6 October 2021, SCA recorded that it needed to update the information it held regarding Customer 25's occupation.

At no time did SCA request source of funds or source of wealth information from Customer 25.

At no time was SCA's understanding of Customer 25's source of wealth and source of funds commensurate with their high value gambling activity.

Between 13 March 2017 and 26 December 2020, Customer 25's recorded estimated buy-in was over $670,000.

SCA's determination of the ML/TF risks posed by Customer 25

900. On and from 11 August 2017, Customer 25 was appropriately rated by SCA as a high risk customer for the purpose of the Act and Rules.

Particulars

On 25 March 2022, SCA rated Customer 25 significant risk, which remained high risk for the purpose of the Act and Rules.

901. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 25 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by it with respect to Customer 25.

Monitoring of Customer 25's transactions

902. At no time did SCA apply appropriate transaction monitoring to Customer 25's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 25 through the SCA Customer account channel, which was a high risk remittance channel.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 25's KYC information

903. SCA did not review, update or verify Customer 25's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 25, including the nature, extent and purpose of Customer 25's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update or verify Customer 25's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 25's risk profile* above, there were higher ML/TF risks associated with Customer 25's source of wealth or source of funds.

In 2017, Customer 25's recorded estimated but in was $637,200. Customer 25's buy-in was not proportionate to their recorded occupation as a student. Nevertheless, SCA did not review, verify or update Customer 25's source of wealth or source of funds.

d. to the extent that SCA reviewed Customer 25's KYC information on and from 12 March 2017, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 25.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

ECDD triggers in respect of Customer 25

904. SCA was required to apply the ECDD program to Customer 25 following any ECDD triggers in respect of Customer 25.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

905. Customer 25 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 11 August 2017 and 16 August 2018, SCA gave the AUSTRAC CEO two SMRs pertaining to Customer 25.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 25* above.

906. Each matter pleaded in paragraph 905 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

907. SCA did not conduct appropriate risk-based ECDD with respect to Customer 25 following an ECDD trigger because:

a. on each occasion prior to 29 March 2022 that SCA conducted ECDD in respect of Customer 25 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 25 and failed to appropriately consider whether the ML/TF risks posed by Customer 25 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501, 511 and 516 to 517 above.

In July 2017, SCA identified that Customer 25 and Person 14 acted as runners for Customer 24 and performed buy-ins on behalf of Customer 24.

On 12 September 2019, SCA prepared an ECDD Report in respect of Customer 25. The report identified that:

a. Customer 25 was a student and SCA did not have any information regarding Customer 25's source of wealth or source of funds;

b. Customer 25's known associates included Customer 24, and Customer 24 appeared to be using Customer 25 to conduct transactions in order for Customer 24 to distance themselves from those transactions; and

c. on at least one occasion, including their first visit to SCA, Customer 25 appeared to attend SCA for the sole purpose of conducting transactions on behalf of Customer 24.

The ECDD conducted by SCA did not have appropriate regard to Customer 25's higher ML/TF risks: see *Customer 25's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 25's source of funds or source of wealth.

By reason of the matters set out in *Customer 25's risk profile* above, there were higher ML/TF risks associated with Customer 25's source of wealth or source of funds.

It was not until 29 March 2022 that SCA issued a ban in respect of Customer 25.

b. on any occasion prior to 29 March 2022 that senior management considered the higher ML/TF risks posed by Customer 25 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 25 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

It was not until 25 March 2022, after elevating Customer 25's risk rating to significant, that an AML Compliance Analyst escalated Customer 25 to the Chief Operating Officer and requested that they determine whether SCA should continue a business relationship with Customer 25.

On 27 March 2022, the Chief Operating Officer determined that SCA should discontinue its business relationship with Customer 25.

On 29 March 2022, SCA issued a ban in respect of Customer 25.

Contravention of s 36 of the Act in respect of Customer 25

908. By reason of the matters pleaded from paragraphs 896 to 907 above, on and from 12 March 2017, SCA:

a. did not monitor Customer 25 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

909. By reason of the matters pleaded at paragraph 908, SCA contravened s 36(1) of the Act on and from 12 March 2017 to 29 March 2022 with respect to Customer 25.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 26

910. Customer 26 was a customer of SCA during the relevant period. Between 10 December 2016 and August 2021, SCA recorded turnover exceeding $83,000,000 for Customer 26.

Particulars

Customer 26 was a customer of SCA from at least 1999.

On 10 September 2021, SCA issued a ban in respect of Customer 26.

911. SCA provided Customer 26 with designated services within the meaning of table 1 and table 3, s 6 of the Act during the relevant period.

Particulars

On 27 October 1999, SCA opened an FMA for Customer 26 which was closed on 10 September 2021 (item 11, table 3, s 6 of the Act).

While a customer of SCA, Customer 26 remitted funds to and from their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 26's risk profile* below.

912. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 26.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 26's risk profile

913. On and from 7 December 2016, Customer 26, and the provision of designated services to Customer 26 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 26's risk profile prior to the relevant period

a. by 7 December 2016, Customer 26 had the following risk history:

i. Customer 26 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs;

Particulars

Between 1999 and 2009, Customer 26's recorded individual rated gambling activity at SCA was an estimated buy-in of $6,100 for table games, and for both table games and EGMs, turnover of $9,457,894 with losses of $712,945.

In 2010, Customer 26's recorded individual rated gambling activity at SCA for EGMs was an estimated turnover of $2,318 with losses of $753.

In 2011, Customer 26's recorded individual rated gambling activity at SCA for EGMs was an estimated turnover of $9,859 with losses of $1,232.

In 2012, Customer 26's recorded individual rated gambling activity at SCA for EGMs significantly escalated to an estimated turnover of $2,291,527 with losses of $58,801.

In 2013, Customer 26's recorded individual rated gambling activity at SCA for EGMs further escalated to an estimated turnover of $4,861,568 with losses of $374,962.

In 2014, Customer 26's recorded individual rated gambling activity at SCA for EGMs was an estimated turnover of $6,485,912 with losses of $305,564.

In 2015, Customer 26's recorded individual rated gambling activity at SCA for EGMs escalated to an estimated turnover of $10,756,568 with losses of $538,644.

ii. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 26 by remitting large amounts of money into, out of and within the casino environment via their accounts, including through high risk remittance channels; and

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

SCA made money available to Customer 26 in the following transactions:

a. Between 7 July 2016 and 20 October 2016, Customer 26 received $45,000 into their SCA FMA via telegraphic transfer in 11 separate transactions.

SCA accepted instructions to transfer funds from Customer 26's accounts for the following transactions:

a. On 8 December 2015, Customer 26 transferred $25,000 from their SCA FMA to their personal bank account.

b. On 2 January 2016, Customer 26 transferred $25,031 from their SCA FMA to their personal bank account.

iii. Customer 26 transacted using large amounts of cash at SCA.

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 17 October 2008 and 29 June 2016, SCA gave the AUSTRAC CEO 52 TTRs detailing outgoing payments made by Customer 26 totalling $893,955, which comprised:

a. six TTRs totalling $76,108 in chip and cash exchanges;

b. six TTRs totalling $115,093 in account withdrawals; and

c. 40 TTRs totalling $702,754 in EGM payouts.

Large cash transactions

SCA recorded that Customer 26 made significant cash outs at SCA. For example:

a. on 20 December 2014, Customer 26 cashed out $21,803. Customer 26 took $21,500 in cash and $303 as a TITO ticket;

b. on 12 January 2015, Customer 26 cashed out $18,391. Customer 26 took $8,000 in cash and deposited the remaining $10,391 into their FMA;

c. on 10 April 2015, Customer 26 cashed out $18,781 following an EGM win. Customer 26 took $18,000 in cash and $781 as a TITO ticket; and

d. on 14 April 2016, Customer 26 cashed out a $22,509 TITO ticket for cash.

Customer 26's risk profile during the relevant period

b. Customer 26 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs. Between 10 December 2016 and 2021, SCA recorded a high turnover estimated at $83,615,494 for Customer 26, with cumulative losses of $5,168,128;

Particulars

In 2016, Customer 26's recorded individual rated gambling activity at SCA for EGMs was an estimated turnover of $6,594,064 with losses of $432,304.

In 2017, Customer 26's recorded individual rated gambling activity at SCA for EGMs escalated to an estimated turnover of $8,161,929 with losses of $571,917.

In 2018, Customer 26's recorded individual rated gambling activity at SCA for EGMs escalated to an estimated turnover of $12,384,487 with losses of $900,415.

In 2019, Customer 26's recorded individual rated gambling activity at SCA for EGMs further escalated to an estimated turnover of $26,480,498 with losses of $1,383,646.

In 2020, despite closures related to the COVID-19 pandemic, Customer 26's recorded individual rated gambling activity at SCA for EGMs remained high, with an estimated turnover of $19,926,213 with losses of $1,222,374.

In 2021, Customer 26's recorded individual rated gambling activity at SCA for EGMs was an estimated turnover of $16,176,399 with losses of $1,027,270.

Between 11 August 2020 and 1 August 2021, Customer 26 appeared on SCA transaction reports that identified them as a significant player on EGMs on at least 139 occasions.

c. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 26 by remitting large amounts of money into and out of the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

In a report dated August 2020, Bank 1 identified Customer 26 as one of the top third party depositors into SCA's bank account during the period 1 September 2018 to 31 August 2019.

In a report dated October 2021, Bank 1 stated that, between 1 September 2019 and 31 May 2021, Customer 26 was the top depositor by volume into SCA's bank account. Bank 1 identified that during this period, Customer 26 made at least 251 deposits totalling $947,500. Bank 1 also considered that the series of transactions by Customer 26 were suspicious and could be indicative of structuring, as often there were multiple transactions made on the same day with each individual transaction being for a relatively low value.

On or around 2 November 2021, after Customer 26 had been banned, SCA completed a review of all bank transactions between 4 September 2019 and 5 October 2021. The results of the review were

sent to an SCA AML Compliance Manager and an SCA AML Analyst. The review identified that Customer 26 had received $1,046,500 into their SCA FMA over 278 transactions during the review period, and stated that the transactions were indicative of structuring.

SCA made money available to Customer 26 in the following transactions:

a. Between 12 December 2016 and 23 August 2021, Customer 26 received at least $1,707,200 into their SCA FMA via telegraphic transfer in 526 separate transactions. On several occasions, Customer 26 received multiple transfers in one day. Some of these transfers were from Customer 26's personal bank account in Australia.

SCA accepted instructions to transfer funds from Customer 26's accounts for the following transactions:

a. Between 15 March 2017 and 2 June 2021, Customer 26 transferred a total of $1,109,858 in 42 separate transactions from their SCA FMA to their personal bank account in Australia.

d. Customer 26 had engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

Particulars

Between 29 August 2019 and 10 August 2021, Customer 26 was included in an internal daily report titled 'Cashless Out over $5k' 130 times. These reports identified cashless transactions equal to or above $5,000, including those that were conducted via a cashless card. The reports were reviewed by the SCA AML team, and showed that Customer 26 often performed multiple transfers from EGMs in one day. For example:

a. on 12 November 2019, Customer 26 made five 'cashless out' transfers totalling $36,594 and ranging between $6,170 and $9,110;

b. on 29 November 2020, Customer 26 made nine 'cashless out' transfers totalling $63,562 and ranging between $5,290 and $9,466; and

c. on 29 May 2021, Customer 26 made 13 'cashless out' transfers totalling $84,529 and ranging between $5,080 and $8,180.

e. designated services provided to Customer 26 included substantial EGM activity at SCA;

Particulars

See paragraphs 352 and 353 above.

See particulars to paragraph 913.b above.

Customer 26 received benefits from SCA due to their substantial EGM activity, including bonuses based on their EGM turnover. Customer 26 received a bonus each time they recorded $1,000,000 EGM turnover in a calendar month (monthly target), and a bonus every time Customer 26 recorded $125,000 EGM turnover (rolling target).

For example, between 1 May 2019 and 30 April 2020, Customer 26 received a $448,000 bonus based on their rolling target and a $92,000 bonus based on their monthly target.

f. Customer 26 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 15 March 2017 and 16 August 2021, SCA gave the AUSTRAC CEO 124 TTRs detailing incoming and outgoing payments made by Customer 26 totalling $2,132,182, which comprised:

a. five TTRs totalling $72,200 in account deposits;

b. 47 TTRs totalling $1,137,265 in account withdrawals; and

c. 72 TTRs totalling $992,717 in EGM payouts.

Large cash transactions

SCA recorded that Customer 26 made significant buy-ins or cash outs at SCA. For example:

a. on 20 August 2017, Customer 26 cashed out a $12,410 TITO ticket for cash;

b. on 3 September 2018, Customer 26 cashed out $10,450 following a jackpot win. Customer 26 took $10,000 in cash and a $450 TITO ticket;

c. on 2 November 2019, Customer 26 cashed out $10,833 following an EGM win. Customer 26 took $10,800 in cash and deposited $33 into their FMA;

d. on 3 September 2020, Customer 26 withdrew $20,000 in cash from their FMA;

e. on 5 January 2021, Customer 26 cashed out $12,191 following an EGM win. Customer 26 took $12,000 in cash and deposited $191.28 into their FMA; and

f. on 16 April 2021, Customer 26 deposited $10,200 in cash into their FMA.

g. Customer 26 had access to private gaming rooms at SCA; and

Particulars

See paragraph 145(e) above.

Customer 26 had access to private gaming rooms at SCA, including the Black Room and the Platinum Room.

h. SCA did not have adequate reason to believe that Customer 26's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 26 by SCA.

Particulars

See paragraph 516 above.

By 7 December 2016, SCA understood that Customer 26's occupation was as an IT business owner. On 20 March 2017, Customer 26 informed SCA that they worked at a communications company.

SCA did not request source of wealth information from Customer 26 until 10 September 2021. By this time, Customer 26 had an estimated recorded turnover exceeding $83,000,000. Since 2019, Customer 26 had sustained losses of more than $1,000,000 per year. Also on 10 September 2021, SCA banned Customer 26 from the casino until they provided appropriate source of wealth information.

Customer 26 declined to provide any source of wealth information.

At no time did SCA request source of funds information from Customer 26.

At no time was SCA's understanding of Customer 26's source of wealth or source of funds commensurate with the high value financial and gambling services that they received at SCA.

SCA's determination of the ML/TF risks posed by Customer 26

914. SCA was unable to appropriately identify or assess the ML/TF risks posed by Customer 26 because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 26.

a. On and from early 2017, Customer 26 should have been recognised by SCA as a high risk customer for the purpose of the Act and Rules for the reasons pleaded above: see *Customer 26's risk profile* above.

Particulars

Sections 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

b. It was not until 20 June 2022 that Customer 26 was rated high risk by SCA for the purpose of the Act and Rules.

Particulars

Customer 26 was not rated as high risk at SCA until 20 June 2022, which was nearly one year after SCA issued a ban in respect of Customer 26.

Monitoring of Customer 26's transactions

915. At no time did SCA apply appropriate transaction monitoring to Customer 26's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities; and

Particulars

Sections 36(1)(a) and (b) of the Act.

See paragraphs 437 to 441 above.

b. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 26 through the SCA Customer account channel, which was a high risk remittance channel.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 26's KYC information

916. SCA did not review, update or verify Customer 26's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 26, including the nature, extent and purpose of Customer 26's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 26's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 26's risk profile* above, there were higher ML/TF risks associated with Customer 26's source of wealth or source of funds.

d. to the extent that SCA reviewed Customer 26's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 26.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

Reviews

Between June 2018 and September 2019, SCA conducted monthly risk monitoring system reviews of Customer 26's visits and play on seven occasions.

On 19 January 2021, SCA conducted a surveillance review of Customer 26's transactions. An SCA AML Advisor was advised of the findings.

Alerts

Between 17 March 2017 and 6 July 2021, there were 26 alerts with respect to Customer 26.

Due diligence screening

On or around 3 September 2021, SCA conducted ongoing customer due diligence screening in respect of Customer 26. The screening noted that Customer 26 worked for a communications company, but that their position in the company and their ownership of the company was not known.

Following the screening, SCA recommended that a completed Source of Wealth Declaration be obtained from Customer 26.

Other due diligence

On 8 September 2021, SCA conducted a review of its customer relationships and determined that it should discontinue its relationship with Customer 26.

On 10 September 2021, SCA issued a ban in respect of Customer 26.

Failure to apply appropriate due diligence suited to the high ML/TF risks

917. Had SCA conducted ongoing customer due diligence on and from 7 December 2016 by:

a. appropriately identifying and assessing the ML/TF risks posed by Customer 26;

b. applying appropriate risk-based transaction monitoring to Customer 26; and

c. appropriately reviewing and updating Customer 26's KYC information, having regard to the high ML/TF risks,

SCA would likely have rated Customer 26 as a high risk customer for the purpose of the Act and Rules at a time before 10 September 2021, when Customer 26 was issued a ban by SCA.

Particulars

Section 36(1)(a) of the Act, r 15.2 and 15.5 of the Rules.

918. Had SCA rated Customer 26 as a high risk customer at a time before 10 September 2021, it would have been required by the Act and the Rules to conduct ECDD in relation to Customer 26 at a time before 10 September 2021, when Customer 26 was issued a ban by SCA.

Particulars

Rule 15.9 of the Rules.

Contravention of s 36 of the Act in respect of Customer 26

919. By reason of the matters pleaded from paragraphs 910 to 917 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 26 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2 and 15.5 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

920. By reason of the matters pleaded at paragraph 919, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 10 September 2021 with respect to Customer 26.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 27

921. Customer 27 was a customer of SCA during the relevant period. Between 7 December 2016 and 30 July 2021, SCA recorded turnover exceeding $51,000,000 for Customer 27.

Particulars

Customer 27 was a customer of SCA from at least 22 April 1994.

On 29 July 2021, SCA issued a ban in respect of Customer 27.

922. SCA provided Customer 27 with designated services within the meaning of table 3, s 6 of the Act during the relevant period.

Particulars

On or before 22 April 1994, SCA opened an FMA for Customer 27 which remained open as at 28 October 2022 (item 11, table 3, s 6 of the Act).

See *Customer 27's risk profile* below.

923. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 27.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 27's risk profile

924. On and from 7 December 2016, Customer 27, and the provision of designated services to Customer 27 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 27's risk profile prior to the relevant period

a. by 7 December 2016, Customer 27 had the following risk history:

i. SCA had formed suspicions for the purposes of s 41 of the Act with respect to Customer 27;

Particulars

SCA gave the AUSTRAC CEO an SMR on eight occasions between 24 June 1998 and 11 September 2015.

The SMRs reported that Customer 27 conducted transactions at SCA indicative of the ML/TF typologies of structuring and cashing out without evidence of play. For example:

a. on 6 July 2015, Customer 27 cashed out $6,000 at one Cashier and immediately cashed out $8,000 at another Cashier: SMR dated 7 July 2015; and

b. on 10 September 2015, Customer 27 cashed out $8,150 and an associate cashed out $9,300 immediately after Customer 27. Customer 27 then cashed out a further $1,300 within a few minutes. There was no play between the transactions and Customer 27 only had recorded wins of around $3,000 for the day. SCA suspected this behaviour was linked to illegal money lending: SMR dated 11 September 2015.

ii. SCA was aware that Customer 27 frequently engaged in disorderly behaviour at SCA;

Particulars

Between 12 October 2013 and 7 August 2014, Customer 27 engaged in disorderly behaviour on at least three occasions, including swearing at SCA employees and swearing at and threatening to kill other SCA customers, resulting in Customer 27 being asked to leave the premises for their disorderly behaviour and being banned for 24 hours.

iii. Customer 27 received high value gambling services (table 3, s 6 of the Act) at SCA other than through junket programs or individual commission programs;

Particulars

In 2015, Customer 27's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $1,668,600, turnover of $6,822,53 and with losses of $125,950.

iv. by 4 August 2007, SCA was aware that Customer 27 was lending money to other SCA customers;

Particulars

On 4 August 2007, SCA questioned Customer 27 in relation to lending money to another SCA customer which Customer 27 confirmed they had done. Customer 27 was advised that because they had previously been formally cautioned for money lending (on 2 January 2007) that they would be banned from the premises under common law pending a formal ban which would be sought by SCA.

On 11 November 2007, Customer 27 was found to be on the SCA premises following the expiry of their ban on 4 November 2007.

v. Customer 27 had engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose, including transactions indicative of loan sharking; and

Particulars

See paragraph 24 above.

Customer 27 engaged in transactions and behaviour which was indicative of loan sharking.

For example, on 19 November 2016, SCA staff observed Customer 27 lending money to Customer 38 at a gaming table. Customer 27 encouraged Customer 38 to borrow more than Customer 38 appeared willing to borrow.

On 18 November 2016, an SCA AML adviser and SCA's VIP Table Games Executive Host considered Customer 27's potential source of wealth and source of funds, as well as Customer 27's behaviour, particularly relating to the potential bags of cash they had brought onto the premises and their potential lending on SCA premises and in front of SCA staff.

vi. Customer 27 transacted using large amounts of cash at SCA.

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 18 November 2012 and 17 June 2016, SCA gave the AUSTRAC CEO four TTRs detailing incoming and outgoing payments made by Customer 27 totalling $93,500, which comprised:

a. three TTRs totalling $68,500 in chip and cash exchanges; and

b. one TTR totalling $25,000 for an account deposit.

Customer 27's risk profile during the relevant period

b. Customer 27 received high value gambling services (table 3, s 6 of the Act) at SCA other than through junket programs. Between 7 December 2016 and 29 July 2021, SCA recorded an estimated buy-in of $15,589,380, a turnover estimated at $51,763,374, with cumulative losses of $1,492,705;

Particulars

In 2016, Customer 27's recorded individual rated gambling activity at SCA for table games escalated to an estimated buy-in of $3,363,500, turnover of $10,319,971 with losses of $215,800.

In 2017, Customer 27's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $3,336,700 for table games, turnover of $13,601,018 with wins of $271,600.

In 2018, Customer 27's recorded individual rated gambling activity at SCA for table games escalated to an estimated buy-in of $4,858,100, turnover of $14,453,358 with losses of $882,300.

In 2019, Customer 27's recorded individual rated gambling activity at SCA was estimated as a buy-in of $2,922,955 for table games, and for both table games and EGMs, turnover of $9,073,592 with losses of $214,555.

In 2020, Customer 27's recorded individual rated gambling activity at SCA was estimated as a buy-in of $2,372,000 for table games, and for both table games and EGMs, turnover of $8,675,377 with losses of $430,060.

In 2021, Customer 27's recorded individual rated gambling activity at SCA was estimated as a buy-in of $1,849,825 for table games, and for both table games and EGMs, turnover of $5,404,153 with losses of $234,986.

c. SCA was aware that Customer 27 had engaged in:

i. large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

ii. transactions involving using large amounts of cash and cash that appeared suspicious, including cash carried in plastic bags; and

iii. transactions indicative of ML/TF typologies and vulnerabilities, including structuring and loan sharking.

Particulars

See paragraphs 24, and 376 to 381 above.

From at least 21 April 2017, SCA was aware that Customer 27 was associated with a number of customers, including Customer 2, that

conducted transactions involving the receipt and movement of significant amounts of cash with no apparent economic or visible purpose and were related to loan sharking activities.

Large and suspicious transactions

On 23 December 2016, over the course of around an hour, Customer 21 handed Customer 27 gaming chips on eight separate occasions. The value of the gaming chips given to Customer 27 totalled around $101,000.

On 21 April 2017, SCA staff observed several instances where chips were passed between Customer 27 and other SCA customers sitting beside Customer 27.

On 1 May 2017, Customer 27 appeared to hand several casino chips to Customer 2, who then attended the Platinum Cashier and presented three $5,000 chips and one $1,000 chip.

On 20 June 2017, Customer 27 held chips which greatly exceeded the value of their wins as recorded by SCA in Bally for the day. The SCA Compliance team noted that Customer 27 had a number of associates that conducted buy-ins on Customer 27's behalf.

In March 2018, SCA staff twice observed Customer 27 passing chips to other SCA customers, including Customer 2, which were then passed to Customer 15, who then cashed out the chips on behalf of Customer 11.

On 21 May 2018, SCA staff observed Customer 27 speaking to Person 5, who then deviated from their normal practices in relation to the method they used to withdraw money at the SCA Cashiers' desk. Person 5 passed the funds they had withdrawn to Customer 27 a short time later.

On 24 May 2018, SCA's CCTV captured Customer 27 passing $54,000 in gaming chips to Person 2, and, a short time later, receiving $100,000 cash from Customer 2.

TTRs and cash that appeared suspicious

Between 17 July 2017 and 23 March 2020, SCA gave the AUSTRAC CEO three TTRs detailing incoming and outgoing payments made by Customer 27 totalling $54,000, which comprised:

a. two TTRs totalling $27,000 in chip and cash exchanges; and

b. one TTR totalling $27,000 for an account deposit.

On 21 December 2016, Customer 27 entered the SCA premises carrying a bag which appeared to contain at least $10,000 in cash.

Loan sharking behaviour

Customer 27 engaged in transactions which were indicative of the ML/TF typology of loan sharking. For example:

a. On 20 December 2016, Customer 27 entered SCA carrying a brown plastic bag which they left at the VIP desk. They subsequently retrieved the bag and removed what appeared to be $10,000 in cash, which they gave to another SCA customer who used the money to buy-in to a baccarat game. Customer 27's level of play for the day was minor: SMR dated 21 December 2016.

b. On 22 December 2016, Customer 27 received with $100,000 worth of chips from Customer 21: SMR dated 23 December 2016.

c. On 19 April 2017, Customer 2 was suspected to have borrowed money from Customer 27, experienced a win and repaid their debt. Customer 27, via Customer 21, was suspected to have repaid Person 18 with the money Customer 27 received from Customer 2. The three customers went to some lengths to disguise the exchanges: SMR dated 21 April 2017.

d. On 30 June 2017, Customer 21 deposited $180,000 into their FMA. They received two $90,000 CPVs which they redeemed separately at two different blackjack tables. Once in possession of the chips they covertly passed the chips to Customer 27 under the table and used Customer 12 to place chips in Customer 27's vest pocket: SMR dated 3 July 2017.

e. On 28 September 2017, Customer 27 attempted to persuade an SCA customer to cash out $50,000 on Customer 27's behalf: SMR dated 4 October 2017.

f. On 18 May 2018, Customer 27 gave Customer 2 a combination of cash and chips totalling $100,000. Customer 2 used the chips to fund additional buy-ins to a program they had commenced. Customer 2 experienced a significant win with this buy-in. Customer 27 then appeared to end Customer 2's game and escorted Customer 2 to the Grange Cashier where Customer 2 cashed out $114,500 of the $249,500 win. Customer 2 and Customer 27 left the premises together in Customer 2's vehicle. SCA suspected that Customer 2 gave Customer 27 $14,500 off site as interest on the $100,000 loaned.

g. On 21 May 2018, Customer 27 used another customer to conduct a $20,000 threshold buy-in on Customer 27's behalf: SMR dated 23 May 2018.

h. On 15 June 2018, Customer 28 exchanged chips for cash before immediately producing $10,000 in cash that they wanted exchanged for chips. They then walked away and passed the $10,000 in chips to Customer 27. The customers shared the same residential address: SMR dated 20 June 2018.

i. On 29 June 2018, Person 5 placed a $50,000 bet that won approximately $47,500. Person 5 gave Customer 27 the winnings: SMR dated 20 July 2018.

j. On 12 July 2018, Person 5 lost approximately $675,000 playing baccarat, which came from winnings from prior SCA trips. Once these funds were exhausted Person 5 turned to Customer 27 and Customer 28 who produced funds that Person 5 used to play. Frontline staff observed that Person 5 produced two plastic bags of cash totalling $101,300 to the Grange Cashier which surveillance confirmed was from Customer 27: SMR dated 13 July 2018.

k. On 17 July 2018, Person 5 presented a $300,000 bank cheque to Cage staff and asked for it to be deposited into their FMA. While awaiting the clearance of the cheque, Customer 27 pestered staff in relation to how long it was taking to clear. When it cleared, Person 5 was issued with a $250,000 CPV which they redeemed at a nearby table and received $250,000 in cash chips. They then separated two amounts from their stack and gave $100,000 to Customer 27 at the baccarat table: SMR dated 17 July 2018.

l. On 2 October 2018, Customer 27 and Customer 2 approached an SCA Cashier with $80,000 in cash chips. Customer 27 asked for the chips to be exchanged for non-negotiable chips, as Customer 2 was playing on a program. SCA recorded that it was obvious that Customer 27 was lending money to Customer 2.

m. On 14 February 2019, Customer 27 approached Customer 2 and placed a black shoulder bag on the table beside Customer 2. Customer 2 passed $50,000 in cash chips to Customer 27, who placed the chips into the bag. Customer 2 took possession of the bag and went to the Platinum Cage, removed $50,000 in cash and deposited it into their FMA. Customer 27 joined Customer 2 at the Platinum Cage and reclaimed possession of the bag.

n. On 18 July 2021, Customer 27 used Customer 40 to conduct a chip colour change and chip purchase on their behalf to avoid being detected: SMR dated 11 August 2021.

d. Customer 27 was connected to other customers at SCA, including players who posed higher ML/TF risks and players who SCA considered had acted suspiciously such as Customer 2, Customer 15, Customer 17, Customer 21, Customer 28, Customer 31, Customer 38, and Customer 40;

Particulars

SCA recorded each of these customers as known associates of Customer 27 in its iTrak system.

e. Customer 27 had access to private gaming rooms at SCA;

Particulars

See paragraph 145(e) above.

Customer 27 had access to private gaming rooms at SCA, including the Platinum Room and the Grange Room.

f. SCA was aware that Customer 27 frequently engaged in disorderly behaviour at SCA;

Particulars

In December 2016, SCA recorded in Customer 27's iTrak profile that they were "an intimidating player".

SCA was aware that Customer 27 frequently engaged in aggressive behaviour towards SCA staff in the relevant period:

a. On 22 January 2019, an SCA contractor complained of harassment by Customer 27.

b. On 11 December 2020, an SCA employee made a complaint against Customer 27 for verbally assaulting them.

c. On 15 February 2021, Customer 27 was allegedly involved in further verbal abuse of staff.

g. SCA did not have adequate reason to believe that Customer 27's source of wealth or source of funds was sufficient to explain the high value gambling services (table 3, s 6 of the Act) provided to Customer 27 by SCA.

Particulars

See paragraph 516 above.

In November 2016 and again in July 2018, SCA recorded that Customer 27 was retired.

In December 2016 and in July 2018, SCA noted in Customer 27's iTrak profile that they were "very secretive" about their source of funds.

SCA was aware that Customer 27 frequently conducted transactions involving the receipt and movement of significant amounts of cash, and often in connection with suspected loan sharking activities

SCA did not request any information regarding Customer 27's source of funds. On 12 August 2021 SCA requested source of wealth information from Customer 27 and Customer 27 declined to provide it.

At no time was SCA's understanding of Customer 27's source of wealth or source of funds commensurate with the extremely high value financial and gambling services that they received at SCA.

SCA's determination of the ML/TF risks posed by Customer 27

925. On and from 6 July 2015, Customer 27 was appropriately rated by SCA as a high risk customer for the purpose of the Act and Rules.

926. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 27 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by it with respect to Customer 27.

Monitoring of Customer 27's transactions

927. At no time did SCA apply appropriate transaction monitoring to Customer 27's transactions because SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

The review, update and verification of Customer 27's KYC information

928. SCA did not review, update or verify Customer 27's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 27, including the nature, extent and purpose of Customer 27's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 27's source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 27's risk profile* above, there were higher ML/TF risks associated with Customer 27's source of wealth or source of funds.

At all times, SCA understood Customer 27 to be retired. Customer 27's turnover was not consistent with their source of wealth.

d. to the extent that SCA reviewed Customer 27's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 27.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

ECDD triggers in respect of Customer 27

929. SCA was required to apply the ECDD program to Customer 27 following any ECDD triggers in respect of Customer 27.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

930. Customer 27 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 21 December 2016 and 11 August 2021, SCA gave the AUSTRAC CEO 12 SMRs with respect to Customer 27.

b. determined to be high risk by SCA for the purpose of the Act and Rules prior to the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 27* above.

931. Each matter pleaded in paragraph 930 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

932. SCA did not conduct appropriate risk-based ECDD with respect to Customer 27 following an ECDD trigger because:

a. on each occasion prior to 29 July 2021 that SCA conducted ECDD in respect of Customer 27 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 27 and failed to appropriately consider whether the ML/TF risks posed by Customer 27 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

In December 2016, April 2017, May 2017, March 2018 and May 2019, SCA staff reviewed CCTV footage of Customer 27 and observed Customer 27 engaged in suspicious behaviour, including:

a. receiving cash or chips from other SCA customers, or passing chips to other SCA customers;

b. attending SCA's premises carrying a bag of cash; and

c. speaking to Person 5, who then withdrew money at the SCA Cashiers' desk in a manner that was unusual for them, and passed the funds they had withdrawn to Customer 27 a short time later.

In June 2017, September 2017, May 2018, June 2018 July 2018, August 2018, January 2019, February 2019, March 2019, June 2019 and August 2019, SCA staff (including an SCA AML Analyst) requested historical reviews of Customer 27's actions on the premises. These historical reviews revealed suspicious behaviour which was subsequently reported in an SMR given to the AUSTRAC CEO.

On 20 April 2017, an SCA AML adviser and SCA's Surveillance Operator / Risk & Analysis Operator / Surveillance Risk & Analysis reviewed transactions involving Customer 27 and noted their concerns regarding:

a. the possibility that Customer 27 was involved in money lending or money laundering;

b. where the funds and chips were coming from and who they were getting disbursed to;

c. the possibility that VIP IB Hosts were facilitating third party transactions and withholding the details of the third parties involved; and

d. the possibility that VIP IB Hosts were facilitating illegal money lending between customers mainly due to the involvement of Customer 27.

On 22 May 2018, an SCA AML Adviser and an SCA surveillance Risk & Analysis Investigator considered the relationship between Customer 27 and another SCA customer, Customer 2. The AML adviser expressed the view that it appeared that Customer 27 lent money to Customer 2 and that Customer 27 was not acting in any other capacity beyond as loan-shark.

The ECDD conducted by SCA did not have appropriate regard to Customer 27's higher ML/TF risks: see *Customer 27's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 27's source of funds or source of wealth.

By reason of the matters set out in *Customer 27's risk profile* above, there were higher ML/TF risks associated with Customer 27's source of wealth or source of funds.

However, it was not until 29 July 2021 that SCA issued a ban in respect of Customer 27.

b. on any occasion prior to 29 July 2021 that senior management considered the higher ML/TF risks posed by Customer 27 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 27 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

On 23 February 2017, an AML/CTF Senior Management Group meeting considered SMRs that were given to the AUSTRAC CEO in respect of Customer 27 in relation to money lending.

On 18 June 2018, SCA's General Manager of Table Games sent an email to the SCA Executive Manager of Finance and the General Manager Adelaide noting that Customer 27 appeared to be the main source of emergency funds for a number of big players. The General Manager of Table Games noted that SCA had previously warned Customer 27 regarding overt money lending to other SCA customers. However, they also noted that private arrangements are difficult to prove and prevent, and further that source of funds was "agnostic when it comes to results; and when the luck turns, players having quick access to funds is a good thing."

On 22 July 2021, an SCA AML Compliance Manager informed an SCA AML Compliance Analyst that SCA would need to complete an exhaustive ECDD report on Customer 27 in order to assess the veracity of a statement made by an SCA AML Compliance Analyst in an Incident File that Customer 27 was a known money lender who SCA suspected collected interest on loans.

It was not until 29 July 2021 that SCA issued a ban in respect of Customer 27.

Contravention of s 36 of the Act in respect of Customer 27

933. By reason of the matters pleaded from paragraphs 921 to 932 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 27 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

934. By reason of the matters pleaded at paragraph 933, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 29 July 2021 with respect to Customer 27.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 28

935. Customer 28 was a customer of SCA during the relevant period. Between September 2017 and August 2019, SCA recorded turnover exceeding $46,000,000 for Customer 28.

Particulars

Customer 28 was a customer of SCA from at least 9 September 2015.

On 9 August 2021, SCA issued a ban in respect of Customer 28 at the direction of the SCA AML team.

936. SCA provided Customer 28 with designated services within the meaning of table 3, s 6 of the Act during the relevant period.

Particulars

Prior to 7 December 2016, SCA opened an FMA for Customer 28 which remained open as at 28 October 2022 (item 11, table 3, s 6 of the Act).

See *Customer 28's risk profile* below.

937. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 28.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 28's risk profile

938. On and from 7 December 2016, Customer 28, and the provision of designated services to Customer 28 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 28's risk profile prior to the relevant period

a. by 7 December 2016, Customer 28 had the following risk history:

   i. SCA had formed suspicions for the purposes of s 41 of the Act with respect to Customer 28;

Particulars

SCA gave the AUSTRAC CEO an SMR on one occasion on 10 March 2015.

The SMR reported that on 10 March 2015, Customer 28 made two cash buy-ins below the transaction threshold. Customer 28 made a buy-in of $9,900 at one table and placed a $300 bet. Customer 28 then moved to another table and removed a $100 note before

conducting a second $9,900 buy-in. These transactions were indicative of the ML/TF typology of structuring.

ii. Customer 28 received high value gambling services (table 3, s 6 of the Act) at SCA;

Particulars

In 2015, Customer 28's recorded individual rated table gambling activity at SCA was estimated as a buy-in of $1,527,740, turnover of $9,343,075 with losses of $140,620.

iii. Customer 28 transacted using large amounts of cash at SCA; and

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 4 February 2014 and 20 September 2016, SCA gave the AUSTRAC CEO 18 TTRs detailing cash and chip exchanges made by Customer 28 totalling $319,340, which comprised:

a. 15 incoming transactions involving the issuance of chips or tokens totalling $288,700; and

b. three outgoing transactions involving cashing out chips or tokens totalling $30,640.

Large cash transactions

Between 9 September 2015 and 22 September 2016, SCA recorded cash buy-ins of approximately $561,300 for Customer 28.

iv. Customer 28 engaged in transactions indicative of ML/TF typologies and vulnerabilities, including structuring.

Particulars

See paragraph 24 above.

See particulars to paragraph 938.a.i above.

Customer 28's risk profile during the relevant period

b. Customer 28 received high value gambling services (table 3, s 6 of the Act) at SCA other than through junket programs. Between 28 September 2017 and 20 September 2019, SCA recorded an estimated buy-in of $4,073,300, a turnover estimated at $46,093,257 for Customer 28, with cumulative losses of $990,260;

Particulars

In 2016, Customer 28's recorded individual rated table gambling activity for table games at SCA was estimated as a buy-in of $1,532,700, turnover of $4,129,578 with losses of $59,500.

In 2017, Customer 28's recorded individual rated table gambling activity for table games at SCA was estimated as a buy-in of $455,350, turnover of $982,559 with losses of $100,700.

In 2018, Customer 28's recorded individual rated table gambling activity for table games at SCA escalated significantly to an estimated buy-in of $7,633,100, turnover of $28,839,391 with losses of $554,315.

In 2019, Customer 28's recorded individual rated gambling activity at SCA was estimated as a buy-in of $3,904,800 for table games, and for both table games and EGMs, turnover of $16,271,308 with losses of $275,745.

c. SCA was aware that Customer 28 had engaged in:

   i. large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose; and

   ii. transactions indicative of ML/TF typologies and vulnerabilities, including structuring, loan sharking and cashing-in large value chips with no evidence of play;

Particulars

See paragraph 24 above.

On 24 February 2018, Customer 28 performed two table buy-ins each for $9,900 in cash. SCA recorded that Customer 28's actions prior to the buy-ins were suspicious, as they had "fiddled" with their bag near the toilets before removing the cash. Prior to each buy-in, it appeared that Customer 28 had a bundle of $100 notes totalling $10,000, but removed one $100 bill from the bundle. On 27 February 2018, Customer 28 performed a third cash-buy-in for $9,900. SCA recorded that the need for Customer 28 to use cash for these buy-ins was questionable, as they had bought $150,000 worth of CPVs to use at gaming tables over the month of February 2018: SMR dated 1 March 2018. These transactions were indicative of the ML/TF typology of structuring.

On 15 June 2018, Customer 28 exchanged an unknown amount of chips for cash at SCA. Immediately after doing so, Customer 28 produced $10,000 in cash to exchange for chips. The Cashier processing the exchange then saw Customer 28 pass the chips to Customer 27, whom SCA suspected to be involved in loan sharking and utilising third parties to conduct transactions on their behalf. SCA recorded that Customer 28 and Customer 27 were known associates and shared the same residential address: SMR dated 20 June 2018.

On 12 July 2018, Person 5 lost approximately $675,000 playing baccarat. During this period, Person 5 exhausted their own funds and turned to Customer 28 and Customer 27, who provided funds for Person 5 to use for gaming. SCA's CCTV cameras captured Customer 27 giving Person 5 plastic bags containing cash. Person 5 then presented two plastic bags containing $101,300 in cash to an SCA Cashier. Later that evening, Customer 28 handed Person 5 $20,000 in chips under the table at which Person 5 was playing. SCA considered that Customer 27 was participating in money lending or

loan sharking activities with Customer 28 and Person 5: SMR dated 13 July 2018.

On 30 August 2018, Customer 27 and Customer 28 approached Cashiers at the same time. Customer 28 cashed out $2,970 while Customer 27 cashed out $2,700. Customer 28 returned to the Cashier a few minutes later and cashed out a further $9,000. Customer 28 did not game between the two cash outs, and left SCA immediately after the second cash out. SCA considered that Customer 28 had structured the cash outs to avoid the reporting obligation: SMR dated 5 September 2018.

On 16 July 2019, Customer 28 approached a gaming table in the Grange Room, removed a $100 note from a bundle of cash from their pocket and then made a buy-in with $9,900. About an hour later, Customer 28 removed another $100 note from a bundle of cash from their pocket and handed $9,900 in cash to a dealer at a different table for a buy-in. SCA recorded that Customer 28 had a history of structuring transactions, and that this incident highlighted the deliberate nature of Customer 28's actions: SMR dated 23 July 2019.

d. Customer 28 was connected to other customers at SCA, including players who posed higher ML/TF risks such as Customer 27 and players who SCA considered had acted suspiciously, such as Person 5;

Particulars

See particulars to paragraph 938.c above.

e. Customer 28 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

See particulars to paragraph 938.c above.

TTRs

Between 19 October 2017 and 24 September 2019, SCA gave the AUSTRAC CEO 60 TTRs detailing incoming and outgoing payments made by Customer 28 totalling $1,885,015, which comprised:

a. 44 TTRs totalling $1,114,915 in chip and cash exchanges;

b. 15 TTRs totalling $311,915 in account deposits; and

c. one TTR totalling $10,000 in a casino prize.

f. Customer 28 had access to private gaming rooms at SCA; and

Particulars

See paragraph 145(e) above.

Customer 28 had access to private gaming rooms at SCA, including the Platinum Room and the Grange Room.

g. SCA did not have adequate reason to believe that Customer 28's source of wealth or source of funds was sufficient to explain the high value gambling services (table 3, s 6 of the Act) provided to Customer 28 by SCA.

Particulars

See paragraph 516 above.

By 7 December 2016, SCA understood that Customer 28's occupation was as a restaurant manager.

Between 28 September 2017 and 20 September 2019, SCA recorded an estimated buy-in of $4,073,300.

By February 2018, SCA was aware that Customer 28 was associated with Customer 27, who was a suspected loan shark: SMR dated 1 March 2018.

In July 2019, SCA recorded that it did not know much about Customer 28's source of funds, other than the fact that Customer 28 was a restaurant manager. SCA considered that Customer 28 could be receiving funds from Customer 27: SMR dated 23 July 2019.

Despite this, SCA did not request source of wealth information from Customer 28 until 9 August 2021. On the same date, SCA banned Customer 28 from attending the casino until an assessment of their Source of Wealth Declaration Form was completed.

At no time was SCA's understanding of Customer 28's source of wealth or source of funds commensurate with the high value gambling services that they received at SCA.

SCA's determination of the ML/TF risks posed by Customer 28

939. On and from 12 August 2016, Customer 28 was appropriately rated by SCA as a high risk customer for the purpose of the Act and Rules.

940. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 28 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by it with respect to Customer 28.

Monitoring of Customer 28's transactions

941. At no time did SCA apply appropriate transaction monitoring to Customer 28's transactions because SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

The review, update and verification of Customer 28's KYC information

942. SCA did not review, update or verify Customer 28's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 28, including the nature, extent and purpose of Customer 28's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review and update Customer 28's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 28's risk profile* above, there were higher ML/TF risks associated with Customer 28's source of wealth or source of funds.

d. to the extent that SCA reviewed Customer 28's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 28.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

Failure to apply appropriate due diligence suited to the high ML/TF risks

943. Had SCA conducted ongoing customer due diligence on and from 7 December 2016 by:

a. appropriately identifying and assessing the ML/TF risks posed by Customer 28;

b. applying appropriate risk-based transaction monitoring to Customer 28; and

c. appropriately reviewing and updating Customer 28's KYC information, having regard to the high ML/TF risks,

SCA would have been required by the Act and Rules to apply the ECDD Program to Customer 28 at a time before the date of the ECDD triggers pleaded below: see *ECDD triggers in respect of Customer 28*.

ECDD triggers in respect of Customer 28

944. SCA was required to apply the ECDD program to Customer 28 following any ECDD triggers in respect of Customer 28.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

945. Customer 28 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 1 March 2018 and 23 July 2019, SCA gave the AUSTRAC CEO four SMRs with respect to or pertaining to Customer 28.

b. determined to be high risk by SCA for the purpose of the Act and Rules prior to the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 28* above.

946. Each matter pleaded in paragraph 945 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

947. SCA did not conduct appropriate risk-based ECDD with respect to Customer 28 following an ECDD trigger because:

a. on each occasion prior to August 2021 that SCA conducted ECDD in respect of Customer 28 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 28 and failed to appropriately consider whether the ML/TF risks posed by Customer 28 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501, 511 and 516 to 517 above.

Watchlist screening

On or around 28 June 2018, SCA conducted a PEP screening in respect of Customer 28.

Transaction reviews

Between February 2018 and July 2019, SCA reviewed transactions involving Customer 28 at SCA on five occasions: see particulars to paragraph 938.c above.

ECDD screenings

On 3 April 2019, SCA conducted ECDD screening in respect of Customer 28. The ECDD screening recorded that:

a. Customer 28 was a known associate of Customer 27;

b. Customer 28 had conducted transactions indicative of structuring; and

c. Customer 28's occupation and source of wealth and source of funds was as a restaurant manager.

Source of wealth ECDD

On 9 August 2021, SCA conducted a review of its customer relationships. As part of this assessment, it requested source of wealth information from Customer 28 and banned them from the casino pending this information.

The ECDD conducted by SCA did not have appropriate regard to Customer 28's higher ML/TF risks: see *Customer 28's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 28's source of funds or source of wealth.

By reason of the matters set out in *Customer 28's risk profile* above, there were higher ML/TF risks associated with Customer 28's source of wealth or source of funds.

b. on any occasion prior to August 2021 that senior management considered the higher ML/TF risks posed by Customer 28 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 28 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

At no time prior to August 2021 were the higher ML/TF risks posed by Customer 28 considered by senior management.

On 4 August 2021, an SCA AML Compliance Manager advised the SCA Chief Operating Officer that they had prepared a letter to Customer 28, requesting further information about their source of wealth.

On 5 August 2021, the Chief Operating Officer queried whether SCA intended to terminate its business relationship with Customer 28 immediately.

The AML Compliance Manager confirmed that SCA would effectively cease doing business with Customer 28 until a response to the letter had been received and reviewed.

On 9 August 2021, SCA issued a ban in respect of Customer 28.

Contravention of s 36 of the Act in respect of Customer 28

948. By reason of the matters pleaded from paragraphs 935 to 947 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 28 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

949. By reason of the matters pleaded at paragraph 948, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 9 August 2021 with respect to Customer 28.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 29

950. Customer 29 was a customer of SCA during the relevant period. Between 17 December 2016 and 22 March 2021, SCA recorded turnover exceeding $85,000,000 for Customer 29.

Particulars

Customer 29 was a customer of SCA from at least 28 October 2007.

On 31 March 2021, SCA issued a ban in respect of Customer 29 at the recommendation of the SCA AML team.

951. SCA provided Customer 29 with designated services within the meaning of tables 1 and 3, s 6 of the Act during the relevant period.

Particulars

Prior to the relevant period, SCA opened an FMA for Customer 29 which remained open as at 28 October 2022 (item 11, table 3, s 6 of the Act).

While a customer of SCA, Customer 29 remitted funds to their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 29's risk profile* below.

952. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 29.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 29's risk profile

953. On and from 7 December 2016, Customer 29, and the provision of designated services to Customer 29 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 29's risk profile prior to the relevant period

a. by 7 December 2016, Customer 29 had the following risk history:

i. SCA formed suspicions for the purposes of s 41 of the Act with respect to Customer 29;

Particulars

Between 21 May 2016 and 20 September 2016, SCA gave the AUSTRAC CEO an SMR pertaining to Customer 29 on four occasions.

The SMRs reported that Customer 29 had engaged in behaviour indicative of ML/TF typologies including refining and structuring.

ii. SCA was aware that Customer 29 had engaged in conduct indicative of refining;

Particulars

For example, in May 2016, an SCA AML Analyst observed that Customer 29 was exchanging their lower denomination notes for higher denomination notes with minimal betting: SMR dated 21 May 2016.

iii. SCA was aware that Customer 29 had engaged in conduct indicative of structuring;

Particulars

For example, in August 2016, an SCA AML Analyst determined that the conduct of Customer 29 and their associate, Customer 35, was concerning, and concluded that they appeared to be deliberately structuring transactions to avoid reporting thresholds: SMR dated 16 August 2016.

iv. SCA was aware that Customer 29 was associated with convicted criminals, including members of their family, and other SCA customers that SCA considered had acted suspiciously;

Particulars

In August 2016, an SCA AML Analyst observed that members of Customer 29's family had been the subject of SMRs given to the AUSTRAC CEO on numerous occasions for behaviour indicative of ML/TF typologies including structuring, refining, irregular spending and avoiding the transaction reporting threshold. Two members of Customer 29's family had been banned from SCA by a law

enforcement agency for extensive criminal history and drug related offences: SMRs dated 2 August 2016 and 16 August 2016.

The SCA AML Analyst also reported that SCA had created a chart in an attempt to discover the relationships between Customer 29's family members and their associates: SMR dated 16 August 2016.

v. SCA was aware that Customer 29's high turnover and gambling activities were not consistent with their source of wealth; and

Particulars

In 2015, Customer 29's recorded individual rated gambling activity at SCA was estimated as a buy-in of $814,640 for table games, and for both table games and EGMs, turnover of $5,993,565 with losses of $108,892.

By August 2016, SCA had formed suspicions that Customer 29's gambling activity was inconsistent with their occupation, which was recorded as a meat packer. An SCA AML Analyst observed that in or around August 2016, Customer 29 had won approximately $360,000 and, based on Customer 29's occupation, it was difficult to determine where their money came from to support the underlying gambling activity.

vi. Customer 29 transacted using large amounts of cash and engaged in suspicious cash transactions at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 4 April 2010 and 26 September 2016, SCA gave the AUSTRAC CEO 51 TTRs detailing incoming and outgoing payments made by Customer 29 totalling $979,850, which comprised:

a. 39 TTRs totalling $719,850 in chip and cash exchanges; and

b. 12 TTRs totalling $260,000 in account deposits.

Suspicious cash transactions

In October 2015, an SCA Cashier requested photo identification from Customer 29 after an incident at the VIP Cage. Customer 29 had requested that the Cashier return their bundle of $20 notes once Customer 29 realised that the Cashier intended to manually count the notes rather than use a counting machine.

Customer 29's risk profile during the relevant period

b. Customer 29 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs. Between 17 December 2016 and 22 March 2021, SCA recorded an estimated buy-in of $13,468,390, a turnover estimated at $85,828,892 for Customer 29, with cumulative losses of $2,608,881;

Particulars

In December 2016, Customer 29's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $3,300, turnover of $22,001 with wins of $5,600.

In 2017, Customer 29's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $952,200, turnover of $3,842,595 with losses of $178,400.

In 2018, Customer 29's recorded individual rated gambling activity at SCA escalated to an estimated buy-in of $3,091,370 for table games, and for both table games and EGMs, turnover of $14,346,811 with losses of $684,403.

In 2019, Customer 29's recorded individual rated gambling activity at SCA was estimated as a buy-in of $3,110,450 for table games, and for both table games and EGMs, turnover of $16,737,491 with losses of $539,831.

In 2020, Customer 29's activity remained high, despite closures related to the COVID-19 pandemic. Customer 29's recorded individual rated gambling activity at SCA was estimated as a buy-in of $3,143,770 for table games, and for both table games and EGMs, turnover of $23,194,148 with losses of $696,594.

Up until March 2021, Customer 29's recorded individual rated gambling activity at SCA significantly escalated to an estimated buy-in of $3,167,300 for table games, and for both table games and EGMs, turnover of $27,687,445 with losses of $515,483.

c. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 29 by remitting large amounts of money into, out of and within the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

SCA made money available to Customer 29 in the following transactions:

Between 23 June 2018 and 11 February 2021, SCA received 42 telegraphic transfers totalling $818,700, each of which was made available to Customer 29's FMA. 29 of these telegraphic transfers totalling $378,000 were sent from Customer 29's personal bank account in Australia.

d. from at least June 2018, SCA was aware that Customer 29 was associated with a number of customers– including junket operator Customer 2 and other players who posed higher ML/TF risks such as Customer 30, Customer 31, Customer 32, Customer 33, Customer 35, Customer 36 and Customer 37 – who conducted large and unusual

transactions and patterns of transactions with each other, which had no apparent economic or visible lawful purpose;

i. the provision of designated services by SCA to Customer 29 and their associates raised red flags reflective of higher ML/TF risks;

Particulars

Red flags reflective of higher ML/TF risks included:

a. handing chips and cash to one another: SMRs dated 12 April 2017, 16 February 2018, 25 May 2018, 18 June 2018, 24 July 2018, 6 August 2020, 24 August 2020, 8 September 2020, 15 September 2020, 18 September 2020, 8 October 2020, 5 February 2021 and 7 April 2021;

b. handing unknown items to one another: SMRs dated 12 April 2017, 18 June 2018 and 8 October 2020;

c. concealing cash and chips in their clothing: SMRs dated 12 April 2017, 18 June 2018, 24 August 2020, 8 September 2020 and 18 September 2020;

d. placing cash and chips into items such as envelopes, handbags, bundles and plastic bags: SMRs dated 12 April 2017, 18 June 2018, 24 August 2020, 8 September 2020, 15 September 2020 and 5 February 2021;

e. exchanging these cash-filled items between each other, including by passing them between one another in the toilets and under tables: SMRs dated 12 April 2017 and 18 June 2018;

f. using their bodies to conceal or obscure chip and cash exchanges from the view of surveillance cameras: SMR dated 18 June 2018;

g. conducting little or no gambling activity to support the amounts of cash and chips exchanged: SMRs dated 25 May 2018, 18 June 2018, 24 August 2020 and 15 September 2020;

h. exchanging cash for chips on multiple gaming Cashiers, tables or Cages in several transactions: SMRs dated 25 May 2018, 18 June 2018, 24 August 2020, 8 September 2020 and 15 September 2020;

i. conducting separate cash and chip transactions below the reporting threshold in quick succession: SMRs dated 25 May 2018, 18 June 2018, 15 September 2020, 5 February 2021 and 7 April 2021;

j. using EFTPOS and ATM facilities to conduct significant cash transactions in quick succession: SMR dated 25 May 2018 and 7 April 2021;

k. conducting significant cash and chip exchanges in the SCA toilets: SMRs dated 18 June 2018, 6 August 2020, 24 August 2020, 5 February 2021 and 7 April 2021;

l. carrying significant amounts of cash and chips into the SCA toilets away from the view of surveillance cameras, and sometimes swapping the cash between different carry items inside the toilets: SMRs dated 18 June 2018 and 18 September 2019;

m. making and receiving phone calls and then conducting cash and chip exchanges shortly thereafter: SMR dated 18 June 2018;

n. presenting rewards cards to the SCA Cashier belonging to other customers: SMRs dated 18 September 2020 and 5 February 2021; and

o. sponsoring associates' access to VIP areas, including individuals known to SCA for criminal association and conduct indicative of ML/TF risks: SMR dated 6 August 2020.

ii. SCA formed suspicions in respect of the conduct of these customers;

Particulars

SCA considered it suspicious that the customers, including Customer 29:

a. conducted transactions in a secretive manner that was designed to conceal and disguise their associations, and distance themselves and their motives from the transactions, by using agents and family members, initiating transactions through phone calls, and by conducting transactions with minimal contact. Customer 29 and their associates knew where the SCA CCTV cameras were located and chose to conduct their business in settings with limited surveillance such as the SCA toilets, balcony areas, lifts or other places away from SCA employees and gaming tables: SMRs dated 12 April 2017, 18 June 2018, 24 August 2020, 18 September 2020 and 8 October 2020;

b. conducted transactions that were not supported by gambling activity: SMRs dated 25 May 2018, 18 June 2018, 24 August 2020 and 15 September 2020;

c. conducted cash and chip exchanges that had no identifiable purpose: SMR dated 18 June 2018;

d. conducted transactions to disguise the true source of their funds at SCA: SMR dated 8 September 2020;

e. were closely associated with SCA customers who had been arrested or reported in SMRs given to the AUSTRAC CEO for drug trafficking and loan sharking offences: SMRs dated 16

February 2018, 25 May 2018, 18 June 2018, 24 July 2018, 24 July 2019, 8 September 2020 and 15 September 2020;

f. SCA was not aware of connections or associations between all participants in the above transactions: SMRs dated 25 May 2018, 18 June 2018 and 24 July 2018;

g. did not have occupations that would account for the size and volume of their transactions: SMR dated 24 August 2020; and

h. conducted transactions indicative of the ML/TF typologies of third party payments, layering, refining, loan sharking and structuring transactions: SMRs dated 12 April 2017, 16 February 2018, 25 May 2018, 18 June 2018, 24 July 2018, 24 July 2019, 6 August 2020, 24 August 2020, 8 September 2020, 15 September 2020, 18 September 2020, 8 October 2020 and 5 February 2021.

Further, customer 29 appeared to be collecting money from their associates for debts owed: SMR dated 25 May 2018; and

g. SCA was aware that Customer 29:

i. had engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

Particulars

On 13 February 2018, Customer 29 took possession of $24,000 in cash chips from another SCA customer at a baccarat table. SCA reported that Customer 29 lost $33,000 over the course of gaming on that day: SMR dated 16 February 2018.

In May 2018, SCA staff observed Customer 29 gaming with chips and cash they received in an envelope from another SCA customer. While Customer 29 was gaming with those funds, one of their associates conducted six $200 EFTPOS transactions and another associate bought $2,000 in cash chips. Another associate, sitting at the same row of EGMs, passed cash from those transactions to Customer 29 on three occasions. SCA recorded that Customer 29 lost $29,000 over the course of gaming in one day during this period: 25 May 2018.

On 19 July 2018, Customer 29 handed $10,000 in cash to another SCA customer who exchanged the cash for chips at the Platinum Cashier. The customer then handed $9,000 in $100 notes to Customer 29. Customer 29 returned the money to the customer who made a buy-in at a gaming table for $9,000 before standing up and moving behind Customer 29. The gaming staff then placed the $9,000 in chips on the gaming table in front of Customer 29 who took possession of the chips. Another SCA customer made a buy-in for $1,000 at the same table and Customer 29 again took possession of their chips: SMR dated 24 July 2018.

On 24 July 2019, SCA reported that Customer 29 lost $444,000 over the course of gaming in one day: SMR dated 24 July 2019.

On 14 August 2020, SCA recorded a series of large cash and chip exchanges between Customer 29 and other SCA customers exceeding $69,000. During the course of the exchanges, Customer 29 accompanied an SCA customer into the toilets. Customer 29 and the customer then met three other SCA customers on the smoking balcony. SCA noted that the conduct was consistent with their pattern of suspicious behaviour: SMR dated 24 August 2020.

SCA identified that on 1 September 2020, Customer 29 and Customer 35 were passing cash chips between one another in the Black Room. SCA considered these transactions were an attempt to misrepresent the origin and destination of the funds: SMR dated 8 September 2020.

ii. had engaged in transactions involving large amounts of cash and cash that appeared suspicious, including cash that had a strong aroma of dirt, at SCA;

Particulars

See paragraphs 376 to 381 above.

See particulars to paragraphs 953.d, 953.g.i and 953.g.iii.

TTRs

Between 27 April 2017 and 30 March 2021, SCA gave the AUSTRAC CEO 217 TTRs detailing incoming and outgoing payments made by Customer 29 totalling $4,670,679, which comprised:

a. 172 TTRs totalling $3,681,690 in chip and cash exchanges;

b. 38 TTRs totalling $814,000 in account deposits;

c. five TTRs totalling $93,000 in account withdrawals;

d. one TTR totalling $11,989 for an EGM payout; and

e. one TTR totalling $70,000 for cashing out a cheque.

Other large and suspicious cash transactions in 2017

In April 2017, SCA recorded a series of large cash and cash chip exchanges between Customer 29 and their associates, including their spouse, Person 19, and Customer 32. SCA determined that in one exchange Customer 29 received $40,000 in cash from Person 19: SMR dated 12 April 2017.

Other large and suspicious cash transactions in 2019

In July 2019, Customer 29 exited SCA via the valet entrance and returned three minutes later with $70,000 in cash. SCA investigators could not confirm the source of this cash, but suspected that Customer 29 retrieved the cash from their vehicle. SCA also recorded that Customer 29 had won approximately $210,000 in the previous two weeks of gaming: SMR dated 24 July 2019.

Other large and suspicious cash transactions in 2020

In September 2020, Customer 29 received five $5,000 cash chips, totalling $25,000 in the Grange Room. Customer 29 then passed $12,000 in cash chips to their associate, Customer 30, who cashed out $26,400 in cash chips. Customer 29 and Customer 30 entered the toilets before leaving SCA together: SMR dated 15 September 2020.

In September 2020, Customer 29 received ten $1,000 cash chips totalling $10,000 from their associate, Customer 32, in the Grange Room: SMR dated 18 September 2020.

In September 2020, SCA reported a series of covert cash exchanges between Customer 29 and their associate, Customer 37, including an instance where Customer 29 received ten $1,000 cash chips from Customer 37. SCA suspected that Customer 37's transactions at the Grange Cashier totalling $25,000 were conducted with funds provided by Customer 29 during the exchanges: SMR dated 18 September 2020.

Other large and suspicious cash transactions in 2021

In January 2021, Customer 29 and their associates, Customer 30 and Customer 33, exchanged large amounts of cash and chips between themselves. SCA noted that this conduct reflected an established pattern of behaviour for both Customer 29 and Customer 30, and that Customer 29 appeared to be using Customer 30 as a third party to avoid reporting requirements: SMR dated 5 February 2021.

On 20 March 2021 and 21 March 2021, Customer 29 engaged in a series of suspicious behaviours and transactions, including exchanging large amounts of cash and cash chips with Customer 30 and other associates. When Customer 29 presented $35,000 in cash at the Grange Cashier on 20 March 2021, SCA front line staff observed that the cash had a strong aroma of dirt. SCA reviewed Customer 29's transactions on 20 March 2021 and 21 March 2021 and determined that Customer 29 conducted cash buy-ins totalling $87,600 with a turnover of $666,038 and losses of $86,344 during those two days: SMR dated 7 April 2021.

iii. had engaged in large buy-ins and cash outs, including with cash and CVIs;

Particulars

For example, on the following occasions Customer in 2016, Customer 29 had engaged in transactions 29 transacted using large amounts of chips at SCA:

a. on 14 April 2019, Customer 29 exchanged $70,000 in chips for a cheque. The next day, Customer 29 made a buy-in with a $70,000 cheque in exchange for chips;

b. on 16 April 2019, Customer 29 exchanged $100,000 in chips for a cheque. On the same day, Customer 29 deposited $60,000 in chips into their FMA;

c. on 23 April 2019, SCA issued Customer 29 $30,000 in chips, using funds from their FMA. Shortly after, Customer 29 deposited $35,000 in chips into their FMA. A few moments later, Customer 29 exchanged $100,000 in chips for a cheque in the full amount. Two days later, on 25 April 2019, Customer 29 bought-in with a cheque in the amount of $100,000 in exchange for chips;

d. on 17 July 2019, Customer 29 made a buy-in with two cheques in the amounts of $50,000 and $60,000 in exchange for $110,000 in chips. Shortly after, Customer 29 exchanged $120,000 in chips for a cheque in the full amount. On the same day, Customer 29 deposited $80,000 in chips into their FMA;

e. on 18 July 2019, SCA issued Customer 29 $80,000 in chips, using funds from their FMA. The next day, SCA issued Customer 29 a total of $175,000 in chips across three transactions, in which Customer 29 used cash, a cheque and money from their FMA;

f. in September 2019, Customer 29 received three cheques from SCA totalling $185,000:

i. on 9 September 2019, Customer 29 received a cheque in the amount of $55,000;

ii. on 19 September 2019, Customer 29 exchanged $40,000 in chips for a cheque; and

iii. on 27 September 2019, Customer 29 exchanged $90,000 in chips for a cheque;

g. on 24 December 2020, Customer 29 made a buy-in with $75,000 across three transactions, in which Customer 29 used cash and money from their FMA, and cashed out $133,000 across four transactions;

h. on 26 December 2020, Customer 29 made a buy-in with $73,000 across three transactions, using money from their FMA;

i. on 6 February 2021, Customer 29 cashed out $65,000 and then made a buy-in with $120,000 across four transactions, using cash and money from their FMA;

j. on 19 February 2021, Customer 29 made a buy-in with $80,000 cash across four transactions, and cashed out $42,205 across two transactions; and

k. on 17 March 2021, Customer 29 cashed out $80,000 in chips, which SCA paid to Customer 29 in cash.

iv. was connected to convicted drug traffickers and SCA customers who had been banned for their extensive criminal history;

Particulars

a. At all times, SCA was aware that Customer 29 had close family ties to Customer 32 and other SCA customers who had been convicted of drug trafficking offences and were subsequently banned from SCA: SMRs dated 25 May 2018, 18 June 2018 and 24 July 2018. see paragraph 953.a.iv.

b. By 23 March 2021, SCA was aware that Customer 29's spouse, Person 19, was a convicted drug trafficker who had been sentenced to three years' imprisonment for trafficking heroin.

c. SCA was aware that Person 19 was involved in suspicious behaviour at SCA, including conduct indicative of the ML/TF typologies of structuring and cashing-in large value chips with no evidence of play. In particular:

    i. Person 19 was a VIP player at SCA;

    ii. in April 2017, an SCA AML Analyst requested a review regarding Person 19's transactions due to unusual activity recorded on their accounts. SCA recorded that Person 19 conducted two transactions on 11 April 2017 totalling $65,000 without any corresponding gambling activity;

    iii. in April 2017, SCA recorded Person 19, Customer 29, Customer 32 and another known associate working together to structure cash outs to disguise the true source of their funds. SCA reported that all four individuals had been previously identified for suspicious behaviour and had been the subject of SMRs given to the AUSTRAC CEO;

    iv. in March 2021, an SCA AML Analyst circulated an enquiry to SCA Surveillance staff identifying a potential association between Person 19 and an SCA dealer;

    v. by September 2021, SCA presumed that Person 19 was an associate of Customer 35; and

    vi. it was not until October 2021 that SCA reviewed Person 19's gambling activity at SCA. In an internal memorandum dated 26 October 2021, an SCA AML Analyst reported that the latest Player Gaming Summary Report for Person 19 showed a cash buy-in of $960,000, winnings of $222,000, and a total turnover of $30,000,000 since 2012;

d. It was not until October 2021 that SCA recorded that Customer 29's parent and two siblings, who were also members at SCA, had received suspended sentences in

2009 following their convictions for the sale and supply of heroin.

e. SCA was aware that Customer 29 was a close associate of Customer 33, who had been convicted several times for dealing drugs, and who was banned from SCA between 2012 and 2014 for using the proceeds of crime to gamble at SCA: see *Customer 33's risk profile,* below.

h. by 15 December 2020, SCA was aware of a number of court lists which named Customer 29 and their spouse, Person 19, as having appeared in an Australian court;

Particulars

On 15 December 2020, SCA became aware of four media articles published on 28 October 2020, 18 November 2020, 2 December 2020 and 7 December 2020. The articles reported on court lists, which showed that Customer 29 and Person 19 had appeared in an Australian court on each of those dates.

i. Customer 29 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including structuring, layering and the use of third parties to conduct transactions;

Particulars

See paragraph 24 above.

See paragraphs 953.d and 953.g above.

Customer 29 was involved in transactions indicative of the ML/TF typology of structuring on the following occasions:

a. in February 2017, SCA staff recorded that Customer 29 appeared to be attempting to avoid the transaction reporting threshold when cashing out chips;

b. in February 2018, SCA noted that Customer 29 had not conducted a threshold transaction since July 2017. Despite this, Customer 29's gaming levels had increased in the period from July 2017 to December 2017: SMR dated 16 February 2018;

c. in August 2020, SCA staff observed that Customer 29 was utilising Customer 36 as a third party to structure transactions. On 2 August 2020, Customer 29 and Customer 36 were observed conducting chip purchases for $7,000 and $5,000 in cash in order to avoid the transaction reporting threshold. SCA noted that Customer 29 had a history of utilising third parties to assist in transaction structuring. In this instance, SCA considered that Customer 29 appeared to be directing Customer 36 to act on their behalf: SMR dated 6 August 2020;

d. in September 2020, SCA staff observed that Customer 29 and their associate Customer 37 utilised third parties to conduct

threshold transactions on their behalf in order to avoid reporting requirements: SMR dated 18 September 2020;

e. in October 2020, SCA staff observed that Customer 29 was utilising Customer 37 to conduct multiple threshold transactions on their behalf in order to avoid reporting requirements. SCA noted that on 26 September 2020, Customer 29 performed multiple transactions with funds provided by Customer 37 in the amount of $25,000: SMR dated 8 October 2020; and

f. in 2021, SCA conducted a review of all bank transactions between 4 September 2019 and 5 October 2021. SCA determined that the transaction documents showed that a number of patrons, including Customer 29, engaged in repeated transactions that were indicative of the ML/TF typology of structuring. For example, on 10 February 2021 Customer 29 transferred $5,000 into their SCA FMA and then another $5,000 the next day.

g. In January 2021, Customer 29 and their associates, Customer 30 and Customer 33, exchanged large amounts of cash and chips between themselves. SCA noted that this conduct reflected an established pattern of behaviour for both Customer 29 and Customer 30, and that Customer 29 appeared to be using Customer 30 as a third party to avoid reporting requirements: SMR dated 5 February 2021.

j. designated services provided to Customer 29 included substantial EGM activity at SCA;

Particulars

See paragraphs 352 and 353 above.

From 2018 to 2021, Customer 29's turnover on EGMs was estimated to be $226,575 with estimated total losses of $16,181.

k. Customer 29 had access to private gaming rooms at SCA; and

Particulars

See paragraph 145(e) above.

Customer 29 had access to private gaming rooms at SCA, including the Grange Room, the Platinum Room, the Opal Room and the Black Room.

l. SCA did not have adequate reason to believe that Customer 29's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 29 by SCA.

Particulars

See paragraph 516 above.

Since the creation of Customer 29's account, SCA recorded their occupation as a meat packer.

Between 17 December 2016 and 22 March 2021, SCA recorded an estimated buy-in of $13,468,390

At all times, Customer 29's turnover was not consistent with their source of wealth.

In July 2019, February 2021 and April 2021 SCA identified that Customer 29's recorded play was substantially higher than their known source of funds: SMRs dated 24 July 2019, 5 February 2021 and 7 April 2021.

At all times, SCA was aware that Customer 29's close family members had been convicted of drug trafficking offences.

On or around 9 December 2020, SCA asked Customer 29 to complete a Source of Funds Declaration Form. Customer 29 did so. The completed form stated that they were unemployed and did not declare any other source of income. Customer 29 further advised SCA staff that they had recently sold their business and house, and that this was where they got their funds from. SCA staff recorded that Customer 29 was not willing to provide the name of their former business when asked.

On 22 December 2020, an SCA AML Analyst described Customer 29's Source of Funds Declaration Form as unsatisfactory. However, it was not until March 2021 that SCA requested Customer 29 complete a Source of Wealth Declaration Form. Meanwhile, between 22 December 2020 and 31 March 2021:

a. Customer 29's total turnover escalated significantly, exceeding $33,800,000;

b. Customer 29's estimated buy-in for table games escalated significantly, exceeding $3,750,000; and

c. Customer 29 conducted multiple transactions exceeding $150,000;

In March 2021, Customer 29 provided an updated Source of Wealth Declaration Form that updated their occupation to "home duties" and recorded the sale of a property as a source of wealth. Customer 29 declined to provide any documentation to support the information provided in their declaration form.

On 30 March 2021, Customer 29 advised SCA VIP hosting staff that they had considerable savings from their previous job as a meatworker, obtained funds from the sale of a house and used funds from Person 19. Customer 29 also advised that the group that they associated with utilised an informal loan club that resulted in a large monthly pot of funds: SMR dated 7 April 2021.

In late March 2021, SCA recorded that no business or house sale could be verified for Customer 29, and that Customer 29's losses of $1,141,645 on table games recorded for the current financial year were not commensurate with Customer 29's purported source of wealth.

It was not until October 2021 that an SCA AML Analyst concluded that the criminal history of several members of Customer 29's family and their close associates raised concerns about the ultimate source of funds that the family used to gamble and the overall risk they represented to the SCA.

During the relevant period, SCA recorded:

a. a high turnover for Customer 29 exceeding $85,000,000;

b. funds remitted into the casino environment via Customer 29's FMA exceeding $800,000; and

c. sustained patterns of large and unusual transactions conducted by Customer 29 and their associates, which had no apparent economic or visible lawful purpose.

At no time was SCA's understanding of Customer 29's source of wealth or source of funds commensurate with the high value financial and gambling services that they received at SCA.

SCA's determination of the ML/TF risks posed by Customer 29

954. On and from 13 June 2016, Customer 29 was appropriately rated by SCA as a high risk customer for the purpose of the Act and Rules.

Particulars

On 24 March 2021, Customer 29 was rated significant risk by SCA, which was high risk for the purpose of the Act and Rules.

955. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 29 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by it with respect to Customer 29.

Monitoring of Customer 29's transactions

956. At no time did SCA apply appropriate transaction monitoring to Customer 29's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 29 through the SCA Customer account channel, which was a high risk remittance channel.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 29's KYC information

957. SCA did not review, update or verify Customer 29's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 29, including the nature, extent and purpose of Customer 29's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update or verify Customer 29's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 29's risk profile* above, there were higher ML/TF risks associated with Customer 29's source of wealth or source of funds.

Since commencing as a customer until 15 December 2020, Customer 29's occupation was listed as a meat packer. On 15 December 2020, Customer 29 declared that they were unemployed.

Between 15 December 2020 and 31 March 2021, Customer 29's buy-in exceeded $13,000,000 At all times, Customer 29's gambling activity was not consistent with their source of wealth.

d. to the extent that SCA reviewed Customer 29's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 29.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

ECDD triggers in respect of Customer 29

958. SCA was required to apply the ECDD program to Customer 29 following any ECDD triggers in respect of Customer 29.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

959. Customer 29 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 12 April 2017 and 7 April 2021, SCA gave the AUSTRAC CEO 14 SMRs pertaining to Customer 29.

b. determined to be high risk by SCA for the purpose of the Act and Rules prior to the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 29* above.

960. Each matter pleaded at paragraph 959 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

961. SCA did not conduct appropriate risk-based ECDD with respect to Customer 29 following an ECDD trigger because:

a. on each occasion prior to December 2020 that SCA conducted ECDD in respect of Customer 29 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 29 and failed to appropriately consider whether the ML/TF risks posed by Customer 29 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501, 511 and 516 to 517 above.

On 5 July 2018 and 1 November 2018, SCA conducted ECDD in respect of Customer 29. The ECDD screenings conducted in July 2018 and November 2018 identified:

a. Customer 29's occupation as a meat packer; and

b. that in 2016, Customer 29 had engaged in transactions that were indicative of the ML/TF typology of refining.

These ECDD screenings were deficient in light of the high ML/TF risks posed by Customer 29, as identified by SCA at the time: SMRs

dated 12 April 2017, 16 February 2018, 25 May 2018, 18 June 2018 and 24 July 2018.

During this period, SCA was aware that Customer 29 and their associates were engaged in significant quantities of large and organised cash transactions that were conducted in suspicious circumstances and were indicative of the ML/TF typologies of structuring, layering, and utilising third parties to conduct transactions. SCA did not have any identifiable information to support Customer 29's high value gaming, particularly in circumstances where SCA was aware that Customer 29:

a. was connected to SCA customers who posed high ML/TF risks;

b. was closely related to SCA customers who had been banned for their extensive criminal histories and drug trafficking offences; and

c. had listed their occupation as a meat packer, which SCA determined was an inadequate explanation for the significant amount of cash Customer 29 used while gaming.

Database alerts

Between 14 November 2016 and 16 November 2020, SCA received five open source Dow Jones watchlist alerts in respect of Customer 29.

Further ECDD screening

SCA also conducted ECDD in respect of Customer 29 between 6 August 2020 and 6 July 2021.

On 6 August 2020, the ECDD screening identified that Customer 36 was observed accepting unknown quantities of cash from Customer 29 before the two individuals made a chip purchase of $7,000 and $5,000 respectively using only $50 notes. Customer 36 engaged in no table game play on this day. The conduct was identified as a suspected attempt at third-party structuring.

On 15 December 2020, the ECDD screening in respect of Customer 29 identified:

a. that Customer 29 had consistently utilised other patrons to perform large transactions on their behalf, structured transactions and gambled at a level not commensurate with their source of income;

b. that Customer 29's family network included individuals who had been convicted of drug trafficking;

c. the source of funds and source of wealth concerns raised in paragraph 953.l above, including that:

i. although Customer 29 stated that they had recently sold their house and business, none of those details could be verified by SCA;

ii. Customer 29 declined to provide any documentation to support the information provided in the Source of Funds Declaration Form;

iii. open source real estate websites indicated that the property referred to in Customer 29's declaration form was sold by private treaty for $350,000 in June 2020, having been purchased in April 2019 for $355,000;

iv. Customer 29 advised SCA that they were using Person 19's money to gamble as well as savings from their meatpacking job; and

v. Customer 29 advised SCA that their player group used an informal loan club and had a large pool of funds to draw from per month; and

d. online court lists containing the names of Customer 29 and Person 19.

On 24 March 2021, the ECDD screening in respect of Customer 29 identified the same issues as the ECDD dated 15 December 2020.

On 31 March 2021, SCA issued a ban in respect of Customer 29. After Customer 29 was banned, SCA made the decision to ban other customers who were known associates of Customer 29.

The ECDD conducted by SCA did not have appropriate regard to Customer 29's higher ML/TF risks: see *Customer 29's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 29's source of funds or source of wealth.

By reason of the matters set out in *Customer 29's risk profile* above, there were higher ML/TF risks associated with Customer 29's source of wealth or source of funds.

b. on any occasion prior to December 2020 that senior management considered the higher ML/TF risks posed by Customer 29 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 29 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

See paragraph 953.l above.

Customer 29 was mentioned in a 'Transaction Monitoring Overview' report for the period 1 August 2019 to 1 November 2019 which was

provided to SCA's Senior Management Group for discussion at its meeting. The report noted that Customer 29 received three cheques from SCA in September 2019 for $55,000, $40,000 and $90,000. The report also recorded that Customer 29 had a total turnover of $3,200,000 and a small win for the month.

However, it was not until 23 March 2021 that an SCA AML Analyst emailed a memorandum to the SCA Chief Operating Officer, the SCA General Counsel and Company Secretary and the SCA General Manager Legal, Compliance & Regulatory Affairs / Executive Manger recommending that SCA discontinue its business relationship with Customer 29.

The memorandum reported that Customer 29's risk rating had been escalated to 'significant risk' after they were unable to provide adequate information about their source of wealth. The memorandum also cited broader concerns about Customer 29's behaviours at SCA that had been observed by SCA frontline staff and subsequently reviewed in investigations, and their close family connections to convicted drug traffickers.

The SCA Chief Operating Officer and the SCA General Counsel and Company Secretary agreed with the SCA AML Analyst's recommendation to discontinue SCA's business relationship with Customer 29. The SCA General Counsel and Company Secretary also observed that Customer 29's spouse Person 19 would likely be considered a significant risk, referring to the sentencing remarks from their recent conviction that referred to their gambling addiction as a driver of their criminal offending.

On 25 March 2021, the SCA Senior Gaming Operations Shift Manager notified SCA staff that, based on a decision by Senior Management, Customer 29 was not allowed to participate in gambling activity at SCA. Shortly after, Customer 29 was observed performing two players cuts at a table in the Grange Room before SCA staff advised them of their restricted play.

On 31 March 2021, SCA issued a ban in respect of Customer 29.

Contravention of s 36 of the Act in respect of Customer 29

962. By reason of the matters pleaded at paragraphs 950 to 961 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 29 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

963. By reason of the matters pleaded at paragraph 962, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 31 March 2021 with respect to Customer 29.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 30

964. Customer 30 was a customer of SCA during the relevant period. Between 7 December 2016 and June 2021, SCA recorded turnover exceeding $34,000,000 for Customer 30.

Particulars

Customer 30 was a customer of SCA from at least 7 September 2004.

On 9 August 2021, SCA issued a ban in respect of Customer 30 at the direction of the AML team.

965. SCA provided Customer 30 with designated services within the meaning of table 3, s 6 of the Act during the relevant period.

Particulars

Prior to 7 December 2016, SCA opened an FMA for Customer 30 which remained open as at 28 October 2022. (item 11, table 3, s 6 of the Act).

See *Customer 30's risk profile* below.

966. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 30.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 30's risk profile

967. On and from 7 December 2016, Customer 30, and the provision of designated services to Customer 30 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 30's risk profile prior to the relevant period

a. by 7 December 2016, Customer 30 had the following risk history:

   i. SCA had formed suspicions for the purposes of s 41 of the Act with respect to Customer 30;

Particulars

SCA gave the AUSTRAC CEO an SMR on two occasions between 24 April 2009 and 27 September 2016 pertaining to Customer 30.

The SMRs reported that:

a. on 24 April 2009, Customer 30 swapped chips with two other SCA customers, including Person 20: SMR dated 24 April 2009; and

b. on 26 September 2016, Person 20 bought in to play at a table for $9,400. Person 20 then handed $2,000 in cash to Customer 30, who bought in at another table, to avoid the transaction reporting threshold: SMR dated 27 September 2016. This transaction was indicative of the ML/TF typology of structuring.

ii. Customer 30 received high value gambling services (table 3, s 6 of the Act) at SCA other than through junket programs;

Particulars

Between 2004 and 2011, Customer 30's recorded individual gambling activity at SCA was estimated as a buy-in of $2,376,935 for table games, and for table games and EGMs, turnover of $11,663,256 with losses of $370,605.

Customer 30 did not attend SCA from 2012 until mid-2016.

In June 2016 and July 2016, Customer 30's recorded individual rated gambling activity for table games at SCA was an estimated buy-in of $1,200, turnover of $4,250 with losses of $300.

iii. Customer 30 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 7 May 2009 and 21 February 2011, SCA gave the AUSTRAC CEO 20 TTRs detailing incoming and outgoing payments made by Customer 30 totalling $308,912, including:

a. 19 TTRs totalling $292,295 in chip and cash exchanges; and

b. one TTR totalling $16,617 for an EGM payout.

iv. Customer 30, and persons associated with them, engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including structuring; and

Particulars

See paragraph 24 above.

See particulars to paragraph 967.a.i above.

v. in 2011, Customer 30 voluntarily excluded themselves from SCA;

Particulars

On 1 March 2011, Customer 30 informed SCA that they wanted to self-exclude themselves from the casino. Customer 30 completed the required documentation and Customer 30 was self-excluded.

The self-exclusion was rescinded on 22 March 2012.

Customer 30's risk profile during the relevant period

b. Customer 30 received high value gambling services (table 3, s 6 of the Act) at SCA other than through junket programs. Between 2018 and 2021, SCA recorded an estimated buy-in of $4,516,273, turnover of $34,188,422 for Customer 30, with cumulative losses of $1,441,272;

Particulars

In 2018, Customer 30's recorded individual rated gambling activity for table games at SCA was estimated as a buy-in of $77,860, turnover of $250,452 with losses of $22,010.

In 2019, Customer 30's recorded individual rated gambling activity at SCA escalated to an estimated buy-in of $287,200 for table games, and for both table games and EGMs, turnover of $950,339 with losses of $75,771.

In 2020, despite closures related to the COVID-19 pandemic, Customer 30's recorded individual rated gambling activity at SCA significantly escalated to an estimated buy-in of $2,819,690 for table games, and for both table games and EGMs, turnover of $13,230,619 with losses of $869,437.

In 2021, Customer 30's recorded individual rated gambling activity at SCA remained high with an estimated buy-in of $2,655,700 for table games, and for both table games and EGMs, turnover of $19,757,012 with losses of $474,054.

Between 8 August 2020 and 26 March 2021, Customer 30 was listed in SCA's 'Early Gaming Report' as a significant player on either table games or EGMs on at least 80 occasions.

c. from at least April 2019, SCA was aware that Customer 30 was associated with customers – including Customer 29, Customer 32, Customer 33, Customer 34, Customer 35, Customer 36, Customer 37 and other customers in respect of whom SCA had formed suspicions, including Person 20 and Person 33 – who conducted transactions involving the receipt and movement of significant amounts of cash with no apparent economic or visible lawful purpose;

i. the provision of designated services to Customer 30 and their associates by SCA raised red flags reflective of higher ML/TF risks;

Particulars

Red flags reflective of higher ML/TF risks included:

a. conducting several cash and chips exchanges: SMRs dated 24 August 2020, 8 September 2020, 15 September 2020 and 7 April 2021;

b. exchanging cash for chips on multiple gaming Cashiers, tables or Cages in several transactions: SMRs dated 24 August 2020, 15 September 2020 and 5 February 2021;

c. conducting separate cash and chip transactions below the reporting threshold in quick succession: SMRs dated 26 April 2019, 6 August 2020, 24 August 2020, 15 September 2020, 21 January 2021, 5 February 2021 and 7 April 2021;

d. handing chips or cash to one another: SMRs dated 6 August 2020, 24 August 2020, 8 September 2020, 15 September 2020, 21 January 2021, 5 February 2021 and 7 April 2021;

e. placing cash and chips into items such as envelopes and handbags: SMRs dated 24 August 2020, 15 September 2020 and 5 February 2021;

f. concealing cash and chips in their clothing, including in their pockets and beneath their jackets: SMRs dated 24 August 2020 and 8 September 2020;

g. entering and exiting the SCA toilets at the same or similar time, sometimes while carrying cash and chips: SMRs dated 24 August 2020, 15 September 2020, 5 February 2021 and 7 April 2021;

h. conducting cash exchanges in the SCA toilets: SMR dated 6 August 2020;

i. conducting cash transactions using cash that was in an unusual condition, including cash that had a strong aroma of dirt and cash that was damp and odorous: SMRs dated 21 January 2021 and 7 April 2021; and

j. using ATM facilities to conduct significant cash transactions in quick succession: SMR dated 7 April 2021.

ii. SCA formed suspicions in respect of the conduct of Customer 30 and their associates; and

Particulars

SCA considered it suspicious that:

a. Customer 30 and their associates conducted transactions that were not supported by gambling activity: SMRs dated 24 August 2020 and 15 September 2020;

b. Customer 30 and their associates conducted transactions indicative of ML/TF typologies and vulnerabilities, including structuring, refinement and layering: SMRs dated 26 April 2019, 6 August 2020, 24 August 2020, 21 January 2021 and 5 February 2021;

c. Customer 30 and their associates were conducting third party transactions on behalf of other customers, sometimes to misrepresent the origin and destination of the funds and hide the ultimate source of the funds: SMRs dated 6 August 2020, 24 August 2020, 8 September 2020, 15 September 2020, 21 January 2021 and 5 February 2021;

d. Customer 30 and their associates, were conducting transactions and gambling at a level that was inconsistent with their stated occupation: SMRs dated 24 August 2020, 8 September 2020, 15 September 2020 and 7 April 2021; and

e. SCA understood that some of Customer 30's associates had family ties to criminals, including associations with known drug dealers: SMRs dated 8 September 2020, 15 September 2020 and 7 April 2021.

iii. Customer 30 and their associates engaged in a series of large cash, chip and other exchange transactions with no visible purpose.

Particulars

Cash to chip transactions

On 11 September 2020, Customer 30 engaged in a cash to chip exchange transaction with SCA totalling $6,000.

Between 14 August 2020 and 20 March 2021, SCA identified that Customer 30's associates (which included Customer 30, Customer 29, Customer 32, Customer 33, Customer 34, Customer 35, Customer 36 and Customer 37) engaged in 14 cash to chips exchange transactions with SCA totalling $163,450.

Chip to cash transactions

Between 14 August 2020 and 28 January 2021, Customer 30 engaged in four chip to cash exchange transactions with SCA totalling $58,930.

Between 26 April 2019 and 28 January 2021, SCA identified that Customer 30's associates engaged in five chip to cash exchange transactions with SCA totalling $15,590.

Cash handovers

On 20 March 2021, SCA identified that Customer 30 engaged in a cash handover with another SCA customer involving $4,500. On 18 January 2021, SCA identified that Customer 30 appeared to be involved in a cash handover of an unknown amount with another SCA customer.

Between 26 April 2019 and 21 March 2021, SCA identified that Customer 30's associates engaged in at least four cash handovers with other customers totalling at least $19,000.

Chip handovers

Between 26 April 2019 and 20 March 2021, SCA identified that Customer 30 had engaged in at least 16 chip handovers with other customers totalling at least $112,800.

Between 26 April 2019 and 20 March 2021, SCA identified that Customer 30's associates engaged in at least 12 chip handovers with other customers totalling at least $62,000.

Other transactions

Between 11 September 2020 and 18 January 2021, Customer 30 colour changed chips totalling $15,000 at SCA.

d. Customer 30 engaged in a series of other large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

Particulars

On 17 February 2021, Customer 35 gave $10,000 in cash to Customer 30 at SCA. Customer 30 then passed the cash to another SCA customer, Person 21. Person 21 exchanged the cash for cash chips. Person 21 kept $1,000 in cash chips for themselves, and gave the remaining $9,000 in chips to Customer 30. Customer 30 passed $5,000 of the cash chips to Customer 35. Person 21 then handed the remaining $1,000 in chips to an unknown customer, who passed them to Customer 30. A few hours later, Customer 30 received $30,000 in cash chips from Customer 29 and proceeded to exchange the chips for cash in the Grange Room.

On 30 March 2021, an SCA customer exchanged $13,000 in cash for cash chips at SCA. Shortly before the buy-in, the customer was observed entering the Grange Room toilets with Customer 29. Following the buy-in, the customer handed the cash chips to Customer 32. Customer 32 then proceeded to game with the chips. Following Customer 32's first $4,000 winning wager, they handed a $1,000 cash chip to Customer 30. Customer 30 handed the chip to another customer who proceeded to cash it out. The customer then split the cash with another customer.

e. designated services provided to Customer 30 included substantial EGM activity at SCA;

Particulars

See paragraphs 352 and 353 above.

Between 2019 and 2021, Customer 30's recorded individual rated gambling activity for EGMs at SCA was estimated as a turnover of $425,667 with losses of $19,354.

f. Customer 30, and persons associated with them, transacted using large amounts of cash and cash that appeared suspicious, including large volumes of cash in small notes and notes that were sticky at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 17 August 2018 and 3 August 2021, SCA gave the AUSTRAC CEO 63 TTRs detailing incoming and outgoing payments made by Customer 30 totalling $971,860, which comprised:

a. 62 TTRs totalling $960,860 in chip and cash exchanges; and

b. one TTR totalling $11,000 for an EGM payout.

Large and suspicious cash transactions

See particulars to paragraphs 967.c and 967.d above.

g. Customer 30, and persons associated with them, engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including structuring;

Particulars

See paragraph 24 above.

See particulars to paragraph 967.c above.

On 24 August 2018, Customer 30 cashed out $5,000 in chips belonging to Person 33. SCA considered that Customer 30 and Person 33 were attempting to avoid the transaction reporting threshold, as Person 33 had a total of $11,100 in chips.

h. Customer 30 had access to private gaming rooms at SCA; and

Particulars

See paragraph 145(e) above.

Customer 30 had access to private gaming rooms at SCA, including the Black Room, Grange Room, Opal Room and the Platinum Room.

i. SCA did not have adequate reason to believe that Customer 30's source of wealth or source of funds was sufficient to explain the high value gambling services (table 3, s 6 of the Act) provided to Customer 30 by SCA.

Particulars

See paragraph 516 above.

By at least 8 August 2020, SCA understood that Customer 30's occupation was as a café worker: SMR dated 8 August 2020.

Between 24 August 2020 and 15 September 2020, SCA reported in three SMRs given to the AUSTRAC CEO that Customer 30's source of wealth and source of funds did not justify the size of Customer 30's transactions at SCA: see particulars to paragraphs 967.c above. One of the SMRs also noted that Customer 30's spouse, Customer 36, was gaming at a level which was not commensurate with their reported occupation as unemployed.

By September 2020, SCA was aware that Customer 30 was part of a network of associates that had family ties to criminals, and was associated with known drug dealers.

On 27 November 2020, an SCA AML Advisor requested that Customer 30 complete a Source of Funds Declaration, because Customer 30's stated occupation was not commensurate with their level of gambling activity, as well as broader concerns around their behaviour and history.

On 14 December 2020, Customer 30 completed the Source of Funds Declaration Form. Customer 30 stated that they worked as a chef at a restaurant, and confirmed that their income from this employment was their primary source of funds.

On 25 January 2021, an SCA AML Advisor suggested that Customer 30 complete a Source of Wealth Declaration. The AML Advisor noted that Customer 30's level of turnover, loss and available cash appeared incompatible with their stated occupation of working as a cook at a small restaurant.

However, SCA did not request source of wealth information from Customer 30 until 9 August 2021. On the same date, SCA banned Customer 30 from attending the casino until an assessment of their Source of Wealth Declaration was completed. Customer 30 declined to provide this information.

By 7 December 2016, SCA had recorded turnover for Customer 30 exceeding $11,500,000. Between 2018 and 2021, SCA recorded turnover for Customer 30 exceeding $34,000,000.

At no time was SCA's understanding of Customer 30's source of wealth or source of funds commensurate with the high gambling services that they received at SCA.

SCA's determination of the ML/TF risks posed by Customer 30

968. On and from 26 September 2016, Customer 30 was appropriately rated by SCA as a high risk customer for the purpose of the Act and Rules.

969. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 30 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by it with respect to Customer 30.

Monitoring of Customer 30's transactions

970. At no time did SCA apply appropriate transaction monitoring to Customer 30's transactions because SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

The review, update and verification of Customer 30's KYC information

971. SCA did not review, update or verify Customer 30's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 30, including the nature, extent and purpose of their transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 30's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 30's risk profile* above, there were higher ML/TF risks associated with Customer 30's source of wealth or source of funds.

Despite several SMRs reporting that Customer 30's source of wealth or source of funds did not justify the size of Customer 30's transactions at SCA, SCA did not request source of wealth information from Customer 30 until August 2021: see particulars to paragraph 967.i above.

d. to the extent that SCA reviewed Customer 30's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 30.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

ECDD triggers in respect of Customer 30

972. SCA was required to apply the ECDD program to Customer 30 following any ECDD triggers in respect of Customer 30.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

973. Customer 30 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 26 April 2019 and 7 April 2021, SCA gave the AUSTRAC CEO eight SMRs with respect to or pertaining to Customer 30.

b. determined to be high risk by SCA for the purpose of the Act and Rules prior to the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 30* above.

974. Each matter pleaded in paragraph 973 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

975. SCA did not conduct appropriate risk-based ECDD with respect to Customer 30 following an ECDD trigger because:

a. on each occasion prior to August 2021 that SCA conducted ECDD in respect of Customer 30 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 30 and failed to appropriately consider whether the ML/TF risks posed by Customer 30 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501, 511 and 516 to 517 above.

Watchlist alerts

On 13 November 2018, SCA conducted a PEP screening for Customer 30.

Between 16 August 2018 and 18 August 2021, SCA received four open source Dow Jones watchlist alerts in respect of Customer 30.

Transaction reviews

Between April 2019 and April 2021, SCA conducted surveillance reviews of transactions involving Customer 30 at SCA on eight occasions. On each occasion, SCA AML Advisors were advised of the findings.

Premium player review

On 14 September 2019, SCA upgraded Customer 30 to premium status. Due to Customer 30's previous self-exclusion from the casino, SCA conducted a three-month review of Customer 30's gaming. This review related to Customer 30's spending and did not consider any ML/TF risks.

ECDD screenings

On 4 September 2020 and 19 November 2020, SCA conducted ECDD in respect of Customer 30. The ECDD screenings in respect of Customer 30 identified that:

a. Customer 30 had been the subject of four SMRs given to the AUSTRAC CEO that involved them acting as a third party to

assist in structuring transactions, receiving funds as a third party as part of a potential layering strategy, and being present while associates conducted suspicious transactions;

b. Customer 30's listed occupation was as a café worker;

c. Customer 30 had a number of known associates at SCA; and

d. there was no open source information available on Customer 30.

Further ECDD screening conducted in early August 2021 in respect of Customer 30 also identified that:

a. Customer 30's family network included individuals that had been convicted of drug dealing. SCA was concerned that Customer 30 was being utilised by family members to help structure transactions and gamble at a level not commensurate with Customer 30's source of income;

b. Customer 30's listed source of income had been as a café worker since they opened their SCA account in 2004, and their spouse Customer 36's occupation was listed as unemployed;

c. in addition to the SMRs of which Customer 30 had been the subject, on several occasions Customer 30's known associates had presented cash that was soiled with a strong aroma of dirt. Customer 30 then received chips from these associates after the cash exchange;

d. Customer 30 had been present for multiple suspicious transactions in 2020 and 2021 between known associates, including Customer 29; and

e. SCA's daily logs indicated that Customer 30 had cashed out transactions that did not reflect their level of play and cash buy-in.

Following this ECDD screening, it was recommended that SCA obtain a completed Source of Wealth Declaration from Customer 30 and terminate its business relationship with them.

Source of wealth ECDD

On 9 August 2021, SCA conducted a review of its customer relationships. As part of this assessment, SCA requested source of wealth information from Customer 30 and banned them from the casino pending provision of this information.

Until August 2021, the ECDD conducted by SCA did not have appropriate regard to Customer 30's higher ML/TF risks: see *Customer 30's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 30's source of funds or source of wealth.

By reason of the matters set out in *Customer 30's risk profile* above, there were higher ML/TF risks associated with Customer 30's source of wealth or source of funds.

On 9 August 2021, SCA issued a ban in respect of Customer 30.

After Customer 30 was banned, SCA made the decision to ban Customer 34 due to their association with Customer 30.

b. at no time prior to August 2021 did senior management consider the higher ML/TF risks posed by Customer 30 in response to an ECDD trigger, or appropriately consider whether the ML/TF risks posed by Customer 30 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

On 4 August 2021, an SCA AML Compliance Manager advised the Chief Operating Officer Australia that they had prepared letters to issue to Customer 30 and nine other customers requesting further information about their source of wealth.

On 5 August 2021, the Chief Operating Officer Australia queried how these customers had been identified, and whether SCA intended to terminate its business relationship with Customer 30 and the other customers immediately.

The AML Compliance Manager confirmed that SCA would effectively cease doing business with Customer 30 until a response to the letter had been received and reviewed.

On 9 August 2021, SCA issued a ban in respect of Customer 30.

Contravention of s 36 of the Act in respect of Customer 30

976. By reason of the matters pleaded at paragraphs 964 to 975 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 30 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

977. By reason of the matters pleaded at paragraph 976, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 9 August 2021 with respect to Customer 30.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 31

978. Customer 31 was a customer of SCA during the relevant period. Between 2016 and 2021, SCA recorded turnover exceeding $30,000,000 for Customer 31.

Particulars

Customer 31 was a customer of SCA from at least 1 July 2015.

On 9 August 2021, SCA issued a ban in respect of Customer 31 at the direction of the SCA AML team.

979. SCA provided Customer 31 with designated services within the meaning of table 3, s 6 of the Act during the relevant period.

Particulars

By 7 December 2016, SCA had opened an FMA for Customer 31 which remained open as at 28 October 2022 (item 11, table 3, s 6 of the Act).

Customer 31's risk profile below.

980. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 31.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 31's risk profile

981. On and from 7 December 2016, Customer 31, and the provision of designated services to Customer 31 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 31's risk profile prior to the relevant period

a. by 7 December 2016, Customer 31 had the following risk history:

   i. SCA had formed suspicions for the purposes of s 41 of the Act with respect to Customer 31;

Particulars

SCA gave the AUSTRAC CEO an SMR in respect of Customer 31 on 5 October 2013 and 25 November 2013.

These SMRs reported that Customer 31 engaged in transactions indicative of the ML/TF typology of structuring and suspicious transactions with other customers: see paragraphs 981.a.v and 981.a.vi below.

   ii. SCA recorded high turnover of $14,157,648 for Customer 31 with cumulative losses of $665,121;

Particulars

Between 1 January 2001 and 31 December 2015, Customer 31's recorded individual rated gambling activity at SCA was estimated as a buy-in of $3,928,605 for table games, and for both table games and EGMs, turnover of $14,157,648 with losses of $665,121.

iii. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 31 by remitting large amounts of money into and out of the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

On 26 October 2016, SCA accepted instructions to transfer $15,000 from Customer 31's FMA to their personal bank account overseas.

On 31 October 2016, one week later, SCA received a telegraphic transfer of $15,000 from Customer 31's personal bank account overseas, which it made available to Customer 31's FMA.

iv. designated services provided to Customer 31 included substantial EGM activity at SCA;

Particulars

See paragraphs 352 and 353 above.

For example, on 17 August 2014, Customer 31 received an EGM payout of $10,380.

v. SCA was aware that Customer 31 had engaged in patterns of transactions with another customer and an unknown person which had no apparent economic or visible lawful purpose;

Particulars

On 24 November 2013, Customer 31 acted in concert with Person 33 and an unknown person to conduct a series of chip and cash exchanges under the transaction reporting threshold and Customer 31 passed cash to Person 33 under a table and outside of the view of SCA's surveillance cameras: SMR dated 25 November 2013.

vi. Customer 31 transacted using large amounts of cash at SCA; and

Particulars

See paragraphs 376 to 381 above.

Between 4 October 2013 and 1 November 2016, SCA gave the AUSTRAC CEO eight TTRs detailing incoming and outgoing payments made by Customer 31 totalling $105,380, which comprised:

a. three TTRs totalling $60,380 in cash and chip exchanges;

b. two TTRs totalling $30,000 in account deposits;

c. one TTR totalling $15,000 for an account withdrawal;

d. one TTR totalling $10,379 for an EGM payout; and

e. one TTR totalling $10,000 for a casino prize.

On 1 November 2016, Customer 31 withdrew a $15,000 chip purchase voucher from their FMA at SCA.

vii. Customer 31 engaged in transactions indicative of ML/TF typologies and vulnerabilities, including structuring and quick turnover of money (without betting).

Particulars

See paragraph 24 above.

Between 4 October 2013 and 12 September 2016, Customer 31 engaged in at least nine transactions indicative of the ML/TF typology of structuring totalling $40,800: see paragraph 981.a.v above.

On 25 October 2016, Customer 31 engaged in two transactions indicative of the ML/TF typology of quick turnover of money (without betting) totalling $30,000: see paragraph 981.a.iii above.

Customer 31's risk profile during the relevant period

b. Customer 31 received high value gambling services (table 3, s 6 of the Act) at SCA other than through junket programs. Between 2016 and 2021, SCA recorded an estimated buy-in of $10,883,827, a turnover estimated at $30,347,505 for Customer 31, with cumulative losses of $354,815;

Particulars

In 2016, Customer 31's recorded individual rated gambling activity at SCA was estimated as a buy-in of $1,259,407 for table games, and for both table games and EGMs, turnover of $4,223,372 with losses of $93,165.

In 2017, Customer 31's recorded individual rated gambling activity at SCA was estimated as a buy-in of $1,945,455 for table games, and for both table games and EGMs, turnover of $5,008,842 with losses of $84,548.

In 2018, Customer 31's recorded individual rated gambling activity at SCA was estimated as a buy-in of $2,091,695 for table games, and for both table games and EGMs, turnover of $5,162,764 with losses of $9,947.

In 2019, Customer 31's recorded individual rated gambling activity at SCA was estimated as a buy-in of $2,388,300 for table games, and for both table games and EGMs, turnover of $5,696,324 with losses of $42,397.

In 2020, despite closures related to the COVID-19 pandemic, Customer 31's recorded individual rated gambling activity at SCA remained high. It was estimated as a buy-in of $1,861,130 for table

games, and for both table games and EGMs, turnover of $5,205,748 with losses of $67,904.

Between 1 January 2021 and 9 August 2021, Customer 31's recorded individual rated gambling activity at SCA was estimated as a buy-in of $1,356,515 for table games, and for both table games and EGMs, turnover of $5,050,455 with losses of $56,854.

c. from at least June 2018, SCA was aware that Customer 31 was associated with customers – including Customer 2, Customer 21, Customer 27, Customer 29, Customer 39, Customer 31's spouse (Person 7), and child (Person 21), and another customer in respect of whom SCA had formed suspicions, Person 2 – who conducted transactions involving the receipt and movement of significant amounts of cash with no apparent economic or visible lawful purpose;

   i. the provision of designated services to Customer 31 and their associates by SCA raised red flags reflective of higher ML/TF risks;

Particulars

Red flags reflective of higher ML/TF risks included:

a. exchanging cash for chips on multiple gaming Cashiers, tables or Cages in several transactions: SMRs dated 25 May 2018 and 18 June 2018;

b. conducting separate cash and chip transactions below the reporting threshold in quick succession: SMRs dated 25 May 2018 and 18 June 2018;

c. handing chips or cash to one another: SMRs dated 25 May 2018, 13 June 2018, 18 June 2018, 11 January 2019, 7 February 2019 and 15 May 2019;

d. handing unknown items to one another: SMR dated 18 June 2018;

e. placing cash and chips into items such as envelopes, handbags, satchels, plastic bags, reusable bags, and wrapped jackets and bundles, or instructing SCA employees to do the same: SMRs dated 25 May 2018, 13 June 2018, 18 June 2018, 11 January 2019, 7 February 2019, 15 May 2019, 15 August 2019 and 8 November 2019;

f. exchanging these cash-filled items between each other, including by passing them under tables, leaving them in open spaces and then signalling each other, and hiding them behind cushions on the couches in private gaming rooms: SMRs dated 25 May 2018, 13 June 2018, 18 June 2018, 11 January 2019 and 15 May 2019;

g. concealing cash and chips in their pockets and in their jackets: SMRs dated 18 June 2018, 18 April 2019, 15 May 2019, 15 August 2019 and 8 November 2019;

h. making and receiving phone calls at identical times and then conducting cash and chip exchanges shortly thereafter: SMRs dated 18 June 2018, 18 April 2019, 15 May 2019, 15 August 2019 and 8 November 2019;

i. carrying significant amounts of cash and chips into the SCA toilets away from the view of surveillance cameras, and sometimes swapping the cash between different carrying items inside the toilets: SMRs dated 13 June 2018, 18 June 2018, 11 January 2019, 7 February 2019, 15 May 2019, 15 August 2019, 18 September 2019, 3 October 2019 and 8 November 2019;

j. conducting significant cash and chip exchanges in the SCA toilets: SMRs dated 18 June 2018, 7 February 2019, 18 April 2019, 15 May 2019, 15 August 2019, 18 September 2019, 3 October 2019 and 8 November 2019;

k. depositing significant amounts of cash in the SCA toilets: SMR dated 7 February 2019;

l. using their bodies to hide chip and cash exchanges from the view of surveillance cameras: SMR dated 18 June 2018;

m. using EFTPOS facilities to conduct significant numbers of cash transactions in quick succession: SMR dated 25 May 2018;

n. withdrawing large amounts of cash from FMAs: SMR dated 11 January 2019; and

o. removing significant amounts of chips from SCA: SMR dated 18 April 2019.

ii. SCA formed suspicions in respect of the conduct of these customers; and

Particulars

SCA considered it suspicious that:

a. Customer 31 and their associates conducted transactions that were not supported by gambling activity: SMRs dated 25 May 2018, 13 June 2018, 18 June 2018, 11 January 2019, 18 April 2019, 18 September 2019, 3 October 2019 and 8 November 2019;

b. Customer 31 carried a significant quantity of chips for the purpose of lending or loaning funds to players in the group who gamed at significant levels: SMR dated 18 September 2019;

c. Customer 31 and their associates conducted transactions indicative of ML/TF typologies and vulnerabilities, including structuring, cashing-in large value chips with no evidence of play and loan sharking: SMRs dated 25 May 2018, 18 June

2018, 15 August 2019, 18 September 2019, 3 October 2019 and 8 November 2019;

d. Customer 31 and their associates conducted transactions that had no identifiable purpose and where the original source of funds was not clear: SMRs dated 13 June 2018, 18 June 2018 and 18 April 2019;

e. Customer 31 and their associates did not appear to be at SCA for gaming-related purposed. Rather, a factor other than gaming was the driving factor between their exchanges: SMRs dated 18 June 2018, 18 April 2019 and 15 May 2019;

f. Customer 31 and their associates conducted transactions in a secretive manner that was designed to conceal and disguise their associations, and distance themselves and their motives from the transactions, by using agents and family members, initiating transactions through phone calls, and by conducting transactions with minimal contact and in settings such as the SCA toilets or other places away from SCA employees and gaming tables: SMRs dated 18 June 2018, 11 January 2019, 18 April 2019, 15 May 2019 and 8 November 2019;

g. SCA was not aware of connections or associations between some of Customer 31's associates, including between Customer 31 and Customer 2, and between Customer 31's associates and customers with whom they conducted transactions: SMR dated 18 June 2018;

h. Customer 31 and their associates appeared to be engaged in money lending between themselves, and with other customers, but sometimes did not receive repayments: SMRs dated 25 May 2018, 13 June 2018, 18 June 2018 and 15 May 2019;

i. Customer 31 and their spouse, Person 7, were in frequent contact with other SCA customers, including Customer 2, Customer 27 and Customer 29, who had previously engaged in behaviour indicative of money laundering and which SCA had reported to the AUSTRAC CEO: SMRs dated 25 May 2018 and 15 May 2019; and

j. SCA understood that Customer 31 and their associates, including Customer 29, had strong family associations with customers who had been previously arrested for drug trafficking offences: SMR dated 25 May 2018.

iii. Customer 31 and their associates engaged in a series of large cash, chip and other exchange transactions with no visible lawful purpose;

Particulars

Cash to chip transactions

On 22 May 2018, Customer 31 engaged in two cash to chip exchange transactions with SCA totalling $5,000.

Between 22 May 2018 and 13 June 2018, SCA identified that Customer 31's associates have engaged in five cash to chip exchange transactions with SCA totalling $95,000.

Cash handovers

Between 9 June 2018 and 7 November 2019, SCA identified that Customer 31 had appeared to engage in at least 12 cash handovers with other customers totalling at least $871,000.

On 24 January 2019, SCA identified that Customer 31's associates had appeared to engage in at least six cash handovers with other customers totalling at least $572,200.

Chip handovers

Between 22 May 2018 and 1 October 2019, SCA identified that Customer 31 had appeared to have engaged in at least three chip handovers with other customers totalling $563,000.

On 22 May 2018, SCA identified that Customer 31's associates had appeared to engage in at least two chip handovers with other customers totalling at least $10,000.

d. Customer 31 was engaged in a series of other large and unusual transactions and patterns of transactions and activity, which had no apparent economic or visible lawful purpose;

Particulars

On 25 November 2019, SCA recorded suspicious behaviour between Customer 31 and Person 2. SCA suspected that Customer 31 and Person 2 conducted a chip exchange in the SCA toilets, but concluded that it could not confirm any exchange.

On 8 March 2021, SCA recorded that Customer 31 accompanied Person 6 into the SCA toilets, which it noted was consistent with their pattern of suspicious behaviour, but SCA did not record any exchange.

On 22 April 2021, Customer 31 handed $9,000 in $50 notes to another SCA customer. Immediately prior to this transaction, and over the course of the next hour, the customer and three of their associates conducted five other chip and cash exchange transactions below $10,000 between themselves and with SCA, totalling $36,000. SCA considered these transactions below the threshold amount to be indicative of layering and may have indicated a general avoidance of the transaction threshold reporting requirement. SCA noted that these transactions were not supported by the gambling activity of any of the

customers for the day, that neither Customer 31 nor any of the other customers recorded threshold transactions in April 2021, and that it was not aware of any association between Customer 31 and the other customers: SMR dated 21 May 2021.

e. designated services provided to Customer 31 included substantial EGM activity at SCA;

Particulars

See paragraphs 352 and 353 above.

Between 24 January 2017 and 23 June 2019, Customer 31 exchanged $10,642 in TITO tickets for cash at SCA in six transactions below the reporting threshold.

Between 26 January 2017 and 5 May 2017, SCA issued $740 in TITO tickets to Customer 31 on three occasions.

On 18 January 2021, Customer 31 recorded a win of over $6,000 on EGM play.

In 2017, Customer 31 recorded turnover of $320,943 with wins of $5,048 on EGMs at SCA.

In 2018, Customer 31 recorded turnover of $291,002 with losses of $6,012 on EGMs at SCA.

In 2019, Customer 31 recorded turnover of $325,439 with losses of $7,192 on EGMs at SCA.

In 2020, despite closures related to the COVID-19 pandemic, Customer 31 recorded turnover of $77,703 with losses of $5,039 on EGMs at SCA.

Between 1 January 2021 and 9 August 2021, Customer 31 recorded turnover of $168,387 with losses of $1,556 on EGMs at SCA.

f. Customer 31 and their associates transacted using large amounts of cash and cash that appeared suspicious, including cash in small denominations, cash covered in dirt, cash contained in a range of different bags and envelopes and counterfeit cash at SCA;

Particulars

See paragraphs 376 to 381 above.

See particulars to paragraphs 981.c and 981.d above.

TTRs

Between 4 December 2017 and 19 April 2017, SCA gave the AUSTRAC CEO two TTRs detailing transactions made by Customer 31 totalling $20,000, which comprised:

a. one TTR totalling $10,000 in account deposits;

b. one TTR totalling $10,000 in account withdrawals.

Between 10 January 2017 and 23 February 2021, Customer 31 deposited a total of $57,367 in cash into their FMA in 61 transactions below the transaction reporting threshold.

Between 22 January 2017 and 19 January 2021, Customer 31 withdrew a total of $59,255 in cash from their FMA in 25 transactions below the reporting threshold.

On 3 December 2017, Customer 31 withdrew a $10,000 chip purchase voucher from their FMA.

Between 29 March 2018 and 30 January 2021, Customer 31 exchanged a total of $191,050 in cash for chips at SCA in 55 transactions below the reporting threshold.

Large and suspicious cash transactions in 2017

On 5 November 2017, an SCA customer presented cash for a buy-in at an SCA gaming table. The cash included a counterfeit $50 note. Customer 31 admitted that they handed the note to the customer prior to the buy-in. SCA subsequently identified two further counterfeit $50 notes in the table's drop box. SCA noted that law enforcement officers attended the premises, concluded that Customer 31 was an innocent party in the matter and had received the note unknowingly, and took no further action.

Large and suspicious cash transactions in 2018

On 1 October 2018, Customer 31 and their spouse, Person 7, exchanged $10,000 in chips for cash in two transactions of $5,000 each at the Platinum Cage. SCA then observed that Customer 31 deliberately attended three different Cage locations during this period to conduct three cash outs under $10,000 despite not participating in any gaming. SCA considered that these transactions had no identifiable purpose and indicated structuring behaviour designed to avoid reporting obligations. SCA concluded that there could be "little doubt" as to Customer 31's intentions: SMR dated 4 October 2018.

On 4 October 2018, after conducting a series of large and suspicious cash transactions, Customer 39 met Customer 31 and Person 7, and handed an unknown amount of chips to Person 7. SCA considered that Customer 39's transactions were suspicious, involving $50 notes that were covered in dirt, and involving multiple buy-ins under $10,000 with little or no gambling activity. SCA noted that Person 7 was an EGMs player and a review of their records between 4 October 2018 and 8 October 2018 indicated that they had not participated in any table games: SMR dated 9 October 2018.

Large and suspicious cash transactions in 2019

On 19 July 2019, SCA staff observed Customer 29 interact with Customer 31 and Customer 39 and then exit SCA's premises. Shortly afterwards, Customer 29 returned to SCA in possession of $70,000 in cash. SCA suspected that they retrieved this cash from their vehicle. SCA considered that this activity was suspicious. Customer 29 was gambling using significant amounts of cash at levels substantially higher than their known source of funds, was associated with suspected drug traffickers and loan sharks, and was involved in third

party payments and transactions indicative of the ML/TF typologies of refining and structuring: SMR dated 24 July 2019.

g. in 2019, Customer 31 was the subject of law enforcement enquiries on at least one occasion at SCA;

Particulars

On 5 November 2019, SCA received a notice from a law enforcement agency seeking information and documents regarding Customer 31 and other customers who were identified as high risk.

h. Customer 31 had access to private gaming rooms at SCA; and

Particulars

See paragraph 145(e) above.

Customer 31 had access to private gaming rooms at SCA, including the Black Room, the Grange Room, the Opal Room and the Platinum Room.

Between 1 January 2018 and 9 August 2021, Customer 31 purchased $201,050 in chips in private gaming rooms at SCA, including the Grange Room and the Platinum Room.

i. SCA did not have adequate reason to believe that Customer 31's source of wealth or source of funds was sufficient to explain the high value gambling services (table 3, s 6 of the Act) provided to Customer 31 by SCA.

Particulars

See paragraph 516 above.

On 15 October 2013, Customer 31 declined to provide information about their occupation to SCA.

On 18 June 2018 and 20 June 2018, SCA recorded that Customer 31 had no occupation and was retired.

On 17 October 2018, SCA staff could not confirm Customer 31's occupation after conducting open source searches.

It was not until August 2021 that SCA again requested source of wealth information from Customer 31 and implemented a ban against them. Customer 31 declined to provide this information.

Between 7 December 2016 and 9 August 2021, Customer 31 recorded an estimated turnover exceeding $25,000,000 for table games at SCA.

At no time was Customer 31's source of wealth or source of funds commensurate with the high value gambling services received by them at SCA. At no time was Customer 31's source of funds verified by SCA.

SCA's determination of the ML/TF risks posed by Customer 31

982. On and from 26 September 2016, Customer 31 was appropriately rated high risk for the purpose of the Act and Rules by SCA.

983. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 31 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by it with respect to Customer 31.

Monitoring of Customer 31's transactions

984. At no time did SCA apply appropriate transaction monitoring to Customer 31's transactions because SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

The review, update and verification of Customer 31's KYC information

985. SCA did not review, update or verify Customer 31's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 31, including the nature, extent and purpose of Customer 31's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 31's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 31's risk profile* above, there were higher ML/TF risks associated with Customer 31's source of wealth or source of funds.

d. to the extent that SCA reviewed Customer 31's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 31.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

ECDD triggers in respect of Customer 31

986. SCA was required to apply the ECDD program to Customer 31 following any ECDD triggers in respect of Customer 31.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1),15.9(3) and 15.10 of the Rules.

987. Customer 31 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 25 May 2018 and 21 May 2021, SCA gave the AUSTRAC CEO 15 SMRs with respect to or pertaining to Customer 31.

b. determined by SCA to be high risk for the purpose of the Act and Rules prior to the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 31* above.

988. Each matter pleaded in paragraph 987 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

989. SCA did not conduct appropriate risk-based ECDD with respect to Customer 31 following an ECDD trigger because:

a. on each occasion prior to 9 August 2021 that SCA conducted ECDD in respect of Customer 31 in response to an ECDD trigger, SCA failed to appropriately consider the ML/TF risks posed by Customer 31 and failed to appropriately consider whether the ML/TF risks posed by Customer 31 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501, 511 and 516 to 517 above.

Between 24 May 2017 and 19 May 2021, SCA conducted ECDD in respect of Customer 31. During this period, SCA was aware that Customer 31 and their associates were engaged in significant quantities of large and coordinated cash transactions that were conducted in highly suspicious circumstances and were indicative of ML/TF typologies, and SCA did not have any identifiable information to justify the wealth and funds that Customer 31 presented.

Database alerts

Between 24 May 2017 and 27 May 2021, SCA received five open source Dow Jones watchlist alerts and five transaction alerts in respect of Customer 31 but resolved to take no further action following manual review conducted by SCA's AML team.

Transaction reviews

Between May 2018 and April 2021, SCA surveillance operators reviewed SCA's records of Customer 31's transactions on 11 occasions. These reviews confirmed that Customer 31 had engaged in suspicious transactions with Customer 2, Customer 27, Customer 29 and Customer 39, along with Person 2, Person 7 and Person 21. SCA AML Analysts subsequently conducted compliance investigations into these transactions, some of which were referred to the SCA General Manager Legal, Compliance & Regulatory Affairs / Executive Manger. On one occasion, these Analysts commented that some of the transactions had no identifiable purpose.

Following these reviews, on or around 9 June 2018, SCA advised Customer 31 that they were not permitted to exchange money on SCA's premises. Despite this, Customer 31 and their associates continued to engage in many transactions that SCA suspected were indicative of money lending, including at least six transactions indicative of loan sharking totalling at least $738,000: see paragraph 981.c above.

ECDD screening

Between June and October 2018, SCA conducted information searches in respect of Customer 31 on three occasions.

Between 22 April 2021 and 19 May 2021, SCA conducted an ECDD screening in respect of Customer 31 on two occasions. This screening consisted of reviews of:

a. Customer 31's source of wealth, recording that they had no occupation and were retired;

b. Customer 31's known associates;

c. Customer 31's gaming history; and

d. SMRs in respect of Customer 31 given to the AUSTRAC CEO between 4 October 2013 and 22 April 2021.

However, it was not until 9 August 2021 that SCA issued a ban in respect of Customer 31.

At the time SCA issued this ban, it conducted a review of its business relationship with Customer 31 and recorded that:

a. surveillance investigations indicated that Customer 31 was a person of interest engaged in money lending and loan sharking behaviour at SCA. The review identified at least 19 such transactions that had taken place between 2013 and 2021;

b. Customer 31 had not provided SCA with adequate documentation to support their current gaming levels. The last request for source of wealth information had been made in 2013;

c. SCA's open source investigations had failed to identify any information to indicate Customer 31's source of funds; and

d. SCA's AML/CTF team recommended that SCA terminate its relationship with Customer 31 on the basis of a lack of appropriate source of wealth documents.

The ECDD conducted by SCA but did not have appropriate regard to the higher ML/TF risks posed by Customer 31: see *Customer 31's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks post by Customer 31 and their source of funds or source of wealth.

By reason of the matters set out in *Customer 31's risk profile* above, there were higher ML/TF risks associated with Customer 31's source of wealth or source of funds.

b. at no time prior to August 2021 did senior management consider the higher ML/TF risks posed by Customer 31 in response to an ECDD trigger, or appropriately consider whether the ML/TF risks posed by Customer 31 were within SCA's ML/TF risk appetite;

Particulars

Rules 15.10(6) and (7) of the Rules.

In August 2021, the SCA Chief Operating Officer requested a review of Customer 31 and nine other customers in respect of whom SCA had formed suspicions.

This review identified that:

a. SCA was not satisfied that it had appropriate source of wealth documents to support Customer 31's gambling activity;

b. SCA had given the AUSTRAC CEO six or more SMRs with respect to Customer 31 since 2016; and

c. Customer 31 was an associate of Customer 29, who had been banned from SCA.

The last SMR in respect of Customer 31 was given to the AUSTRAC CEO on 21 May 2021.

During this period, SCA's AML/CTF team conducted an internal compliance investigation into Customer 31 and recommended that SCA terminate its relationship with Customer 31 on the basis of a lack of appropriate source of wealth documents, noting that they were also a person of interest engaged in money lending and loan sharking behaviour. The behaviour identified dated from at least June 2018.

On 9 August 2021, SCA issued a ban in respect of Customer 31 and sent a letter requesting that they provide information to support their source of wealth.

Contravention of s 36 of the Act in respect of Customer 31

990. By reason of the matters pleaded at paragraphs 978 to 989 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 31 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

991. By reason of the matters pleaded at paragraph 990, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 9 August 2021 with respect to Customer 31.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 32

992. Customer 32 was a customer of SCA during the relevant period. Between 7 December 2016 and 8 August 2021, SCA recorded turnover exceeding $44,000,000 for Customer 32.

Particulars

Customer 32 was a customer of SCA from 17 June 2005.

On 9 August 2021 SCA issued a ban in respect of Customer 32.

993. SCA provided Customer 32 with designated services within the meaning of table 3, s 6 of the Act during the relevant period.

Particulars

On 17 June 2005, SCA opened an FMA for Customer 32 which remained open as at 28 October 2022 (item 11, table 3, s 6 of the Act).

See *Customer 32's risk profile* below.

994. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 32.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 32's risk profile

995. On and from 7 December 2016, Customer 32, and the provision of designated services to Customer 32 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 32's risk profile prior to the relevant period

a. by 7 December 2016, Customer 32 had the following risk history:

   i. SCA had formed suspicions for the purposes of s 41 of the Act with respect to Customer 32;

Particulars

SCA gave the AUSTRAC CEO an SMR pertaining to Customer 32 on 12 occasions between 28 September 2009 and 20 September 2016.

The SMRs reported that Customer 32 structured cash transactions at SCA to avoid the transaction reporting threshold, and avoided cashing out transactions themselves:

a. On 26 September 2009, Customer 32 had their partner (who was not playing at table games) cash out $5,075. Customer 32 then cashed out $6,000 to avoid the transaction reporting threshold.

b. On 7 June 2010, Customer 32 split cash outs totalling $13,000 to avoid the transaction reporting threshold.

c. On 12 March 2011, Customer 32 attempted to split a payout at two different windows by giving chips to an associate (who had not been playing). Customer 32 initially refused to provide identification, but provided their driver's licence when they were told that they could not receive a payout without identification. SCA paid out $9,800 in cash to Customer 32. Customer 32's associate left without cashing out the other $9,000.

d. On 2 June 2012, Customer 32 attempted to have family members (who were not playing) cash out $13,700 in chips on their behalf.

e. On 3 June 2012, another SCA customer, Person 19, cashed out $3,000 cash for Customer 32 at SCA.

f. On 2 November 2013, Customer 32 bought into a game with $9,900 in cash.

ii. SCA was aware that Customer 32 was an associate of known criminals;

Particulars

SCA was aware that two of Customer 32's siblings were banned from SCA for drug related activity: SMR dated 12 August 2016.

SCA was aware that Customer 32 was a member of a family that had extensive links to criminal activity: SMR dated 20 September 2016.

iii. Customer 32 received high value gambling services (table 3, s 6 of the Act) at SCA;

Particulars

From 2005 to 2015, Customer 32 had estimated total buy-in for table games of $41,522,130 and estimated total turnover for both table games and gaming EGMs of $273,197,861.

iv. SCA was aware that Customer 32's turnover and losses were not consistent with their source of wealth;

Particulars

On 3 June 2016, SCA staff observed that Customer 32 was a truck driver, and that since 2012 they had sustained losses of nearly $1,000,000 at SCA. SCA staff observed that Customer 32's spouse was a courier and had lost over $1,100,000 at SCA since 2012. SCA staff observed that Customer 32's spouse's occupation as a courier and Customer 32's occupation as a truck driver could not cover a loss of that size: SMR dated 3 June 2016.

v. Customer 32 transacted using large amounts of cash at SCA.

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 18 August 2009 and 31 October 2016, SCA gave the AUSTRAC CEO 218 TTRs detailing incoming and outgoing payments made by Customer 32 totalling $5,150,336, which comprised:

a. 204 TTRs totalling $4,794,345 in chip and cash exchanges;

b. 11 TTRs totalling $242,000 in account deposits;

c. two TTRs totalling $94,000 in account withdrawals; and

d. one TTR totalling $19,990 for an EGM payout.

Customer 32's risk profile during the relevant period

b. Customer 32 received high value gambling services (table 3, s 6 of the Act) at SCA other than through junket programs. Between 7 December 2016 and 8 August 2021, SCA recorded an estimated buy-in of $6,787,200, a turnover estimated at $44,243,846 for Customer 32, with cumulative losses of $1,402,847;

Particulars

In 2016, Customer 32's recorded individual rated gambling activity at SCA was estimated as a buy-in of $3,104,630 for table games, and for both table games and EGMs, turnover of $22,818,094 with losses of $530,339.

In 2017, Customer 32's recorded individual rated gambling activity at SCA was estimated as a buy-in of $1,410,350 for table games, and for both table games and EGMs, turnover of $9,307,087 with losses of $16,711.

In 2018, Customer 32's recorded individual rated gambling activity at SCA was estimated as a buy-in of $1,072,600 for table games, and for both table games and EGMs, turnover of $5,613,185 with losses of $381,121.

In 2019, Customer 32's recorded individual rated gambling activity at SCA was estimated as a buy-in of $652,600 for table games, and for both table games and EGMs, turnover of $3,982,614 with losses of $88,366.

In 2020, despite closures related to the COVID-19 pandemic, Customer 32's recorded individual rated gambling activity at SCA escalated to an estimated buy-in of $1,438,600 for table games, and for both table games and EGMs, turnover of $10,647,142 with losses of $533,413.

Between January 2021 and August 2021, Customer 32's recorded individual rated gambling activity at SCA further escalated to an estimated buy-in of $2,213,050 for table games, and for both table games and EGMs, turnover of $14,686,651 with losses of $351,833. Customer 32 was banned from SCA on 9 August 2021.

c. By at least August 2020, SCA was aware that:

i. Customer 32 had engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose; and

ii. Customer 32 was connected to other customers at SCA, including players who posed higher ML/TF risks such as Customer 29, Customer 30, Customer 36, Customer 37 and Customer 38, and players who SCA considered had acted suspiciously such as Person 19 and Person 33;

Particulars

Customer 32's connection to customers posing higher ML/TF risks

SCA was aware that Customer 32 was a member of a family with a history of extensive criminal behaviour, including the sale and supply

of heroin. Several members of this family were loyalty members at SCA during the relevant period, including Person 19 and Person 33.

SCA banned two of Customer 32's siblings from SCA due to their extensive criminal histories and drug related offences: see paragraph 995.a.ii above.

SCA formed suspicions about Customer 32's spouse, Person 33, for the purpose of s 41 of the Act; multiple SMRs were submitted by SCA about Person 33 due to their structuring with known associates and family members. SCA staff observed that Person 33's occupation could not support their sustained losses at SCA: see paragraph 995.a.iv above.

Large and unusual transactions involving other customers

On 10 April 2017 and 11 April 2017, SCA staff observed Customer 32 passing chips to other customers, including Customer 29, Person 19 and Person 33, who subsequently cashed out the chips then swapped the cash for chips amongst themselves. This was done in a covert way, including Customer 29 placing the cash into their undergarments and storing cash in their pants.

On 14 August 2020, Customer 32, Customer 37 and Person 23 arrived at SCA together. The three patrons separated. Customer 37 exchanged $10,000 in cash for chips, and Person 23 exchanged $9,000 in cash for chips. Person 23 then gave Customer 37 an unknown amount of chips. Customer 37 subsequently approached Customer 32 and placed a number of chips into Customer 32's pocket. Around 20 minutes later, Person 23 handed Customer 32 $10,000 in chips, which Customer 32 used for gaming. Customer 32 won $20,000, and passed these winning chips ($20,000 total) to Person 23. Around 45 minutes later, Customer 37 again placed an unknown number of chips in Customer 32's pocket. Early the following morning, Person 23 exchanged $10,000 in cash for chips and then handed these chips to Customer 32. At no time was Customer 37 observed to engage in any gambling activity.

On 4 September 2020, while in the elevator together, Customer 32 handed $10,000 in cash to Person 32. Person 32 hid the cash under their jumper and then removed it. Person 32 then changed this cash into chips. A few minutes later, Customer 32 removed another $10,000 cash from their jacket pocket. Person 32 gave Customer 32 the $10,000 worth of chips, and Customer 32 gave Person 32 the $10,000 in cash and Customer 32's rewards card. Person 32 approached the Cage and presented the $10,000 cash and Customer 32's rewards card. Customer 32 subsequently passed on the $10,000 in chips in their possession to another associate (Customer 29), before collecting $10,000 in cash chips from Person 32: SMR dated 18 September 2020.

See paragraph 995.f below.

d. designated services provided to Customer 32 included substantial EGM activity at SCA;

Particulars

See paragraphs 352 and 353 above.

From 7 December 2016 to 8 August 2021, Customer 32's turnover on EGMs was estimated to be $396,507 and their total losses were estimated to be $48,897.

e. Customer 32 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 23 January 2017 and 9 August 2021, SCA gave the AUSTRAC CEO 137 TTRs detailing incoming and outgoing payments made by Customer 32 totalling $2,551,440, which comprised:

a. 133 TTRs totalling $2,499,440 in chip and cash exchanges;

b. three TTRs totalling $42,000 in account deposits; and

c. one TTR totalling $10,000 for an account withdrawal.

Large and suspicious cash transactions

See particulars to paragraphs 995.c and 995.f.

f. Customer 32 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including structuring, layering and the use of third parties to conduct transactions;

Particulars

See paragraph 24 above.

On 20 January 2017, Customer 37 conducted a cash buy-in of $10,000 on Customer 32's behalf. Immediately after the buy-in, Customer 37 handed the chips to Customer 32. SCA staff concluded that the behaviour was an attempt to distance Customer 32 from a large cash transaction: SMR dated 25 January 2021.

In August 2020, Customer 32 and two of their associates (Customer 29 and Customer 30) used Customer 37 and Person 23 to conduct threshold transactions on their behalf, to avoid the transaction reporting threshold. SCA observed that Customer 29, Customer 32 and Customer 30 were engaging in layering by using third parties to disguise their buy-ins and chip purchases, in order to create the perception of genuine wins generated from their gambling activity: SMR dated 24 August 2020.

On 11 September 2020, Customer 32 exchanged $7,450 in cash for chips at the Baccarat Pavilion, and then left without gaming. Approximately 30 minutes later, Customer 32 was observed handing

$3,000 worth of chips to Customer 30. Around the same time, Customer 29 was also observed handing $12,000 in chips to Customer 30: SMR dated 15 September 2020.

On 15 April 2021 and 16 April 2021, SCA staff observed interactions and patterns of transactions suggesting that Customer 32 likely passed $11,020 in chips to an associate. The associate subsequently cashed out the chips in three separate transactions, all of which were below the reporting threshold. SCA noted concerns that Customer 32's associate was structuring transactions and assisting Customer 32 to avoid the threshold reporting requirements: SMR dated 28 April 2021.

g. Customer 32 had access to private gaming rooms at SCA;

Particulars

See paragraph 145(e) above.

Customer 32 had access to private gaming rooms at SCA, including the Black Room, Platinum Room and Grange Room.

h. SCA did not have adequate reason to believe that Customer 32's source of wealth or source of funds was sufficient to explain the high value gambling services (table 3, s 6 of the Act) provided to Customer 32 by SCA.

Particulars

See paragraph 516 above.

SCA understood Customer 32 to be a truck driver.

Between 7 December 2016 and 8 August 2021, Customer 32 turned over more than $44,000,000 at SCA.

At all times, SCA was aware that Customer 32 was associated with a number of individuals known to have been convicted for various offences including drug dealing.

At no time was SCA's understanding of Customer 32's source of wealth or source of funds commensurate with the high value gambling services that they received at SCA.

SCA's determination of the ML/TF risks posed by Customer 32

996. On and from 9 May 2016, Customer 32 was appropriately rated by SCA as a high risk customer for the purpose of the Act and Rules.

997. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 32 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by it with respect to Customer 32.

Monitoring of Customer 32's transactions

998. At no time did SCA apply appropriate transaction monitoring to Customer 32's transactions because SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

The review, update and verification of Customer 32's KYC information

999. SCA did not review, update or verify Customer 32's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 32, including the nature, extent and purpose of Customer 32's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 32's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 32's risk profile* above there were higher ML/TF risks associated with Customer 32's source of wealth or source of funds.

SCA did not require Customer 32 to provide evidence supporting their alleged source of wealth until 9 August 2021.

d. to the extent that SCA reviewed Customer 32's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 32.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

ECDD triggers in respect of Customer 32

1000. SCA was required to apply the ECDD program to Customer 32 following any ECDD triggers in respect of Customer 32.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

1001. Customer 32 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 25 January 2017 and 28 April 2021, SCA gave the AUSTRAC CEO six SMRs pertaining to Customer 32.

~~b.~~ determined by SCA to be high risk for the purpose of the Act and Rules by SCA prior to the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 32* above.

1002. Each matter pleaded in paragraph 1001 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

1003. SCA did not conduct appropriate risk-based ECDD with respect to Customer 32 following an ECDD trigger because:

a. on each occasion prior to 9 August 2021 that SCA conducted ECDD in respect of Customer 32 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 32 and failed to appropriately consider whether the ML/TF risks posed by Customer 32 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501, 511 and 516 to 517 above.

On 29 June 2018 and 1 November 2018, SCA conducted ECDD in respect of Customer 32, including open source information searches.

During this period, SCA was aware the Customer 32 engaged in, and was associated with customers who engaged in, large and organised cash transactions that were conducted in suspicious circumstances and were indicative of the ML/TF typologies of structuring, layering and the use of third parties to conduct transactions. SCA did not have any identifiable information to support Customer 32's high value

gaming, particularly in circumstances where SCA was aware that Customer 32:

a. was connected to other SCA customers who posed high ML/TF risks;

b. was related to SCA customers who had been banned for their extensive criminal histories and drug trafficking offences; and

c. had listed their occupation as a truck driver.

The ECDD conducted by SCA did not have appropriate regard to Customer 32's higher ML/TF risks: see *Customer 32's risk profile* above

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 32's source of funds or source of wealth.

By reason of the matters set out in *Customer 32's risk profile* above, there were higher ML/TF risks associated with Customer 32's source of wealth or source of funds.

However, it was not until 9 August 2021 that SCA issued a ban in respect of Customer 32.

b. at no time prior to 9 August 2021 did senior management consider the higher ML/TF risks posed by Customer 32 in response to an ECDD trigger, or appropriately consider whether the ML/TF risks posed by Customer 32 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

It was not until 9 August 2021 that SCA issued a ban in respect of Customer 32.

Contravention of s 36 of the Act in respect of Customer 32

1004. By reason of the matters pleaded at paragraphs 992 to 1003 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 32 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1005. By reason of the matters pleaded at paragraph 1004, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 9 August 2021 with respect to Customer 32.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 33

1006. Customer 33 was a customer of SCA during the relevant period. Between 2020 and 2021, SCA recorded turnover exceeding $33,000,000 for Customer 33.

Particulars

Customer 33 was a customer of SCA from 10 December 2002.

On 9 August 2021, SCA issued a ban in respect of Customer 33 at the direction of the SCA AML team.

1007. SCA provided Customer 33 with designated services within the meaning of tables 1 and 3, s 6 of the Act during the relevant period.

Particulars

On 10 February 2002, SCA opened an FMA for Customer 33 which remained open as at 28 October 2022 (item 11, table 3, s 6 of the Act).

While a customer of SCA, Customer 33 remitted funds to their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 33's risk profile* below.

1008. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 33.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 33's risk profile

1009. On and from 7 December 2016, Customer 33, and the provision of designated services to Customer 33 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 33's risk profile prior to the relevant period

a. by 7 December 2016, Customer 33 had the following risk history:

   i. SCA had formed suspicions for the purposes of s 41 of the Act with respect to Customer 33;

Particulars

SCA gave the AUSTRAC CEO an SMR on 24 November 2013.

This SMR reported that, on 22 November 2013, Customer 33 engaged in two transactions indicative of structuring and cashing-in large value chips totalling $17,000 with no evidence of play, and acted nervously when SCA requested identification: SMR dated 24

November 2013. SCA processed these transactions despite there being a banning order in force with respect to Customer 33 at this time.

ii. between 2002 and 2012, SCA recorded escalating rates of high turnover of $8,989,853 for Customer 33, with cumulative losses of $369,201;

Particulars

Between 2002 and 2007, Customer 33's recorded individual rated gambling activity for table games at SCA was estimated as a, buy-in of $76,385, turnover of $331,952 with losses of $35,160.

In 2008, Customer 33's recorded individual rated gambling activity for table games at SCA escalated to an estimated turnover of $955,143, buy-in of $180,071 with losses of $41,196.

In 2009, Customer 33's recorded individual rated gambling activity for table games at SCA significantly escalated to an estimated buy-in of $936,790, turnover of $5,670,807 with losses of $165,545.

In 2010, Customer 33's recorded individual rated gambling activity for table games at SCA was estimated as a, buy-in of $459,300, turnover of $1,969,690 with losses of $116,200.

In 2012, Customer 33's recorded individual rated gambling activity for table games at SCA was estimated as a, buy-in of $18,950, turnover of $62,261 with losses of $11,100.

iii. Customer 33 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 18 May 2009 and 29 November 2013, SCA gave the AUSTRAC CEO 10 TTRs detailing incoming and outgoing payments made by Customer 33 at SCA totalling $171,700, which comprised:

a. nine TTRs totalling $156,700 in cash and chip exchanges; and

b. one TTR totalling $15,000 for an account withdrawal.

iv. SCA was aware that Customer 33 had been banned from its premises by a law enforcement agency and that there were reports that Customer 33 was engaged in criminal activity; and

Particulars

On 26 April 2012, a law enforcement agency issued an order banning Customer 33 from SCA's premises until 22 December 2014. SCA's records indicate that the reason for this exclusion was that Customer 33 was a known drug dealer and that the law enforcement agency reasonably apprehended that money used by Customer 33 at SCA may have been obtained through unlawful means.

On 22 November 2013, SCA processed a chip cash out of $17,000 for Customer 33, despite the fact that they were subject to an order banning them from SCA's premises at the time.

Between 28 September 2012 and 9 August 2014, Customer 33 attended SCA's premises on multiple occasions in breach of this banning order. On a number of occasions, Customer 33 was identified in the Baccarat Pavilion in breach of their exclusion order and was escorted from SCA's premises.

v. in 2009, Customer 33 engaged in other conduct indicative of money lending;

Particulars

In July 2009, SCA security staff recorded their suspicions that Customer 33 was engaged in begging for alms and prohibited money lending activities with baccarat players in the Baccarat Pavilion.

Customer 33's risk profile during the relevant period

b. Customer 33 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs. Between December 2020 and August 2021, SCA recorded an estimated buy in of $5,275,355, escalating rates of high turnover of $34,488,017 for Customer 33, with cumulative losses of $893,755;

Particulars

In 2020, Customer 33's recorded individual rated gambling activity for table games at SCA was estimated as a turnover of $10,759,450, buy-in of $1,420,120 with losses of $159,470. These estimated rates of activity were significantly higher than those prior to 7 December 2016.

Between January 2021 and March 2021, Customer 33 was among SCA's top five local customers for cash deposits and turnover.

Between 1 January 2021 and 5 August 2021, Customer 33's recorded individual rated gambling activity for table games at SCA escalated significantly to an estimated buy-in of $3,855,235, turnover of $23,728,567 with losses of $734,285.

c. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 33 by remitting large amounts of money into the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

Between 31 December 2020 and 11 May 2021, SCA received 11 telegraphic transfers totalling $97,000 from Customer 33's personal bank account in Australia, each of which was made available to Customer 33's FMA.

d. SCA was aware that Customer 33 and their associates, including Customer 30 and Customer 29, had engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

Particulars

On 29 January 2021, SCA staff observed that Customer 33 acted in concert with Customer 30 and Customer 29 to conduct transactions involving the receipt and movement of significant amounts of cash and chips with no apparent economic or visible lawful purpose, with a total value of at least $85,010.

The red flags indicative of higher ML/TF risks included:

a. conducting several cash and chip transactions at multiple gaming Cashiers below the reporting threshold in quick succession;

b. exchanging chips between each other, including under Cashier counters;

c. presenting each other's rewards cards when conducting transactions at the Cage;

d. placing significant amounts of chips into bags;

e. carrying significant amounts of cash into the SCA toilets away from the view of surveillance cameras;

f. conducting suspected exchanges of significant amounts of cash in the SCA toilets; and

g. advising SCA staff that the purpose of their transactions was to "pay their friend".

The suspicious transactions included:

a. four chip to cash exchange transactions with SCA totalling $31,010; and

b. three chip handovers between Customer 29, Customer 30 and Customer 33 totalling $54,000.

SCA considered that this activity was suspicious and involved attempts to avoid transaction reporting requirements. It reported that it was concerned about the ultimate source of the funds: SMR dated 5 February 2021.

e. Customer 33 was connected to other customers at SCA, including players who posed higher ML/TF risks such as Customer 29, Customer 30 and Customer 32;

Particulars

SCA was aware that Customer 33 was acting in concert with Customer 29 and Customer 30 to complete suspicious transactions: see paragraph 1009.d above.

SCA was aware that Customer 33 was an associate of Customer 29 and their family, and that members of this family also conducted transactions on Customer 33's behalf and were connected with Customer 32. SCA was aware that Customer 29's family network included individuals who had been convicted of drug trafficking.

For example, in February 2021, SCA recorded that Customer 33 played high value games of baccarat alongside other customers in respect of whom it had formed suspicions, including Customer 21, Customer 29 and Customer 30.

f. designated services provided to Customer 33 included substantial EGM activity at SCA;

Particulars

See paragraphs 352 and 353 above.

Between 6 December 2020 and 31 December 2020, Customer 33's recorded individual rated gambling activity for EGMs at SCA was estimated as a turnover of $10,805 with losses of $3,754.

Between 1 January 2021 and 2 August 2021, Customer 33's recorded individual rated gambling activity for EGMs at SCA was estimated as a turnover of $25,175 with losses of $2,535.

g. Customer 33 and their associates transacted using large amounts of cash and cash that appeared suspicious at SCA;

Particulars

See paragraphs 376 to 381 above.

See particulars to paragraph 1009.d above.

TTRs

Between 11 December 2020 and 30 April 2021, SCA gave the AUSTRAC CEO 66 TTRs detailing incoming and outgoing payments made by Customer 33 totalling $852,545, which comprised:

a. 58 TTRs totalling $746,305 in cash and chip exchanges;

b. six TTRs totalling $83,220 in account deposits; and

c. two TTRs totalling $23,020 in account withdrawals.

Large and suspicious cash transactions

Between 18 December 2020 and 11 May 2021, Customer 33 made six account deposits in cash below the transaction reporting threshold totalling $30,000.

Between 31 December 2020 and 11 May 2021, Customer 33 made seven account withdrawals in cash below the transaction reporting threshold totalling $30,600.

Between 22 December 2020 and 16 June 2021, Customer 33 conducted 11 cash to chip exchanges with SCA below the transaction reporting threshold totalling $49,600.

On 16 April 2021, an SCA customer that SCA suspected to be acting on behalf of Customer 33 conducted three chip to cash exchanges with SCA below the transaction reporting threshold in quick succession totalling $11,020.

h. Customer 33 and their associates engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including structuring and cashing-in large value chips with no evidence of play;

Particulars

See paragraph 24 above.

Between 17 January 2021 and 16 April 2021, Customer 33 and their associates conducted at least six transactions indicative of the ML/TF typology of structuring. The total value of these transactions was at least $22,030: see paragraphs 1009.d and 1009.g above.

On 29 January 2021, Customer 33 and their associates conducted at least two transactions indicative of the ML/TF typology of cashing-in large value chips with no evidence of play. The total value of these transactions was at least $27,530: see paragraph 1009.d above.

i. Customer 33 had access to a private gaming room at SCA;

Particulars

See paragraph 145(e) above.

Customer 33 had access to the Grange Room, which is a private gaming room at SCA.

j. by 2017, court reports identified that Customer 33 had been convicted for drug trafficking;

Particulars

In March 2011 and November 2017, court sentencing remarks identified that Customer 33 was convicted for drug trafficking.

It was not until 21 June 2022 that SCA became aware of these convictions, after it had issued a ban in respect of Customer 33 on 9 August 2021.

k. by 2018, SCA was aware from discussions with Customer 33 that they were engaged in criminal activity and were attending SCA's casino premises in breach of a parole order;

Particulars

On 5 December 2018, SCA recorded that Customer 33 had advised SCA staff members on two occasions that they were attending the casino premises in breach of a parole order and would be arrested if their parole officer discovered that they were on the premises. Customer 33 immediately departed the casino premises after they were noticed by certain SCA staff members.

l. by 2021, SCA was aware of reports that Customer 33 was engaged in and connected to criminal activity related to illicit drugs;

Particulars

In March 2021 and April 2021, SCA officers circulated reports that Customer 33 was a known drug dealer and a media article that contained a video of Customer 33 attending a dinner with a person who was convicted for selling illicit drugs and money laundering.

m. SCA did not have adequate reason to believe that Customer 33's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 33 by SCA.

Particulars

See paragraph 516 above.

By 7 December 2016, SCA had limited records in its possession indicating Customer 33 was employed as a part-time waiter and a farm worker.

On 25 June 2018, SCA recorded that it was unable to identify Customer 33's occupation after conducting searches of open source information.

On or around 3 December 2020, SCA recorded that Customer 33 had advised they were employed as a cleaner.

Between 1 December 2020 and 30 March 2021, SCA recorded turnover for Customer 3 exceeding $31,000,000.

In around April 2021, SCA recorded that Customer 33's occupation was in cleaning and they operated a cleaning business, but it did not identify any evidence in support of this claim or whether it had been verified besides citing an ABN that presented only a possible match with Customer 33's personal details.

Between 1 April 2021 and 5 August 2021, SCA recorded turnover for Customer 33 exceeding $2,800,000.

In August 2021, SCA requested further information about Customer 33's source of wealth but Customer 33 declined this request.

At no time was SCA's understanding of Customer 33's source of wealth or source of funds commensurate with the extremely high value financial and gambling services that they received at SCA.

SCA's determination of the ML/TF risks posed by Customer 33

1010. SCA was unable to appropriately identify or assess the ML/TF risks posed by Customer 33 because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 33.

a. On and from 7 December 2016, Customer 33 should have been recognised by SCA as a high risk customer for the purpose of the Act and Rules for the reasons pleaded above: see *Customer 33's risk profile* above.

Particulars

Sections 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

b. It was not until 24 October 2018 that Customer 33 was rated high risk by SCA for the purpose of the Act and Rules.

Monitoring of Customer 33's transactions

1011. At no time did SCA apply appropriate transaction monitoring to Customer 33's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities;

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 33 through: the SCA Customer account channel, which was a high risk remittance channel;

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 33's KYC information

1012. SCA did not review, update or verify Customer 33's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 33, including the nature, extent and purpose of Customer 33's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 33's source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 33's risk profile* above, there were real risks that Customer 33's source of wealth and source of funds were not legitimate.

d. to the extent that SCA reviewed Customer 33's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 33.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

Failure to apply appropriate due diligence suited to the high ML/TF risks

1013. Had SCA conducted ongoing customer due diligence on and from 7 December 2016 by:

a. appropriately identifying and assessing the ML/TF risks posed by Customer 33;

b. applying appropriate risk-based transaction monitoring to Customer 33; and

c. appropriately reviewing and updating Customer 33's KYC information, having regard to the high ML/TF risks,

SCA would have been required by the Act and Rules to apply the ECDD Program to Customer 33 at a time before the date of the ECDD triggers pleaded below: see *ECDD triggers in respect of Customer 33*.

ECDD triggers in respect of Customer 33

1014. SCA was required to apply the ECDD program to Customer 33 following any ECDD triggers in respect of Customer 33.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

1015. Customer 33 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 5 February 2021 and 28 April 2021, SCA gave the AUSTRAC CEO two SMRs with respect to Customer 33.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 33* above.

1016. Each matter pleaded in paragraph 985 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

1017. SCA did not conduct appropriate risk-based ECDD with respect to Customer 33 following an ECDD trigger because:

a. on each occasion prior to August 2021 that SCA conducted ECDD in respect of Customer 33 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 33 and failed to appropriately consider whether the ML/TF risks posed by Customer 33 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501, 511 and 516 to 517 above.

Database alerts

Between 4 December 2020 and 4 August 2021, SCA received three open source Dow Jones watchlist alerts and eight transaction alerts in respect of Customer 33 involving over $1,254,000 but resolved to take no further action following manual review conducted by SCA's AML team.

ECDD screening

In June 2018, SCA conducted ECDD screening in respect of Customer 33, which identified that:

a. SCA had previously identified that Customer 33 was engaged in transactions indicative of structuring;

b. SCA had been unable to verify the information provided by Customer 33 relating to their occupation, source of funds and source of wealth;

c. some of Customer 33's associates were unknown to SCA; and

d. SCA had been unable to identify any open source information in respect of Customer 33.

At all times, SCA was aware that, from 2012 to 2014, Customer 33 had been subject to an exclusion order due to suspicions that they were a drug dealer and had used proceeds of crime to fund gaming at SCA.

By November 2017, Customer 33 had been convicted for drug trafficking on two occasions.

By 2018, SCA had been unable to verify Customer 33's stated occupation, source of funds and source of wealth. SCA was aware that Customer 33 had been involved in a number of suspicious transactions at SCA, including transactions that were indicative of ML/TF typologies, often with other customers whom SCA considered to be suspicious.

In December 2020, Customer 33 returned to record individual rated gambling activity at SCA after a long period of absence and proceeded to turn over more than $10,000,000 that month.

Despite this, it was not until 30 April 2021 that SCA requested that Customer 33 provide further information regarding their occupation and source of funds. By that time, Customer 33 had recorded individual rated gambling activity of more than $30,000,000 since December 2020.

In around April 2021, ECDD conducted by SCA confirmed that:

a. SCA had not been able to verify the information provided by Customer 33 regarding their occupation as a cleaner, and their source of funds and source of wealth;

b. Customer 33's turnover had increased significantly in 2020 and 2021;

c. Customer 33 was associated with Customer 30 and Customer 29 and these individuals had conducted multiple suspicious transactions together, including transactions indicative of structuring;

d. Customer 33 had been banned from SCA in 2012 due to suspicions that they were a drug dealer who used money obtained through unlawful means, and had breached this ban on multiple occasions;

e. SCA suspected that Customer 33 had a "possible criminal history" as they had acknowledged in 2018 that they were on parole and had breached the terms of their parole by being present on SCA premises. There are no records to suggest that SCA took any steps to verify Customer 33's criminal history, or that SCA identified Customer 33's prior convictions for drug trafficking; and

f. a media article dated 29 April 2021 reported that Customer 33 attended a dinner with a person who was convicted for selling illicit drugs and money laundering.

However, it was not until 9 August 2021 that SCA issued a ban in respect of Customer 33 due to concerns regarding their source of wealth and source of funds.

Between 1 May 2021 and 9 August 2021, Customer 33 recorded turnover of more than $1,400,000 at SCA.

Prior to April 2021, the ECDD conducted by SCA in respect of Customer 33 did not have appropriate regard to the ML/TF risks posted by Customer 33: see *Customer 33's risk profile* above.

Prior to April 2021, the ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 33's source of funds or source of wealth.

By reason of the matters set out in *Customer 33's risk profile* above, there were real risks that Customer 33's source of wealth and source of funds were not legitimate.

b. at no time prior to August 2021 did senior management consider the higher ML/TF risks posed by Customer 33 in response to an ECDD trigger, or appropriately consider whether the ML/TF risks posed by Customer 33 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

In August 2021, the SCA Chief Operating Officer requested a review of Customer 33 and nine other customers in respect of whom SCA had formed suspicions.

This review identified that:

a. SCA was not satisfied that it had appropriate source of wealth documents to support Customer 33's gambling activity; and

b. Customer 33 was an associate of Customer 29, who had been banned from SCA.

In August 2021, SCA's AML/CTF team conducted an internal review which recommended that SCA terminate its relationship with Customer 33 on the basis that they were a known drug dealer who was engaged in transactions indicative of the ML/TF typology of structuring. This recommendation was only made in August 2021, despite the fact that:

a. SCA first recorded that it was aware that Customer 33 was a drug dealer on 26 April 2012: see particulars to paragraph 1009.a.iv; and

b. by August 2021, SCA had given the AUSTRAC CEO two SMRs outlining Customer 33's involvement in transactions indicative of structuring: SMRs dated 24 November 2013 and 5 February 2021.

On 9 August 2021, SCA issued a ban in respect of Customer 33 and sent a letter requesting that they provide information to support their source of wealth.

Despite this, on 16 August 2021, the SCA Security Operations Manager advised the General Manager Legal, Compliance and Regulatory Affairs, the AML Compliance Manager and SCA VIP

Services officers that Customer 33 and ten other customers were continuing to attend SCA premises despite their bans being in effect.

Contravention of s 36 of the Act in respect of Customer 33

1018. By reason of the matters pleaded at paragraphs 1006 to 1017 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 33 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1019. By reason of the matters pleaded at paragraph 1018, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 9 August 2021 with respect to Customer 33.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 34

1020. Customer 34 was a customer of SCA during the relevant period. Between 7 December 2016 and 13 March 2020, SCA recorded turnover exceeding $4,800,000 for Customer 34.

Particulars

Customer 34 was a customer of SCA from at least 5 September 2016.

On 22 March 2022, SCA issued a ban in respect of Customer 34 at the direction of the SCA AML team.

1021. SCA provided Customer 34 with designated services within the meaning of tables 1 and 3, s 6 of the Act during the relevant period.

Particulars

Prior to 7 December 2016, SCA opened an FMA for Customer 34 which was closed on 11 October 2021 (item 11, table 3, s 6 of the Act).

While a customer of SCA, Customer 34 remitted funds to their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 34's risk profile* below.

1022. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 34.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 34's risk profile

1023. On and from 7 December 2016, Customer 34, and the provision of designated services to Customer 34 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 34's risk profile prior to the relevant period

a. by 7 December 2016, Customer 34 had the following risk history:

   i. SCA had formed suspicions for the purposes of s 41 of the Act with respect to Customer 34;

Particulars

On 10 October 2016, SCA gave the AUSTRAC CEO an SMR pertaining to Customer 34.

The SMR reported that, on 7 October 2016, Customer 34 and two associates engaged in suspicious behaviour which SCA considered involved attempts to structure transactions to avoid the transaction reporting threshold. Customer 34 and the two other SCA customers were also observed covertly passing chips between each other.

Customer 34's risk profile during the relevant period

b. Customer 34 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs. Between 7 December 2017 and March 2020, SCA recorded an estimated buy-in of $1,220,880, and turnover estimated at $4,838,093 for Customer 34, with cumulative losses of $199,550;

Particulars

In 2016, Customer 34's recorded individual rated gambling activity at SCA was estimated as a buy-in of $271,960 for table games, and for both table games and EGMs, turnover of $922,790 with losses of $23,640.

In 2017, Customer 34's recorded individual rated gambling activity at SCA was estimated as a buy-in of $247,400 for table games, and for both table games and EGMs, turnover of $824,434 with losses of $40,871.

In 2018, Customer 34's recorded individual rated gambling activity at SCA was estimated as a buy-in of $220,850 for table games, and for both table games and EGMs, turnover of $646,692 with losses of $31,706.

In 2019, Customer 34's recorded individual rated gambling activity at SCA escalated to an estimated buy-in of $989,780 for table games, and for both table games and EGMs, turnover of $2,811,449 with losses of $109,464.

Between 1 January 2020 and 13 March 2020, prior to closures related to the COVID-19 pandemic, Customer 34's recorded individual rated gambling activity at SCA was estimated as a buy-in of $10,250 for table games, and for both table games and EGMs, turnover of $27,888 with losses of $5,884. Customer 34 was imprisoned from August 2020.

c. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 34 by remitting money into and out of the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

Between 12 July 2019 and 14 August 2019, Customer 34 transferred $2,455 from their personal bank account in Australia to their SCA FMA. SCA made these funds available to Customer 34.

On 8 August 2019, SCA accepted instructions to transfer $1,000 from Customer 34's SCA FMA to their personal bank account in Australia.

d. Customer 34 had engaged in unusual transactions, which had no apparent economic or visible lawful purpose;

Particulars

For example, in November 2019, SCA identified that Customer 34 and Person 22 had been passing cash and cash chips between each other. On one occasion, Person 22 placed two cash chips worth $1,000 each in Customer 34's jacket pocket.

e. Customer 34 was connected to other customers at SCA, including players who posed higher ML/TF risks such as Customer 30 and Customer 36, and players who SCA considered had acted suspiciously such as Person 20;

Particulars

For example:

a. on 26 April 2019, Customer 34, Customer 30 and Person 20 engaged in conduct that SCA suspected involved structuring: SMR dated 26 April 2019; and

b. a surveillance review on 17 June 2019 showed Customer 34 and Customer 36 passing cash and cash chips between each other.

f. designated services provided to Customer 34 included EGM activity at SCA;

Particulars

See paragraphs 352 and 353 above.

In 2016, Customer 34 had turnover of $6,646 on EGMs with losses of $1,185.

In 2017, Customer 34 had turnover of $24,451 on EGMs with losses of $2,606.

In 2018, Customer 34 had turnover of $5,152 on EGMs with losses of $1,456.

In 2019, Customer 34 had turnover of $38,372 on EGMs with losses of $7,434.

Between 1 January 2020 and 10 March 2020, prior to closures related to the COVID-19 pandemic, Customer 34 had turnover of $461 on EGMs with losses of $223. Customer 34 was imprisoned from August 2020.

g. Customer 34 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 28 September 2018 and 18 September 2019, SCA gave the AUSTRAC CEO 11 TTRs detailing chip and cash exchanges made by Customer 34 totalling $168,340 including:

a. eight outgoing transactions involving cashing out chips or tokens totalling $128,240; and

b. three incoming transactions involving the issuance of chips or tokens totalling $40,000.

h. Customer 34 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including structuring:

Particulars

See paragraph 24 above.

On 26 April 2019, Customer 34 attended SCA with Customer 30 and Person 20, who passed Customer 34 $12,000 worth of cash chips. Customer 34 cashed out $6,000 in cash chips and handed the cash to Person 20.

Three minutes later, Customer 34 returned to the main Cage and cashed out a further $6,100 in chips, before leaving the casino with Customer 30.

SCA suspected that Customer 34 was attempting to structure cash out transactions to avoid the transaction reporting threshold and was not the owner of the gaming chips they cashed out: SMR dated 26 April 2019.

i. Customer 34 had access to private gaming rooms at SCA;

Particulars

See paragraph 145(e) above.

Customer 34 had access to private gaming rooms at SCA, including the Black Room and Grange Room.

j. from January 2021 to April 2021, SCA was aware that Customer 34 appeared on the criminal law list of an Australian court charged with money laundering and trafficking in a controlled drug;

Particulars

On 29 January 2021, Customer 34's name appeared on the list of an Australian court for arraignment on charges of knowingly engaging in money laundering, trafficking in a controlled drug and possessing prescribed equipment.

On 26 March 2021, Customer 34's name appeared on the list of an Australian court for a guilty plea arraignment on further charges of money laundering and trafficking in a controlled drug.

On 21 April 2021, both of Customer 34's matters were listed for sentence.

On 30 April 2021, both of Customer 34's matters were again listed for sentence.

k. in late April 2021, SCA was aware of a number of media articles which reported that Customer 34 had been jailed for over eight years for money laundering, trafficking in heroin and possessing prescribed equipment; and

Particulars

On 28 April 2021, media reports stated that Customer 34 had:

a. become involved in drug trafficking to service gambling debts;

b. been arrested and placed on home detention bail on 8 May 2020 when a law enforcement agency found heroin and cash in Customer 34's possession; and

c. been detained in custody from 13 August 2020, after a law enforcement agency conducted a further search and found more heroin and cash in Customer 34's possession.

On 3 May 2021, media reports stated that Customer 34 had been sentenced by an Australian court to imprisonment for eight years, two months and 22 days with a non-parole period of four years and six months.

l. SCA did not have adequate reason to believe that Customer 34's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 34 by SCA.

Particulars

See paragraph 516 above.

Prior to September 2018, SCA did not request source of wealth or source of funds information from Customer 34.

On 26 September 2018, Customer 34 informed SCA that they were employed as a farm hand. By that time, Customer 34's historical individual rated gambling activity at SCA was estimated at a total buy-in of $519,360 with turnover of at least $1,866,539.

SCA took no further steps to determine Customer 34's source of wealth or source of funds, despite:

a. Customer 34's gambling activity escalating from September 2018, with their buy-ins for table games increasing from $220,850 in 2018 to $989,780 in 2019 and, for both table games and EGMs, their turnover increasing from $646,692 to $2,811,449 and losses increasing from $31,706 to $109,464 between 2018 and 2019;

b. SCA identifying that Customer 34 had engaged in transactions that were indicative of ML/TF typologies; and

c. SCA's awareness that Customer 34 was associated with other suspicious customers who posed higher ML/TF risks, including Customer 30 and Customer 36.

At no time was SCA's understanding of Customer 34's source of wealth or source of funds commensurate with the high value financial and gambling services that they received at SCA.

SCA's determination of the ML/TF risks posed by Customer 34

1024. SCA was unable to appropriately identify or assess the ML/TF risks posed by Customer 34 because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 34.

a. On and from 7 December 2016, Customer 34 should have been recognised by SCA as a high risk customer for the purpose of the Act and Rules for the reasons pleaded above: see *Customer 34's risk profile* above.

Particulars

Sections 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

b. It was not until 11 September 2019 that Customer 34 was rated high risk by SCA for the purpose of the Act and Rules.

Particulars

On 26 October 2021, Customer 34 was rated significant risk by SCA, which was high risk for the purpose of the Act and Rules.

Monitoring of Customer 34's transactions

1025. At no time did SCA apply appropriate transaction monitoring to Customer 34's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities;

Particulars

Section 36(1)(a), (b) of the Act and rules 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 34 through the SCA Customer account channel, which was a high risk remittance channel;

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 34's KYC information

1026. SCA did not review, update or verify Customer 34's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 34, including the nature, extent and purpose of their transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 34's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 34's risk profile* above, there were real risks that Customer 34's source of wealth and source of funds were not legitimate

On and from 7 December 2016, Customer 34's turnover was high. Customer 34's turnover was not proportionate to their source of wealth, suggesting that there were real ML/TF risks as to Customer 34's source of funds. SCA made no attempts to verify Customer 34's source of funds: see particulars to paragraph 1023.l above.

d. to the extent that SCA reviewed Customer 34's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 34.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

Failure to apply appropriate due diligence suited to the high ML/TF risks

1027. Had SCA conducted ongoing customer due diligence on and from 7 December 2016 by:

a. appropriately identifying and assessing the ML/TF risks posed by Customer 34;

b. applying appropriate risk-based transaction monitoring to Customer 34; and

c. appropriately reviewing and updating Customer 34's KYC information, having regard to the high ML/TF risks,

SCA would have been required by the Act and Rules to apply the ECDD Program to Customer 34 at a time before the date of the ECDD triggers pleaded below: see *ECDD triggers in respect of Customer 34*.

ECDD triggers in respect of Customer 34

1028. SCA was required to apply the ECDD program to Customer 34 following any ECDD triggers in respect of Customer 34.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

1029. Customer 34 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 26 April 2019 and 14 July 2019 SCA gave the AUSTRAC CEO two SMRs pertaining to Customer 34.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 34* above.

1030. Each matter pleaded in paragraph 1029 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

1031. SCA did not conduct appropriate risk-based ECDD with respect to Customer 34 following an ECDD trigger because:

a. on each occasion prior to late 2021 that SCA conducted ECDD in respect of Customer 34 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 34 and failed to appropriately consider whether the ML/TF risks posed by Customer 34 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

Transaction Reviews

SCA conducted a surveillance review of transactions involving Customer 34, Customer 30 and Person 20 in response to an alert from front line staff: see particulars to paragraph 1023.h above.

ECDD

On 14 November 2019, SCA conducted ECDD in respect of Customer 34.

In around August 2021, SCA conducted further ECDD following Customer 34's convictions for money laundering and drug trafficking offences. The ECDD identified Customer 34's convictions and recommended that SCA ban Customer 34 from the casino.

However, it was not until 22 March 2022 that SCA issued a ban in respect of Customer 34 following in-house investigations by the SCA AML team and the publication of adverse open source media identifying Customer 34.

The ECDD conducted by SCA did not have appropriate regard to Customer 34's higher ML/TF risks: see *Customer 34's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 34's source of funds or source of wealth.

By reason of the matters set out above, there were real risks that Customer 34's source of wealth and source of funds were not legitimate: see *Customer 34's risk profile* above.

b. at no time prior to 22 March 2022 did senior management consider the higher ML/TF risks posed by Customer 34 in response to an ECDD trigger, or appropriately consider whether the ML/TF risks posed by Customer 34 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

There is no evidence of senior management consideration prior to 21 March 2022. On 22 March 2022, SCA issued a ban in respect of Customer 34.

Contravention of s 36 of the Act in respect of Customer 34

1032. By reason of the matters pleaded at paragraphs 1020 to 1031 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 34 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1033. By reason of the matters pleaded at paragraph 1032, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 22 March 2022 with respect to Customer 34.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 35

1034. Customer 35 was a customer of SCA during the relevant period. Between 7 December 2016 and 24 August 2021, SCA recorded turnover exceeding $13,000,000 for Customer 35.

Particulars

Customer 35 was a customer of SCA from at least 19 August 2009.

On 24 August 2021, SCA issued a ban in respect of Customer 35 at the direction of the SCA AML team.

1035. SCA provided Customer 35 with designated services within the meaning of table 3, s 6 of the Act during the relevant period.

Particulars

Prior to the relevant period, SCA opened an FMA for Customer 35 which was closed on 24 August 2021 (item 11, table 3, s 6 of the Act).

See *Customer 35's risk profile* below.

1036. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 35.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 35's risk profile

1037. On and from 7 December 2016, Customer 35, and the provision of designated services to Customer 35 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 35's risk profile prior to the relevant period

a. by 7 December 2016, Customer 35 had the following risk history:

i. SCA had formed suspicions for the purposes of s 41 of the Act with respect to Customer 35;

Particulars

SCA gave the AUSTRAC CEO an SMR on one occasion between 19 August 2009 and 6 December 2016.

The SMR reported that on 12 August 2016, Customer 35 gambled, changed chips, cashed out chips and conducted threshold transactions on behalf of Customer 29, who was a known associate of other individuals who were involved in crime and banned from SCA. The SMR raised concern about Customer 35's association with Customer 29, noting that the behaviour of the two individuals appeared to be an effort to launder funds and prevent Customer 29 from being reported for threshold transactions.

ii. SCA was aware that Customer 35 received high value gambling services (table 3, s 6 of the Act) at SCA since 2009:

Particulars

In 2009, Customer 35's recorded individual rated gambling activity at SCA was estimated as a buy-in of $150,295 for table games, and turnover of $505,088, with losses of $35,245.

In 2010, Customer 35's recorded individual rated gambling activity at SCA escalated to an estimated buy-in of $390,685 for table games, and turnover of $1,852,977 with losses of $37,280.

In 2011, Customer 35's recorded individual rated gambling activity at SCA was estimated as a buy-in of $271,280 for table games, and turnover of $1,714,715, with losses of $6,680.

In 2012, Customer 35's recorded individual rated gambling activity at SCA significantly escalated to an estimated buy-in of $3,120,050 for table games, and for both table games and EGMs, turnover of $36,759,674 with wins of $641,962.

In 2013, Customer 35's recorded individual rated gambling activity at SCA was estimated as a buy-in of $445,050 for table games, and for both table games and EGMs, turnover of $2,494,117 with losses of $69,215.

In 2014, Customer 35's recorded individual rated gambling activity at SCA was estimated as a buy-in of $478,000 for table games, and for both table games and EGMs, turnover of $3,377,301 with wins of $27,510.

In 2015, Customer 35's recorded individual rated gambling activity at SCA escalated to an estimated buy-in of $700,380 for table games, and for both table games and EGMs, turnover of $4,508,767 with losses of $219,126.

iii. Customer 35 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 17 August 2009 and 15 August 2016, SCA gave the AUSTRAC CEO 120 TTRs detailing incoming and outgoing payments made by Customer 35 totalling $2,013,025, which comprised:

a. 114 TTRs totalling $1,936,025 in chip and cash exchanges;

b. four TTRs totalling $50,000 in account deposits; and

c. two TTRs totalling $27,000 in EGM payouts.

iv. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 35 by remitting large amounts of money into the casino environment via their accounts, including through high risk remittance channels; and

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCEG customer account channel

In 2015, SCA gave the AUSTRAC CEO four incoming IFTIs totalling $50,000 where Customer 35 was named as the customer. SCA made these funds available to Customer 35.

v. Customer 35 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including structuring;

Particulars

See paragraph 24 above.

On the following occasions, Customer 35 was involved in transactions indicative of the ML/TF typology of structuring:

a. On 7 February 2010, Customer 35 had their partner cash out $1,500 on their behalf before they cashed out a further $9,000 to avoid the transaction reporting threshold.

b. On 16 January 2012, Customer 35 attempted to cash out $10,000 but was refused due to having no identification. One hour later, Customer 35 returned with another SCA customer and they each cashed out $5,000 with no identification.

Customer 35's risk profile during the relevant period

b. Customer 35 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs. Between 7 December 2016 and 24 August 2021, SCA recorded an estimated buy-in of $2,097,310, a high turnover estimated at $13,877,025 for Customer 35, with cumulative losses of $158,840;

Particulars

In 2016, Customer 35's recorded individual rated gambling activity at SCA was estimated as a buy-in of $532,810 for table games, and for both table games and EGMs, turnover of $3,609,719 with losses of $119,406.

In 2017, Customer 35's recorded individual rated gambling activity at SCA was estimated as a buy-in of $67,950 for table games, and for both table games and EGMs, turnover of $389,189 with losses of $64,738.

In 2018, Customer 35's recorded individual rated gambling activity at SCA escalated to an estimated buy-in of $607,550 for table games, and for both table games and EGMs, turnover of $5,293,632 with wins of $33,061.

In 2019, Customer 35's recorded individual rated gambling activity at SCA was estimated as a buy-in of $423,550 for table games, and for both table games and EGMs, turnover of $4,562,753 with wins of $60,609.

In 2020, despite closures related to the COVID-19 pandemic, Customer 35's recorded individual rated gambling activity at SCA was estimated as a buy-in of $319,650 for table games, and for both table games and EGMs, turnover of $1,803,642 with losses of $149,793.

In 2021, Customer 35's recorded individual rated gambling activity at SCA was estimated as a buy-in of $145,800 for table games, and for both table games and EGMs, turnover of $1,827,809 with losses of $37,979.

c. Customer 35 was connected to other customers at SCA, including players who posed higher ML/TF risks such as Customer 29, Customer 30 and Customer 36, and other players who SCA considered had acted suspiciously;

Particulars

Customer 35 was a known associate of Customer 29. SCA knew that Customer 29 had structured transactions, gambled at a level not commensurate to their stated income, utilised other patrons to perform large transactions on their behalf and belonged to a family network that included individuals that had been convicted of drug trafficking.

On 1 September 2020, Customer 35 was observed exchanging cash and chips, and gambling, with Customer 29, Customer 30 and Customer 36. Customer 29, Customer 30 and Customer 36 were known by SCA to be associated with a network of known drug dealers.

d. Customer 35 engaged in large and unusual transactions and patters of transactions, which had no apparent economic or visible lawful purpose;

Particulars

On 1 September 2020:

a. Customer 35 gave a bundle of cash comprising 200 $50 notes ($10,000 in total) to Customer 36, who then purchased two $5,000 cash chips. Customer 36 later handed the chips to Customer 30, who then gave the chips to Customer 35. SCA suspected that Customer 35 and Customer 36 were attempting to misrepresent the origin and destination of this transaction;

b. shortly after handing a bundle of cash to Customer 36, Customer 35 purchased chips using 38 $100 notes and 124 $50 notes ($10,000 in total), for which Customer 35 received ten $1,000 cash chips; and

c. later, Customer 35 removed $5,000 cash chips from their pocket, despite the fact that Customer 35 was not observed at any point to have obtained any $5,000 cash chips during gaming or from chip purchases.

Between October 2016 and March 2017, Customer 35 was included in an SCA internal report titled 'AML Unusual Changes in Betting' on two occasions.

e. designated services provided to Customer 35 included substantial EGM activity at SCA;

Particulars

See paragraphs 352 and 353 above.

From 2016 to 2021, Customer 35's turnover on EGMs was estimated to be $1,347,826 and their total losses were estimated to be $62,586.

f. Customer 35 transacted using large amounts of cash and cash that appeared suspicious, including large volumes of cash in small notes in rubber bands, at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 24 April 2017 and 4 March 2021, SCA gave the AUSTRAC CEO 61 TTRs detailing incoming and outgoing payments made by Customer 35 totalling $1,052,729, which comprised:

a. 51 TTRs totalling $868,020 in chip and cash exchanges;

b. two TTRs totalling $30,000 in account deposits; and

c. eight TTRs totalling $154,709 in EGM payouts.

Large and suspicious cash transactions in 2020

On 1 September 2020, Customer 35 removed two bundles of cash from their bag and handed one of the bundles of cash to Customer 36. When Customer 36 presented the bundle of cash to exchange for

chips, it consisted of 200 $50 notes ($10,000 in total). Customer 35 exchanged the second bundle for chips, which consisted of 38 $100 notes and 124 $50 notes ($10,000 in total).

g. Customer 35 had access to private gaming rooms at SCA; and

Particulars

See paragraph 145(e) above.

Customer 35 had access to private gaming rooms at SCA, including the Black Room, Grange Room and Platinum Room.

h. SCA did not have adequate reason to believe that Customer 35's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (table 3, s 6 of the Act) provided to Customer 35 by SCA.

Particulars

See paragraph 516 above.

From December 2016, SCA was aware that Customer 35's occupation was as a self-employed owner of a "Farming & Nail Shop".

Between 2016 and 2021, Customer 35's turnover was over $1,000,000 each year except for 2017, and was approximately $5,200,000 in 2018.

At all times from December 2016, SCA was aware that Customer 35 was associated with individuals involved in crime and banned from SCA, and observed colour changing chips and conducting threshold transactions on behalf of Customer 29, person in respect of whom SCA had formed suspicions, in a potential effort to launder funds.

At no time was SCA's understanding of Customer 35's source of wealth or source of funds commensurate with the high value gambling services that they received at SCA.

Despite this, SCA did not request Customer 35's updated occupation information during the relevant period.

It was not until August 2021 that SCA requested details about Customer 35's source of wealth, but Customer 35 refused to provide that information.

SCA's determination of the ML/TF risks posed by Customer 35

1038. SCA was unable to appropriately identify or assess the ML/TF risks posed by Customer 35 because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risk reasonably faced by SCA with respect to Customer 35.

a. On and from 7 December 2016, Customer 35 should have been recognised by SCA as a high risk customer for the purpose of the Act and Rules for the reasons pleaded above: see *Customer 35's risk profile* above.

Particulars

Sections 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

b. It was not until around 27 March 2019 that Customer 35 was rated high risk by SCA for the purpose of the Act and Rules.

Particulars

On 24 August 2021, Customer 35 was rated significant risk by SCA, which was high risk for the purpose of the Act and Rules, and SCA issued a ban in respect of Customer 35.

Monitoring of Customer 35's transactions

1039. At no time did SCA apply appropriate transaction monitoring to Customer 35's transactions because SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

The review, update and verification of Customer 35's KYC information

1040. SCA did not review, update or verify Customer 35's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 35, including the nature, extent and purpose of their transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update or verify Customer 35's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 35's risk profile* above, there were higher ML/TF risks associated with Customer 35's source of wealth or source of funds.

d. to the extent that SCA reviewed Customer 35's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 35.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

Failure to apply appropriate due diligence suited to the high ML/TF risks

1041. Had SCA conducted ongoing customer due diligence on and from 7 December 2016 by:

a. appropriately identifying and assessing the ML/TF risks posed by Customer 35;

b. applying appropriate risk-based transaction monitoring to Customer 35; and

c. appropriately reviewing and updating Customer 35's KYC information, having regard to the high ML/TF risks,

SCA would have been required by the Act and Rules to apply the ECDD Program to Customer 35 at a time before the date of the ECDD triggers pleaded below: see *ECDD triggers in respect of Customer 35*.

ECDD triggers in respect of Customer 35

1042. SCA was required to apply the ECDD program to Customer 35 following any ECDD triggers in respect of Customer 35.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

1043. Customer 35 was determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 35* above.

1044. The matter pleaded in paragraph 1043 was an ECDD trigger.

Particulars

See paragraphs 496 and 504 above.

1045. SCA did not conduct appropriate risk-based ECDD with respect to Customer 35 following an ECDD trigger because:

a. on each occasion prior to 24 August 2021 that SCA conducted ECDD in respect of Customer 35 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 35 and failed to appropriately consider whether the ML/TF risks posed by Customer 35 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

Between 27 March 2019 and 8 September 2020, SCA conducted ECDD in respect of Customer 35.

On 27 March 2019, the ECDD screening in respect of Customer 35 identified that:

a. on 7 February 2010, Customer 35 structured transactions below $10,000 to avoid the threshold for TTRs;

b. on 16 January 2012, Customer 35 attempted to cash out $10,000 but was refused due to having no identification, and then later returned to structure transactions totalling $10,000 with another SCA customer in order to avoid the reporting threshold; and

c. on 12 August 2016, Customer 35 cashed out chips on behalf of Customer 29, who was a known associate of persons banned from SCA due to their extensive criminal histories and drug related offences.

On 1 September 2020, SCA conducted ECDD screening in respect of Customer 35 which involved reviewing a number of transactions that took place on 1 September 2020.

On 8 September 2020, SCA conducted ECDD screening in respect of Customer 36 which identified SCA's concerns that Customer 36 was performing threshold transactions on behalf of other customers, including Customer 35.

The ECDD conducted by SCA did not have appropriate regard to Customer 35's higher ML/TF risks: see *Customer 35's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 35's source of funds or source of wealth.

By reason of the matters set out in *Customer 35's risk profile* above, there were real risks that Customer 35's source of wealth and source of funds were not legitimate.

However, it was not until 24 August 2021 that SCA issued a ban in respect of Customer 35.

b. on any occasion prior to August 2021 that senior management considered the higher ML/TF risks posed by Customer 35 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 35 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

Between 7 December 2016 and 24 August 2021, Customer 35 was mentioned in a 'Transaction Monitoring Overview' report for the period 1 August 2018 to 1 November 2018 which was provided to SCA's Senior Management Group for discussion at its meeting.

On 23 August 2021, after elevating Customer 35's risk rating to significant, an SCA AML Compliance Analyst emailed the SCA Chief Operating Officer to determine whether SCA should continue a business relationship with Customer 35. On 23 August 2021, the SCA Chief Operating Officer determined that SCA should cease its business relationship with Customer 35.

On 24 August 2021 SCA issued a ban in respect of Customer 35.

Contravention of s 36 of the Act in respect of Customer 35

1046. By reason of the matters pleaded at paragraphs 1034 to 1045 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 35 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1047. By reason of the matters pleaded at paragraph 1046, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 24 August 2021 with respect to Customer 35.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 36

1048. Customer 36 was a customer of SCA during the relevant period. Between 15 July 2019 and 9 August 2021, SCA recorded turnover exceeding $900,000 for Customer 36.

Particulars

Customer 36 was a customer of SCA from at least 15 July 2019.

On 9 August 2021, SCA issued a ban in respect of Customer 36.

1049. SCA provided Customer 36 with designated services within the meaning of table 3, s 6 of the Act during the relevant period.

Particulars

On 15 July 2019, SCA opened an FMA for Customer 36 which remained open as at 28 October 2022 (item 11, table 3, s 6 of the Act).

See *Customer 36's risk profile* below.

1050. At all times from 15 July 2019, SCA was required to conduct ongoing customer due diligence in respect of Customer 36.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 36's risk profile

1051. On and from 15 July 2019, Customer 36, and the provision of designated services to Customer 36 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 36's risk profile during the relevant period

a. Customer 36 received high value gambling services (table 3, s 6 of the Act) at SCA other than through junket programs. Between 21 December 2019 and 9 August 2021, SCA recorded an estimated buy-in of $5,000, and turnover estimated at $907,367 for Customer 36, with cumulative losses of $96,881;

Particulars

In 2019, Customer 36's recorded individual rated gambling activity at SCA was estimated as turnover for EGMs of $1,376 with wins of $441.

In 2020, despite closures related to the COVID-19 pandemic, Customer 36's recorded individual rated gambling activity at SCA escalated to turnover of $526,350 with losses of $65,314 for both table games and EGMs.

In 2021, Customer 36's recorded individual rated gambling activity at SCA was estimated as a buy-in of $5,000 for table games, and for both table games and EGMs, turnover of $379,641 with losses of $27,007.

b. Customer 36 was connected to other customers at SCA – including players who posed higher ML/TF risks such as Customer 29, Customer 30, Customer 32, Customer 34, Customer 35, and other players in respect of whom SCA had formed suspicions – (including customers who conducted transactions involving the receipt and movement of significant amounts of cash with no apparent economic or visible lawful purpose);

i. SCA had formed suspicions in respect of Customer 36 and their associates;

Particulars

SCA considered it suspicious that:

a. Customer 36 and their associates conducted transactions that were not supported by gambling activity: SMRs dated 24 August 2020 and 15 September 2020;

b. Customer 36 and their associates conducted transactions indicative of ML/TF typologies and vulnerabilities, including structuring, refinement and layering: SMRs dated 26 April 2019, 6 August 2020, 24 August 2020, 21 January 2021 and 5 February 2021;

c. Customer 36 and their associates were conducting third party transactions on each other's behalves, sometimes to apparently misrepresent the origin and destination of the funds and hide the ultimate source of the funds: SMRs dated 6 August 2020, 24 August 2020, 8 September 2020, 15 September 2020, 21 January 2021 and 5 February 2021;

d. Customer 36 and their associates were conducting transactions and gambling at a level that was inconsistent with their stated occupations: SMRs dated 24 August 2020, 8 September 2020, 15 September 2020 and 7 April 2021;

e. Customer 36 and their associates conducted little to no gambling activity to support the amounts of cash and chips exchanged: SMR dated 6 August 2020;

f. Customer 36 and their associates conducted significant cash and chip exchanges in areas with limited surveillance such as the SCA bathrooms and balconies: SMR dated 6 August 2020; and

g. Customer 36 and some of their associates, had family ties to criminals, including known drug dealers: SMRs dated 8 September 2020, 15 September 2020 and 7 April 2021.

ii. Customer 36 and their associates engaged in a series of large cash, chip and other exchange transactions with no visible purpose;

Particulars

Cash handovers

Between 26 April 2019 and 21 March 2021, SCA identified that Customer 36 and their associates engaged in at least four cash handovers with other customers totalling at least $19,000.

Specifically, Customer 36 was observed:

a. exchanging cash with Customer 29 on 2 August 2020; and

b. accepting cash from Customer 35 on 1 September 2020.

Chip handovers

Between 26 April 2019 and 20 March 2021, SCA identified that Customer 36 and their associates engaged in at least 12 chip handovers with other customers totalling at least $62,000.

Specifically, on 2 August 2020, Customer 36 was observed exchanging chips with Customer 29.

c. designated services provided to Customer 36 included substantial EGM activity at SCA;

Particulars

See paragraphs 352 and 353 above.

Between 2019 and 2021, Customer 36's turnover on EGMs was estimated to be $904,301, with a total loss of $96,881.

d. Customer 36 transacted using large amounts of cash and cash that appeared suspicious, including large volumes of cash in small notes, at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 5 August 2020 and 31 July 2021, SCA gave the AUSTRAC CEO 14 TTRs detailing incoming and outgoing payments made by Customer 36 totalling $167,900, and all comprising of chip and cash exchanges.

Between 10 August 2020 and 3 August 2021, SCA gave the AUSTRAC CEO 14 TTRs detailing cash and chip exchanges made by Customer 36 totalling $167,900, which comprised:

a. 12 incoming transactions involving the issuance of chip or tokens totalling $127,900; and

b. two outgoing transactions involving cashing out chips or tokens totalling $40,000.

Large and suspicious cash transactions in 2020

On 2 August 2020, Customer 36 accepted an unknown amount of cash from Customer 29 before making a chip purchase of $7,000 using cash comprising only $50 notes.

On 25 August 2020, Customer 36 gave a wad of cash comprising 30 $100 notes and 100 $50 notes (totalling $8,000) to Customer 32. Customer 32 then claimed to an SCA Cashier the cash was theirs and proceeded to buy chips.

On 1 September 2020, Customer 36 accepted a bundle of cash consisting of 200 $50 notes (totalling $10,000) from Customer 35, before presenting the cash to purchase chips.

e. Customer 36 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including third party structuring;

Particulars

See paragraph 24 above.

Customer 36 was involved in transactions indicative of the ML/TF typology of third-party structuring. For example, on 2 August 2020, Customer 36 was observed accepting an unknown amount of cash from Customer 29 before both individuals approached the Cage to conduct chip purchases of $7,000 and $5,000 respectively. Shortly afterwards, Customer 36 was observed handing an unknown number

of chips to Customer 29. Customer 36 had no recorded play on any table games on or around that day.

f. Customer 36 had access to private gaming rooms at SCA; and

Particulars

See paragraph 145(e) above.

Customer 36 had access to private gaming rooms at SCA, including the Grange Room and Platinum Room.

g. SCA did not have adequate reason to believe that Customer 36's source of wealth or source of funds was sufficient to explain the high value gambling services (table 3, s 6 of the Act) provided to Customer 36 by SCA.

Particulars

See paragraph 516 above.

Since the date Customer 36's account was created, Customer 36's occupation was listed as unemployed.

From at least 1 September 2020, SCA was aware that Customer 36 resided at the same address as, and was likely the spouse of, Customer 30, whose reported occupation was as a 'café worker'.

From at least 1 September 2020, SCA was aware that Customer 36's source of wealth did not adequately explain the amount of money Customer 36 used when gambling at SCA.

Between 15 July 2019 and 9 August 2021, SCA recorded turnover exceeding $900,000 for Customer 36. From 2020, SCA's understanding of Customer 36's source of wealth or source of funds was not commensurate with the high value gambling services that they received at SCA.

Despite having the above knowledge, SCA did not request source of funds information from Customer 36 at any time. On 9 August 2021, SCA requested source of wealth information from Customer 36, but Customer 36 declined to provide that information.

SCA's determination of the ML/TF risks posed by Customer 36

1052. On and from 6 August 2020, Customer 36 was appropriately rated by SCA as a high risk customer for the purpose of the Act and Rules.

1053. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 36 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by it with respect to Customer 36.

Monitoring of Customer 36's transactions

1054. At no time did SCA apply appropriate transaction monitoring to Customer 36's transactions because SCA's transaction monitoring program did not include appropriate risk-based

systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

The review, update and verification of Customer 36's KYC information

1055. SCA did not review, update or verify Customer 36's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 36, including the nature, extent and purpose of their transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 36's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 36's risk profile* above, there were higher ML/TF risks associated with Customer 36's source of wealth or source of funds.

d. to the extent that SCA reviewed Customer 36's KYC information on and from 15 July 2019, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 36.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

On 6 August 2020, SCA conducted a review of Customer 36's transactions on 2 August 2020. An SCA AML Adviser was advised of the findings.

ECDD triggers in respect of Customer 36

1056. SCA was required to apply the ECDD program to Customer 36 following any ECDD triggers in respect of Customer 36.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

1057. Customer 36 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 15 July 2019 and 9 August 2021, SCA gave the AUSTRAC CEO three SMRs with respect to Customer 36.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 36* above.

1058. Each matter pleaded in paragraph 1057 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

1059. SCA did not conduct appropriate risk-based ECDD with respect to Customer 36 following an ECDD trigger because:

a. on each occasion prior to 9 August 2021 that SCA conducted ECDD in respect of Customer 36 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 36 and failed to appropriately consider whether the ML/TF risks posed by Customer 36 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501, 511 and 516 to 517 above.

On 8 September 2020 and 28 October 2020, SCA conducted ECDD in respect of Customer 36.

On 8 September 2020, SCA conducted ECDD in respect of Customer 36 which identified SCA's concerns that Customer 36 was performing threshold transactions on behalf of other customers, including Customer 35. The ECDD further recognised that Customer 36's gambling activity was not commensurate with Customer 36's stated occupation, which was that they were unemployed.

On 28 October 2020, the ECDD screening in respect of Customer 36 identified that:

a. multiple SMRs had been given to the AUSTRAC CEO with respect to Customer 36 in 2020 regarding third-party transactions;

b. Customer 36's stated occupation was unemployed; and

c. Customer 36 was a known associate of the following individuals who SCA considered to be suspicious: Customer 30 (who was identified as Customer 36's spouse), Customer 29, Customer 32, Customer 34 and Customer 35, among others.

However, it was not until 9 August 2021 that SCA issued a ban in respect of Customer 36.

The ECDD conducted by SCA did not have appropriate regard to Customer 36's higher ML/TF risks: see *Customer 36's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 36's source of funds or source of wealth.

By reason of the matters set out in *Customer 36's risk profile* above, there were higher ML/TF risks associated with Customer 36's source of wealth or source of funds.

b. on any occasion prior to August 2021 that senior management considered the higher ML/TF risks posed by Customer 36 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 36 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

At no time prior to August 2021 were the higher ML/TF risks posed by Customer 36 considered by senior management.

Between 4 August 2021 and 5 August 2021, the Chief Operating Officer of SCA was notified by an SCA AML Compliance Manager of the following:

a. a letter would be sent to Customer 36 requesting information concerning Customer 36's source of wealth;

b. SCA would effectively cease doing business with Customer 36 until SCA received a response to its letter and was satisfied with Customer 36s source of wealth; and

c. Customer 36 was identified for a source of wealth check because Customer 36 was identified as an associate of banned patron Customer 29.

On 9 August 2021, SCA issued a ban in respect of Customer 36.

Contravention of s 36 of the Act in respect of Customer 36

1060. By reason of the matters pleaded at paragraphs 1048 to 1059 above, on and from 15 July 2019, SCA:

a. did not monitor Customer 36 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1061. By reason of the matters pleaded at paragraph 1060, SCA contravened s 36(1) of the Act on and from 6 August 2020 to 9 August 2021 with respect to Customer 36.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 37

1062. Customer 37 was a customer of SCA during the relevant period. Between 7 December 2016 and 2021, SCA recorded turnover exceeding $160,000 for Customer 37.

Particulars

Customer 37 was a customer of SCA from at least 1999.

On 29 March 2022, SCA issued a ban in respect of Customer 37 at the direction of the AML team.

1063. SCA provided Customer 37 with designated services within the meaning of table 3, s 6 of the Act during the relevant period.

Particulars

Prior to the relevant period, SCA opened an FMA for Customer 37 which was closed on 29 March 2022 (item 11, table 3, s 6 of the Act).

See *Customer 37's risk profile* below.

1064. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 37.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 37's risk profile

1065. On and from 7 December 2016, Customer 37, and the provision of designated services by SCA to Customer 37, posed higher ML/TF risks because of the following red flags:

Customer 37's risk profile prior to the relevant period

a. by 7 December 2016, Customer 37 had the following risk history:

i. Customer 37 received high value gambling services (table 3, s 6 of the Act) at SCA other than through junket programs; and

Particulars

Between 2001 and November 2016, Customer 37's recorded individual rated gambling activity at SCA was estimated as a buy-in of $1,942,700 for table games, and for both table games and EGMs, turnover of $7,767,872 with losses of $361,489.

ii. Customer 37 transacted using large amounts of cash at SCA.

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 6 December 2013 and 28 April 2016, SCA gave the AUSTRAC CEO four TTRs detailing cash and chip exchanges made by Customer 37 totalling $63,850, which comprised:

a. three incoming transactions involving the issuance of chip or tokens totalling $49,900; and

b. one outgoing transaction involving cashing out chips or tokens totalling $13,950.

Large cash transactions

Between 12 April 2001 to 6 December 2016, SCA recorded that Customer 37 conducted 34 cash buy-ins totalling $1,079,460.

Customer 37's risk history from 7 December 2016

b. Customer 37 received gambling services (table 3, s 6 of the Act) at SCA other than through junket programs. Between 20 January 2017 and 6 August 2021, SCA recorded an estimated buy-in of $148,850, and turnover estimated at $177,952 for Customer 37, with cumulative losses of $16,455;

Particulars

In 2017, Customer 37's recorded individual rated gambling activity at SCA was estimated as a buy-in of $82,800 for table games, and for both table games and EGMs, turnover of $88,299 with losses of $23,233.

In 2018, Customer 37's recorded individual rated gambling activity at SCA was estimated as a buy-in of $47,300 for table games, and for both table games and EGMs, turnover of $43,018 with wins of $8,000.

In 2019, Customer 37's recorded individual rated gambling activity at SCA was estimated as a buy-in of $10,000 for table games, and for both table games and EGMs, turnover of $13,286 with losses of $400.

In 2020, despite closures related to the COVID-19 pandemic, Customer 37's recorded individual rated gambling activity at SCA was

estimated as a buy-in of $500 for table games, and for both table games and EGMs, turnover of $3,182 with losses of $33.

In 2021, Customer 37's recorded individual rated gambling activity at SCA was estimated as a buy-in of $11,250 for table games, and for both table games and EGMs, turnover of $30,168 with losses of $788.

c. from at least January 2017, SCA was aware that Customer 37 was associated with other SCA customers, including players who posed higher ML/TF risks such as Customer 29, Customer 30, Customer 32 and Person 23, and SCA customers that conducted large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

i. the provision of designated services by SCA to Customer 37 and their associates raised red flags reflective of high ML/TF risks;

Particulars

Red flags reflective of higher ML/TF risks included:

a. handing chips and cash to one another: SMRs dated 25 January 2017, 24 August 2020 and 8 October 2020;

b. handing unknown items to one another: SMR dated 8 October 2020;

c. placing cash chips into their clothing and items such as bags: SMR dated 24 August 2020;

d. using their clothing to conceal exchanges of cash chips: SMR dated 24 August 2020;

e. conducting little or no gambling activity to support the amounts of cash and chips exchanged: SMR dated 24 August 2020;

f. exchanging cash for chips at multiple gaming Cashiers, tables or Cages in several transactions: SMR dated 24 August 2020; and

g. conducting significant cash and chip exchanges in areas with limited surveillance such as the SCA bathrooms and balconies: SMR dated 24 August 2020.

ii. SCA formed suspicions in respect of the conduct of Customer 37 and their associates; and

Particulars

SCA considered it suspicious that:

a. Customer 37 and their associates conducted transactions in a secretive manner that was designed to conceal and disguise their associations, and distance themselves and their motives from the transactions, by using agents and family members, initiating transactions through phone calls, and by conducting

transactions with minimal contact: SMRs dated 24 August 2020 and 8 October 2020;

b. Customer 37 and their associates conducted transactions that were not supported by gambling activity: SMR dated 24 August 2020;

c. Customer 37 and their associates conducted cash and chip exchanges that had no identifiable purpose: SMR dated 8 October 2020;

d. Customer 37 and their associates conducted transactions to disguise the true source of their funds: SMR dated 25 January 2017;

e. Customer 37 and their associates were associated with SCA customers who had been arrested or reported to AUSTRAC for drug trafficking and loan sharking offences;

f. SCA was not aware of the nature of the connections or associations between Customer 37 and their associates and customers with whom they conducted transactions: SMR dated 8 October 2020;

g. Customer 37 and their associates did not have occupations that would account for the size and volume of their transactions: SMR dated 24 August 2020; and

h. Customer 37 and their associates conducted transactions indicative of the ML/TF typologies of third party payments, layering, refining, and structuring transactions: SMRs dated 25 January 2017, 24 August 2020 and 8 October 2020.

iii. Customer 37 and their associates engaged in series of large cash, chip and other exchange transactions with no visible lawful purpose;

Particulars

On 20 January 2017, Customer 37 conducted a cash buy-in of $10,000 and passed the chips to Customer 32. SCA noted that Customer 37 rarely played and had not previously conducted a buy-in of that size. SCA staff considered that the cash used by Customer 37 likely belonged to Customer 32, and therefore recorded the transaction under Customer 32's name. SCA considered that it was an attempt by Customer 32 to distance themselves from a large cash transaction: SMR dated 25 January 2017.

On 25 August 2018, Customer 37 provided Person 23 with a bundle of cash. Customer 37 then made a chip buy-in for $7,900 and separately Person 23 made a chip buy-in of $6,100. Customer 37 and Person 23 later attended the Baccarat Pavilion and gamed, before Customer 37 took possession of chips from Person 23 and cashed them out for a total of $29,000.

On 14 August 2020 and 15 August 2020, SCA staff observed a number of suspicious transactions involving the exchange of cash to chips by Customer 37 and Person 23, with unconfirmed portions of the chips then provided to Customer 29, Customer 30 and Customer 32. The total value of the cash to chip exchanges SCA facilitated by Customer 37 and Person 23 was $69,000.

At no point on 14 August 2020 or 15 August 2020 did SCA observe Customer 37 engage in any gambling activity. The transactions appeared to be attempts to refine funds belonging to Customer 29, Customer 30 and Customer 32 and to avoid the transaction reporting threshold for each customer: SMR dated 24 August 2020.

On 26 September 2020 and 27 September 2020, Customer 37 conducted cash buy-ins of $10,000 and $15,000 respectively with funds SCA suspected were provided by Customer 29. Customer 37 gave an unknown amount of chips to Customer 29. SCA believed that Customer 29 was using Customer 37 to conduct threshold transactions on their behalf to avoid reporting requirements: SMR dated 8 October 2020.

d. Customer 37 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 23 January 2017 and 30 December 2020, SCA gave the AUSTRAC CEO 19 TTRs detailing incoming and outgoing payments made by Customer 37 totalling $292,430, which comprised:

a. 18 TTRs totalling $292,430 in chip and cash exchanges; and

b. one TTR totalling $10,000 for an account deposit.

Large cash transactions

See paragraph 1065.c.iii above.

Between 7 December 2016 and 6 August 2021, SCA recorded that Customer 37 conducted cash table buy-ins to the value of $124,850.

e. Customer 37 had access to private gaming rooms at SCA; and

Particulars

See paragraph 145(e) above.

Customer 37 had access to private gaming rooms at SCA, including the Grange Room and the Platinum Room.

f. SCA did not have adequate reason to believe that Customer 37's source of wealth or source of funds was sufficient to explain the high value gambling services (table 3, s 6 of the Act) provided to Customer 37 by SCA.

Particulars

See paragraph 516 above.

On and from 7 December 2016, SCA was aware that Customer 37's occupation was as a 'Process Worker'.

From at least 2017, SCA identified Customer 37 as part of a group of customers who engaged in transactions indicative of ML/TF typologies, including layering and structuring: see particulars to paragraph 1065.c above.

At no time did SCA request or obtain source of funds information or source of wealth information from Customer 37.

At no time was SCA's understanding of Customer 37's source of wealth or source of funds commensurate with the high value financial and gambling services that Customer 37 received at SCA.

SCA's determination of the ML/TF risks posed by Customer 37

1066. On and from 24 February 2017, Customer 37 was appropriately rated by SCA as a high risk customer for the purpose of the Act and Rules.

Particulars

On 25 March 2022, Customer 37 was rated significant risk rating by SCA, which was high risk for the purpose of the Act and Rules.

1067. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 37 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by it with respect to Customer 37.

Monitoring of Customer 37's transactions

1068. At no time did SCA apply appropriate transaction monitoring to Customer 37's transactions because SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

The review, update and verification of Customer 37's KYC information

1069. SCA did not review, update or verify Customer 37's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 37, including the nature, extent and purpose of their transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 37's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 37's risk profile* above, there were higher ML/TF risks associated with Customer 37's source of wealth or source of funds.

On 3 August 2018 SCA was unable to identify Customer 37's occupation through an extensive open source search.

d. to the extent that SCA reviewed Customer 37's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 37.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

ECDD triggers in respect of Customer 37

1070. SCA was required to apply the ECDD program to Customer 37 following any ECDD triggers in respect of Customer 37.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

1071. Customer 37 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 25 January 2017 and 8 October 2020, SCA gave the AUSTRAC CEO three SMRs with respect to Customer 37.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 37* above.

1072. Each matter pleaded in paragraph 1071 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

1073. SCA did not conduct appropriate risk-based ECDD with respect to Customer 37 following an ECDD trigger because:

a. on each occasion prior to March 2022 that SCA conducted ECDD in respect of Customer 37 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 37 and failed to appropriately consider whether the ML/TF risks posed by Customer 37 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501, 511 and 516 to 517 above.

Database watchlist

On 25 January 2017, SCA received a Dow Jones watchlist screening result in respect of Customer 37 which showed that Customer 37 was not recorded on the Dow Jones watchlist.

Transaction reviews

Between January 2017 and October 2020, SCA reviewed SCA's records of Customer 37's transactions on six occasions. The reviews confirmed that Customer 37 had engaged in suspicious transactions with Customer 29, Customer 32 and Customer 30 and that Customer 37 was conducting transactions as a third party for others. SCA's compliance team determined that Customer 37 would continue to be monitored.

ECDD screening

On 3 August 2018 and 12 November 2019, SCA conducted ECDD screening in respect of Customer 37, which identified:

a. the suspicious transactions conducted by Customer 37;

b. the information that SCA had regarding Customer 37's occupation; and

c. Customer 37's lack of gambling activity, noting that Customer 37 rarely played but performed cash transactions as a third party.

The ECDD conducted by SCA in respect of Customer 37 did not have appropriate regard to the higher ML/TF risks posed by Customer 37: see *Customer 37's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 37's source of funds or source of wealth.

By reason of the matters set out in *Customer 37's risk profile* above, there were higher ML/TF risks associated with Customer 37's source of wealth or source of funds.

However, it was not until 29 March 2022 that SCA issued a ban in respect of Customer 37.

b. on any occasion prior to March 2022 that senior management considered the higher ML/TF risks posed by Customer 37 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 37 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

Customer 37 was identified in two 'Transaction Monitoring Overview' reports for the periods 1 November 2017 to 1 February 2018 and 1 February 2018 to 1 May 2018, which were provided to the AML/CTF Senior Management Group for discussion at its meetings.

On 25 March 2022, after elevating Customer 37's risk rating to significant, an SCA AML Compliance Analyst emailed the SCA Chief Operating Officer to determine whether SCA should continue a business relationship with Customer 37. On 27 March 2022, the SCA Chief Operating Officer determined that SCA should discontinue its business relationship with Customer 37.

On 29 March 2022, SCA issued a ban in respect of Customer 37.

Contravention of s 36 of the Act in respect of Customer 37

1074. By reason of the matters pleaded at paragraphs 1062 to 1073 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 37 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1075. By reason of the matters pleaded at paragraph 1074, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 29 March 2022 with respect to Customer 37.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 38

1076. Customer 38 was a customer of SCA during the relevant period. Between 7 December 2016 and 9 August 2021, SCA recorded turnover exceeding $43,000,000 for Customer 38.

Particulars

Customer 38 became a customer of SCA in 2003.

On 9 August 2021, SCA issued a ban in respect of Customer 38.

1077. SCA provided Customer 38 with designated services within the meaning of tables 1 and 3, s 6 of the Act during the relevant period.

Particulars

Prior to 7 December 2016, SCA opened an FMA for Customer 38 which remained open as at 28 October 2022 (item 11, table 3, s 6 of the Act).

While a customer of SCA, Customer 38 remitted funds to and from their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 38's risk profile* below.

1078. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 38.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 38's risk profile

1079. On and from 7 December 2016, Customer 38, and the provision of designated services to Customer 38 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 38's risk profile prior to the relevant period

a. by 7 December 2016, Customer 38 had the following risk history:

   i. SCA formed suspicions for the purposes of s 41 of the Act with respect to Customer 38;

Particulars

SCA gave the AUSTRAC CEO an SMR on one occasion on 1 August 2016. The SMR reported that Customer 38 was knowingly cashing out amounts structured below the reporting threshold.

   ii. SCA was aware that Customer 38 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA; and

Particulars

From 2003 to 2015, Customer 38's recorded individual rated gambling activity at SCA was estimated as a buy-in of $2,027,905 for

table games, and for table games and EGMs, turnover of $11,289,872 and losses of $94,140.

iii. SCA was aware that Customer 38 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 28 August 2013 and 30 November 2016, SCA gave the AUSTRAC CEO 50 TTRs detailing incoming and outgoing payments made by Customer 38 totalling $716,290, which comprised:

a. 42 TTRs totalling $596,290 in chip and cash exchanges; and

b. eight TTRs totalling $120,000 in account deposits.

Customer 38's risk profile during the relevant period

b. Customer 38 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs. Between 7 December 2016 and 5 December 2019 (the last date SCA recorded play for Customer 38 before their ban), SCA recorded an estimated buy-in of $8,995,025, a high turnover estimated at $43,316,082 for Customer 38, with cumulative wins of $33,045;

Particulars

In 2016, Customer 38's recorded individual rated gambling activity at SCA escalated to an estimated buy-in of $2,392,600 for table games, turnover of $10,692,354 and wins of $138,550.

In 2017, Customer 38's recorded individual rated gambling activity at SCA escalated to an estimated buy-in of $3,249,825 for table games, and for both table games and EGMs, turnover of $11,123,811 and wins of $84,177.

In 2018, Customer 38's recorded individual rated gambling activity at SCA escalated to an estimated buy-in of $5,911,000 for table games, and for both table games and EGMs turnover of $22,662,620 and losses of $50,002. In 2018, SCA staff noted that Customer 38 had a gaming preference for baccarat.

In 2019, Customer 38's recorded individual rated gambling activity at SCA was estimated as a buy-in of $2,701,300 for table games, and for both table games and EGMs, turnover of $9,518,915 and losses of $6,336. SCA did not record any play for Customer 38 after 5 December 2019.

c. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 38 by remitting large amounts of money into and out of the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

In an internal report dated July 2020, Bank 1 identified Customer 38 as one of the top customers who deposited money into SCA's bank account during the period 1 September 2018 to 31 August 2019.

Between 2017 and 2019, SCA received 49 telegraphic transfers totalling $1,330,000, each of which was made available to Customer 38's FMA. Some of these transfers were sent from Customer 38's personal bank account.

Between 2017 and 2019, SCA accepted instructions to send seven telegraphic transfers totalling $210,300 from Customer 38's FMA to bank accounts including Customer 38's personal bank account.

d. SCA was aware that Customer 38 had engaged in unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

Particulars

On 4 August 2017, SCA staff observed that Customer 38 cashed out around $50,000 worth of chips, despite only having won approximately $7,000.

On 12 February 2019, SCA staff observed that Customer 38 and their spouse, Customer 39, purchased a total of $10,000 in chips (across two transactions) at a time when no games were running on either table where they completed their buy-ins.

e. Customer 38 was connected to other customers at SCA, in respect of whom SCA had formed suspicions, such as Customer 27, Customer 31, Customer 32 and Customer 38's spouse, Customer 39;

Particulars

Each of these customers was listed as a known associate of Customer 38 in Customer 38's iTrak file.

f. Customer 38 transacted using large amounts of cash and cash that appeared suspicious, including cash that was in poor condition and was covered in dirt as if it had been buried;

Particulars

See paragraphs 376 to 381 above.

Large cash transactions

On 1 November 2017, Customer 38 was named in a 'TG $100k Cumulative Buy-ins' spreadsheet, which showed that Customer 38's total cash buy-in at table games for the period 1 October 2017 to 31 October 2017 was $223,200. Customer 38's spouse, Customer 39, was also included in the spreadsheet, with a total buy-in of $124,300 for the same period.

Suspicious cash

On 4 October 2018, Customer 38 and their spouse Customer 39 conducted a buy-in of $13,000 (structured into two transactions each under the reporting threshold) with cash that was in poor condition and was covered in dirt as if it had been buried.

In October 2019, SCA staff observed that Customer 38 and their spouse, Customer 39, regularly possessed large amounts of cash: SMR dated 16 October 2019.

TTRs

Between 16 January 2017 and 10 December 2019, SCA gave the AUSTRAC CEO 324 TTRs detailing incoming and outgoing payments made by Customer 38 totalling $6,677,515, which comprised:

a. 263 TTRs totalling $5,060,215 in chip and cash exchanges;

b. 56 TTRs totalling $1,495,000 in account deposits; and

c. five TTRs totalling $122,300 in account withdrawals.

g. Customer 38 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including structuring and quick turnover of money (without betting);

Particulars

See paragraph 24 above.

During February 2018, Customer 38 appeared to structure cash buy-ins to remain below the reporting threshold. These cash buy-ins often occurred at gaming tables in circumstances where Customer 38 would accompany the cash buy-in with a chip buy-in: SMR dated 7 March 2018.

On 17 May 2018, Customer 39 gave some cash to Customer 38. Customer 38 and Customer 39 then split up, with Customer 38 entering the Grange Room via Premium Dining, while Customer 39 entered the Grange Room via the Grange toilet corridor. In the Grange Room, Customer 39 conducted a $2,000 cash buy-in and Customer 38 conducted a $9,000 cash buy-in. Customer 38 and Customer 39 later attended the Platinum Cashier. Customer 38 conducted a $9,950 cash-out, and Customer 39 conducted a $2,540 cash-out. Customer 38 gave approximately $9,000 cash to Customer 39 before the pair departed the building together.

In October 2018, frontline SCA staff reported a number of incidents where Customer 38 and Customer 39 structured transactions at the Cage and at gaming tables. SCA staff reported that the structuring behaviour appeared to have escalated around that time, and that Customer 38 and Customer 39 were sharing funds so they could conduct transactions under the reporting threshold: SMR dated 17 October 2018.

On 15 October 2018, Customer 38 conducted three cash buy-ins of $8,000, $5,000 and $4,000: SMR dated 16 October 2018.

h. Customer 38 had access to private gaming rooms at SCA; and

Particulars

See paragraph 145(e) above.

Customer 38 had access to private gaming rooms at SCA, including the Grange Room, the Black Room and the Platinum Room.

i. SCA did not have adequate reason to believe that Customer 38's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 38 by SCA.

Particulars

See paragraph 516 above.

From at least August 2013, SCA recorded that Customer 38's source of wealth and source of funds was from their occupation as a market gardener.

On or around 16 February 2016, SCA entered a note on Bally that SCA needed to obtain Customer 38's occupation details due to the number of threshold transactions conducted. Following this, SCA reported 369 further threshold transactions totalling $7,332,385 in respect of Customer 38.

Despite this, SCA did not take any steps to verify Customer 38's source of wealth and source of funds until 9 August 2021, when Customer 38 was banned from SCA.

In a Source of Wealth Declaration Customer 38 completed shortly after their ban from SCA, Customer 38 declared that their total taxable income for the period from the 2017 financial year to the 2021 financial year was $241,079.

Customer 38's total buy-in at SCA during that same period exceeded $13,500,000 (more than $13,000,000 greater than their taxable income).

At no time was SCA's understanding of Customer 38's source of wealth or source of funds commensurate with the high value financial and gambling services that they received at SCA.

SCA's determination of the ML/TF risks posed by Customer 38

1080. SCA was unable to identify or assess the ML/TF risks posed by Customer 38 appropriately because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 38.

a. On and from 7 December 2016, Customer 38 should have been recognised by SCA as a high risk customer for the purpose of the Act and Rules for the reasons pleaded above: see *Customer 38's risk profile*.

Particulars

Sections 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

b. It was not until 4 May 2018 that Customer 38 was rated high risk for the purpose of the Act and Rules by SCA.

Monitoring of Customer 38's transactions

1081. At no time did SCA apply appropriate transaction monitoring to Customer 38's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 38 through the SCA Customer account channel, which was a high risk remittance channel.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 38's KYC information

1082. SCA did not review, update or verify Customer 38's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 38, including the nature, extent and purpose of Customer 38's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 38's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 38's risk profile* above, there were real risks that Customer 38's source of wealth and source of funds were not legitimate.

Customer 38 declared that their total taxable income for the period from the 2017 financial year to the 2021 financial year was $241,079.

Customer 38's total buy-in at SCA from the 2017 financial year to the 2021 financial year exceeded $13,500,000, despite the fact that their total taxable income in that same period was $241,079.

d. to the extent that SCA reviewed Customer 38's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 38.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

Failure to apply appropriate due diligence suited to the high ML/TF risks

1083. Had SCA conducted ongoing customer due diligence on and from 7 December 2016 by:

a. appropriately identifying and assessing the ML/TF risks posed by Customer 38;

b. applying appropriate risk-based transaction monitoring to Customer 38; and

c. appropriately reviewing and updating Customer 38's KYC information, having regard to the high ML/TF risks,

SCA would have been required by the Act and Rules to apply the ECDD Program to Customer 38 at a time before the date of the ECDD triggers pleaded below: see *ECDD triggers in respect of Customer 38*.

ECDD triggers in respect of Customer 38

1084. SCA was required to apply the ECDD program to Customer 38 following any ECDD triggers in respect of Customer 38.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

1085. Customer 38 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 7 March 2018 and 16 October 2019, SCA gave the AUSTRAC CEO five SMRs pertaining to Customer 38.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 38* above.

1086. Each matter pleaded at paragraph 1085 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

1087. SCA did not conduct appropriate risk-based ECDD with respect to Customer 38 following an ECDD trigger because:

a. on each occasion prior to 9 August 2021 that SCA conducted ECDD in respect of Customer 38 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 38 and failed to appropriately consider whether the ML/TF risks posed by Customer 38 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

On 17 May 2018, an SCA review identified that Customer 38 and Customer 39 were sharing bankroll.

On 24 October 2018, SCA conducted ECDD on Customer 38. SCA noted that no open source information in respect of Customer 38 had been identified.

On 12 February 2019, SCA frontline staff reported that Customer 38 and Customer 39 bought-in for a total of $10,000 split into $4,000 and $6,000 buy-ins. The purchase occurred at one of SCA's gaming pits at a time when there was no game play on either table at which they bought in. Following the report, a compliance investigation found that Customer 38 and Customer 39 were well known to SCA for buying-in at tables for under $10,000, but did not recommend further action.

The ECDD conducted by SCA did not have appropriate regard to Customer 38's higher ML/TF risks: see *Customer 38's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 38's source of funds or source of wealth.

By reason of the matters set out in *Customer 38's risk profile* above, there were real risks that Customer 38's source of wealth and source of funds were not legitimate.

It was not until 9 August 2021 that SCA issued a ban in respect of Customer 38 pending their response to a request for a source of wealth declaration. Customer 38 returned the declaration on or around 24 September 2021, but the ban remained in place because their declared income was not commensurate with their volume of gambling activity (see paragraph 1079.i above).

b. on any occasion prior to 9 August 2021 that senior management considered the higher ML/TF risks posed by Customer 38 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 38 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

Between 1 May 2018 and 1 May 2019, Customer 38 was mentioned in two 'Transaction Monitoring Overview' reports for the periods 1 May 2018 to 1 August 2018 and 1 November 2018 to 1 February 2019. These reports were provided to SCA's Senior Management Group for discussion at its meetings.

The 'Transaction Monitoring Overview' report for the period 1 May 2018 to 1 August 2018 identified that Customer 38 was issued a casino cheque for $50,000 after a baccarat win.

The 'Transaction Monitoring Overview' report for the period 1 November 2018 to 1 February 2019 identified that SCA's Compliance team was aware that Customer 39 was cashing out on behalf of their spouse, Customer 38.

The 'Transaction Monitoring Overview' report for the period 1 February 2019 to 1 May 2019 identified that Customer 39 and their spouse Customer 38 had appeared on the February 2019 report, that Customer 39's play had dropped off in past two months and that Customer 39 cashing out for Customer 38 was an established pattern of behaviour.

It was not until 9 August 2021 that SCA issued a ban in respect of Customer 38.

Contravention of s 36 of the Act in respect of Customer 38

1088. By reason of the matters pleaded at paragraphs 1076 to 1087 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 38 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Section 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1089. By reason of the matters pleaded at paragraph 1088, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 9 August 2021 with respect to Customer 38.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 39

1090. Customer 39 was a customer of SCA during the relevant period. Between 7 December 2016 and 17 November 2019, SCA recorded turnover exceeding $2,700,000 for Customer 39.

Particulars

Customer 39 was a customer of SCA from at least 25 December 2015.

SCA agreed to a request from Customer 39 on 7 December 2019 to bar themselves from SCA. This bar came into force on 9 December 2019 and lapsed on 7 March 2020. SCA then issued a ban of Customer 39 on 10 September 2021, which revoked the initial barring, and which subsequently lapsed on 10 September 2022.

As at 28 October 2022, Customer 39 remained a customer of SCA and had not been banned.

1091. SCA provided Customer 39 with designated services within the meaning of table 3, s 6 of the Act during the relevant period.

Particulars

Prior to the relevant period, SCA opened an FMA for Customer 39 which remained open as at 28 October 2022 (item 11, table 3, s 6 of the Act).

See *Customer 39's risk profile* below.

1092. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 39.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 39's risk profile

1093. On and from 7 December 2016, Customer 39, and the provision of designated services by SCA to Customer 39, posed higher ML/TF risks because of the following red flags:

Customer 39's risk profile prior to the relevant period

a. by 7 December 2016, Customer 39 had the following risk history:

   i. Customer 39 received gambling services (table 3, s 6 of the Act) at SCA;

Particulars

In 2015, Customer 39's recorded individual rated gambling activity at SCA was estimated as a buy-in of $500 for table games, turnover of $3,600, and with losses of $500.

In 2016, Customer 39's recorded individual rated table gambling activity at SCA escalated to an estimated buy-in of $171,100, turnover of $627,676, and with losses of $17,800.

   ii. Customer 39 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 27 January 2016 and 15 November 2016, SCA gave the AUSTRAC CEO three TTRs detailing outgoing payments made by Customer 39 totalling $30,645, which comprised of chip or token cash outs.

Large cash transactions

Between 26 December 2015 and 29 November 2016, Customer 39 made buy-ins using cash totalling $129,200.

Customer 39's risk profile during the relevant period

b. Customer 39 received high value gambling services (table 3, s 6 of the Act) at SCA other than through junket programs. Between 31 December 2016 and 17 November 2019, SCA recorded an estimated buy-in of $1,397,400, a high turnover estimated at $2,794,266 for Customer 39, with cumulative losses of $23,800;

Particulars

In 2017, Customer 39's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $597,700, turnover of $1,386,417, and with wins of $11,500.

In 2018, Customer 39's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $465,900, turnover of $878,919, and with losses of $14,700.

In 2019, Customer 39's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $333,300, turnover of $527,230 and losses of $20,600.

In December 2019, Customer 39 self-excluded from SCA. SCA's records do not record any gambling activity for Customer 39 since their self-exclusion.

c. Customer 39 transacted at SCA using large amounts of cash and cash that appeared suspicious, including large volumes of cash and cash that was in poor condition and was covered in dirt as if it had been buried;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 11 August 2017 and 24 July 2019, SCA gave the AUSTRAC CEO 17 TTRs detailing incoming and outgoing payments made by Customer 39 totalling $305,490, which comprised:

a. 16 TTRs totalling $280,490 in cash and chip exchanges; and

b. one TTR totalling $25,000 for an account deposit.

Large cash transactions

On 1 November 2017, Customer 39 was named in a 'TG $100k Cumulative Buy-ins' spreadsheet, which showed that Customer 39's total cash buy-in at table games for the period 1 October 2017 to 31 October 2017 was $124,300. Customer 39's spouse, Customer 38, was also included in the spreadsheet, with a total buy-in of $223,200 for the same period.

In 2017, Customer 39 made buy-ins using cash totalling $337,100.

In 2018, Customer 39 made buy-ins using cash totalling $364,200.

In 2019, Customer 39 made buy-ins using cash totalling $267,300.

Suspicious cash transactions

On 4 October 2018, Customer 39 attended SCA with their spouse, Customer 38. Customer 39 conducted a $9,000 cash buy-in with $50 notes. The cash was in poor condition and was covered in dirt as if it had been buried. Customer 39 then attended a gaming table and made a second cash buy-in of $4,000. After this buy-in, Customer 39 handed the $4,000 in chips to Customer 38. Customer 39 then went to another gaming table and made a further cash buy-in of $7,000. Customer 39 did not game with the $16,000 in chips they had purchased. Instead, about an hour later, Customer 39 met with Customer 31 and their spouse Person 7. Customer 39 handed an unknown amount of chips to Person 7: SMR dated 9 October 2018. These transactions were indicative of the ML/TF typology of structuring.

In October 2019, SCA staff observed that Customer 39 and their spouse Customer 38 were regularly in possession of large amounts of cash: SMR dated 16 October 2019.

d. SCA was aware that Customer 39 had engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

Particulars

On 13 June 2018, Customer 39 gave an unknown amount of cash to another SCA customer, Person 21, by placing it directly in Person 21's bag while in the Platinum Room. Customer 39, Person 7 and Person 21 used their bodies to shield the exchange from SCA's surveillance camera system: SMR dated 18 June 2018.

In October 2018 and December 2018, Customer 39 was named in an SCA internal report titled 'AML Unusual Changes in Betting'.

e. Customer 39 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including structuring;

Particulars

See paragraph 24 above.

On 6 March 2018, Customer 39 and Customer 38 attended the Grange Room. Customer 39 conducted two cash buy-ins, each in the amount of $9,000, and handed all chips to Customer 38. Customer 39 handed Customer 38 an amount of money in $100 notes after counting it first. As Customer 39 did not hand Customer 38 the total amount of cash in their possession, SCA believed that they may have been deliberately limiting the amount of the buy-in to ensure the amount was under the transaction threshold: SMR dated 8 March 2018.

On 17 May 2018, Customer 39 gave some cash to Customer 38. Customer 39 and Customer 38 then separated, with Customer 38 entering the Grange Room via Premium Dining, while Customer 39 entered the Grange Room via the Grange toilet corridor. In the Grange Room, Customer 39 conducted a $2,000 cash buy-in and Customer 38 conducted a $9,000 cash buy-in. Customer 39 and Customer 38 later attended the Platinum Cashier. Customer 39 conducted a $2,540 cash-out and Customer 38 conducted a $9,950 cash-out. Customer 38 gave approximately $9,000 cash to Customer 39 before the pair departed the building together.

On 16 June 2018, Customer 39 structured a cash out of $11,000 across two different Cashiers: SMR dated 18 June 2018.

On 4 October 2018, Customer 39 conducted three transactions under the reporting threshold within a short period of time, namely a chip purchase of $9,000 and two table buy-ins of $4,000 and $7,000 each. The cash used to purchase the $9,000 worth of chips was covered in dirt as if it had been buried. Customer 39 handed $4,000 in chips to Customer 38 and later met with Customer 31 and Person 7 and discreetly handed an unknown amount of chips to Person 7: SMR dated 9 October 2018.

On 12 February 2019, Customer 39 and their spouse Customer 38 purchased a total of $10,000 of chips (across two transactions) at a time when no games were running on either table where they completed their buy-in: SMR dated 8 March 2018.

On 13 October 2019 and 15 October 2019, Customer 39 conducted multiple chip purchases under the reporting threshold and gave all the chips to their spouse Customer 38 who used the chips to game while Customer 39 did not game. Customer 38 cashed out above the reporting threshold on each day: SMR dated 16 October 2019.

f. Customer 39 was connected to other customers at SCA, including players in respect of whom SCA had formed suspicions (such as Customer 31 and Customer 38);

Particulars

Each of these customers was listed as a known associate of Customer 39 in Customer 39's iTrak file.

See *Customer 31's risk profile* and *Customer 38's risk profile* above.

g. Customer 39 had access to private gaming rooms at SCA; and

Particulars

See paragraph 145(e) above.

Customer 39 had access to private gaming rooms at SCA, including the Grange Room, the Black Room and the Platinum Room.

h. SCA did not have adequate reason to believe that Customer 39's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (table 3, s 6 of the Act) provided to Customer 39 by SCA.

Particulars

See paragraph 516 above.

From at least January 2016, SCA recorded that Customer 39's source of wealth and source of funds was from their occupation as a farmer, and from at least October 2018 as an owner and operator of a farm.

Between 2017 and 2019, Customer 29's total buy-in was around $1,400,000.

On 12 August 2021, SCA requested source of wealth and source of funds information from Customer 39. At that time, Customer 39 did not have any recorded gambling activity at SCA since 7 December 2019.

On 24 September 2021 SCA obtained source of wealth information relating to Customer 39 from Customer 38, which showed that Customer 39 received approximately $58,000 for the 2021 financial year and $42,000 for the 2022 financial year for their share in the profits from the company Customer 39 and Customer 38 owned and operated. Other documents that Customer 38 provided suggested that Customer 39's share in the profits from their company would have been fairly similar for the 2017 to 2019 financial years.

SCA understood that Customer 39's sole source of wealth and funds was from the company owned and operated by Customers 38 and 39. Customer 39's gambling activity was not commensurate with their gaming being funded by their profit share from this company. This source of wealth information was obtained after Customer 39 was banned from SCA. SCA allowed Customer 39's ban to lapse on 10 September 2022.

At no time was SCA's understanding of Customer 39's source of wealth or source of funds commensurate with the high value financial and gambling services that they received at SCA.

SCA's determination of the ML/TF risks posed by Customer 39

1094. SCA was unable to identify or assess the ML/TF risks posed by Customer 39 appropriately because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 39.

a. On and from 7 December 2016, Customer 39 should have been recognised by SCA as a high risk customer for the purpose of the Act and Rules for the reasons pleaded above: see *Customer 39's risk profile* above.

Particulars

Sections 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

b. It was not until 21 May 2018 that Customer 39 was rated high risk for the purpose of the Act and Rules by SCA.

Particulars

On 1 December 2017, Customer 39 was rated moderate risk, which was medium risk for the purpose of the Act and Rules.

On 21 May 2018, Customer 39 was rated high risk.

Monitoring of Customer 39's transactions

1095. At no time did SCA apply appropriate transaction monitoring to Customer 39's transactions because SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

The review, update and verification of Customer 39's KYC information

1096. SCA did not review, update or verify Customer 39's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 39, including the nature, extent and purpose of Customer 39's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 39's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 39's risk profile* above, there were real risks that Customer 39's source of wealth and source of funds were not legitimate.

d. to the extent that SCA reviewed Customer 39's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 39.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

On 7 June 2017 and 8 March 2018, SCA conducted a Jade search in relation to Customer 39. No results were returned.

Failure to apply appropriate due diligence suited to the high ML/TF risks

1097. Had SCA conducted ongoing customer due diligence on and from 7 December 2016 by:

a. appropriately identifying and assessing the ML/TF risks posed by Customer 39;

b. applying appropriate risk-based transaction monitoring to Customer 39; and

c. appropriately reviewing and updating Customer 39's KYC information, having regard to the high ML/TF risks,

SCA would have been required by the Act and Rules to apply the ECDD Program to Customer 39 at a time before the date of the ECDD triggers pleaded below: see *ECDD triggers in respect of Customer 39*.

ECDD triggers in respect of Customer 39

1098. SCA was required to apply the ECDD program to Customer 39 following any ECDD triggers in respect of Customer 39.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

1099. Customer 39 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 18 June 2018 and 16 October 2019, SCA gave the AUSTRAC CEO six SMRs with respect to or pertaining to Customer 39.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 39* above.

1100. Each matter pleaded at paragraph 1099 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

1101. SCA did not conduct appropriate risk-based ECDD with respect to Customer 39 following an ECDD trigger because:

a. on each occasion prior to 10 September 2021 that SCA conducted ECDD in respect of Customer 39 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 39 and failed to appropriately consider whether the ML/TF risks posed by Customer 39 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

On 19 December 2019, after Customer 39 had self-excluded, SCA conducted ECDD in respect of Customer 39. SCA recorded concerns that Customer 39 and Customer 38 appeared to have structured transactions to avoid the transaction reporting threshold, that Customer 39's occupation was recorded as 'farmer', and that there was no open source information available in respect of Customer 39. These concerns replicated concerns contained in an SMR dated 16 October 2019.

The ECDD conducted by SCA did not have appropriate regard to Customer 39's higher ML/TF risks: see *Customer 39's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 39's source of funds or source of wealth.

By reason of the matters set out in *Customer 39's risk profile* above, there were real risks that Customer 39's source of wealth and source of funds were not legitimate.

On 9 December 2019 Customer 39 self-excluded from SCA. SCA then issued a ban of Customer 39 on 10 September 2021 which replaced the initial ban and subsequently lapsed on 10 September 2022.

b. on any occasion prior to 10 September 2021 that senior management considered the higher ML/TF risks posed by Customer 39 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 39 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

Between 1 February 2018 and 1 November 2019, Customer 39 was mentioned in five 'Transaction Monitoring Overview' reports. These reports were provided to SCA's Senior Management Group for discussion at its meetings. The reports identified that Customer 39 had regular occurrences of buying-in with little or no corresponding play, and made cash outs on behalf of their spouse Customer 38.

On 9 December 2019, Customer 39 self-excluded from SCA. SCA then issued a ban of Customer 39 on 10 September 2021 which replaced the initial ban and subsequently lapsed on 10 September 2022.

Contravention of s 36 of the Act in respect of Customer 39

1102. By reason of the matters pleaded at paragraphs 1090 to 1101 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 39 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1103. By reason of the matters pleaded at paragraph 1102, SCA contravened s 36(1) of the Act on and from 21 May 2018 with respect to Customer 39.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 40

1104. Customer 40 was a customer of SCA during the relevant period. Between 3 January 2018 and 26 November 2021, SCA recorded turnover exceeding $32,000,000 for Customer 40.

Particulars

Customer 40 was a customer of SCA from at least 3 January 2018.

On 26 November 2021, SCA issued a ban in respect of Customer 40 at the direction of the SCA AML team.

1105. SCA provided Customer 40 with designated services within the meaning of table 3, s 6 of the Act during the relevant period.

Particulars

On 3 January 2018, SCA opened an FMA for Customer 40 which remained open as at 28 October 2022 (item 11, table 3, s 6 of the Act).

See *Customer 40's risk profile* below.

1106. At all times from 3 January 2018, SCA was required to conduct ongoing customer due diligence in respect of Customer 40.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 40's risk profile

1107. On and from 3 January 2018, Customer 40, and the provision of designated services to Customer 40 by SCA, posed higher ML/TF risks because of the following red flags:

a. Customer 40 received high value gambling services (table 3, s 6 of the Act) at SCA other than through junket programs. Between 3 January 2018 and 26 November 2021, SCA recorded buy-in estimated at $6,562,075 for Customer 40, high turnover estimated at $32,085,456, with cumulative losses of $794,852;

Particulars

In 2018, Customer 40's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $605,985, turnover of $2,481,980 and losses of $83,785.

In 2019, Customer 40's recorded individual rated gambling activity at SCA for table games escalated to an estimated buy-in of $1,555,350, turnover of $7,015,044 and losses of $163,715.

In 2020, despite closures related to the COVID-19 pandemic, Customer 40's recorded individual rated gambling activity at SCA escalated to an estimated buy-in of $2,694,040 for table games, and

for both table games and EGMs, turnover of $8,991,389 and losses of $285,220.

In 2021, until they were banned on 26 November 2021, Customer 40's recorded individual rated gambling activity at SCA was estimated as a buy-in of $1,706,700 for table games, and for both table games and EGMs, turnover of $13,597,043 and losses of $262,132.

b. SCA was aware that Customer 40 had engaged in:

   i. large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

   ii. transactions involving using large amounts of cash and cash that appeared to be wet and dirty; and

   iii. transactions indicative of ML/TF typologies and vulnerabilities, including structuring;

Particulars

See paragraphs 24, and 376 to 381 above.

TTRs

Between 11 July 2018 and 13 April 2021, SCA gave the AUSTRAC CEO 36 TTRs detailing chip and cash exchanges made by Customer 40 totalling $485,075, which comprised:

a. 22 incoming transactions involving the issue of chip or tokens totalling $311,000; and

b. 14 outgoing transactions involving cashing out chips or tokens totalling $174,075.

Large and suspicious transactions, including transactions indicative of structuring

On 7 December 2020, Customer 40 cashed out $8,220 worth of gaming chips at SCA. Immediately following this transaction, another SCA customer, Person 24, cashed out $10,000 worth of gaming chips. Immediately after this, Customer 40 cashed out a further $1,900 worth of gaming chips. During this transaction, Customer 40 was holding an additional $5,000 in gaming chips, however they did not exchange these chips. Customer 40 and Person 24 then proceeded to another area of the casino, where they appeared to split up the cash from Person 24's transaction. SCA recorded that Customer 40 had used a third party to structure a series of transactions to avoid the threshold reporting requirement: SMR dated 11 December 2020.

On 27 January 2021, Customer 40 purchased chips for $16,000 with cash that was damp, soiled and in a variety of denominations. Immediately following this transaction, Customer 40 approached a gaming table and exchanged a $5,000 chip for five $1,000 chips. Customer 40 then entered the toilets. A few minutes later, after

coming out of the toilets, Customer 40 gave a $5,000 chip to another SCA customer. Customer 40 then attended a Cashier and exchanged $9,000 worth of gaming chips for cash. Two minutes later, the other customer attended the same Cashier and exchanged $6,000 worth of gaming chips for $5,000 in cash, and deposited the remaining $1,000 into their FMA. The customer then handed the cash to Customer 40. SCA recorded that Customer 40 did not engage in any gambling activity between the above transactions. SCA was not aware of any known association between Customer 40 and the other customer. SCA recorded that Customer 40 had used a third party to structure transactions in order to avoid the threshold reporting requirement: SMR dated 28 January 2021.

On 18 July 2021, Customer 27 approached Customer 40 at an EGM and took Customer 40's member card. Customer 27 then attempted to cash out $15,000 in cash chips (comprised of three $5,000 chips) and $5,000 in cash using Customer 40's card. The SCA Cashier declined the transaction due to the card belonging to Customer 40. Customer 27 subsequently returned to the Cashier with Customer 40, who confirmed the request and was issued with two $10,000 cash chips. Customer 40 then handed the cash chips to Customer 27. SCA recorded that Customer 27 had used Customer 40 to conduct the transactions on their behalf to avoid being detected: SMR dated 11 August 2021.

On 27 October 2021, SCA staff observed that Customer 40 and their associate entered the toilets together. Customer 40 exited shortly after and was observed with $5,000 in cash in their hand. The other customer exited the toilets a few minutes later. Customer 40 then attended a Cashier and exchanged $5,000 in cash for chips. The SCA Cashier struggled to count the notes, which appeared to be wet or dirty. Shortly after, the other SCA customer attended the same Cashier and exchanged $5,000 in cash to chips. The customer then approached Customer 40 at an EGM and passed the chips to Customer 40. SCA recorded that Customer 40 had utilised their associate to structure a buy-in, to avoid scrutiny over their funds: SMR dated 2 November 2021.

On 18 November 2021, Customer 40 played on an EGM for several hours using another SCA customer's card. Customer 40 subsequently used their own card and then printed a $2,000 TITO. Customer 40 then inserted the other customer's card again and printed another $2,000 TITO. Customer 40 cashed out both TITOs and received $4,000 in cash. While Customer 40 was conducting this cash out, a known associate of Customer 40 inserted $200 in cash into the EGM that Customer 40 had just been playing on while the other customer's card was still inserted and placed two bets of $100 each. Customer 40 returned to the EGM, withdrew a TITO for $200 and then withdrew the customer's card. Customer 40 then inserted their own membership card and inserted the TITO. SCA recorded that

Customer 40 was concealing their gambling activity by using another customer's account: SMR dated 25 November 2021.

c. SCA was aware that Customer 40 was connected to other customers at SCA, including players who posed higher ML/TF risks and players who SCA considered had acted suspiciously such as Customer 27, Customer 41 and Person 24;

Particulars

See *Customer 27's risk profile* above and *Customer 41's risk profile* below.

See particulars to paragraph 1107.b above.

On 27 August 2018, SCA formed the suspicion that Customer 40's associates, including Customer 41, were part of a prostitution syndicate and were potentially attempting to launder funds at SCA.

In December 2020, one of Customer 40's associates, Person 24, was found to be in possession of counterfeit notes at SCA and was interviewed by a law enforcement agency. After the incident, Person 24 departed the premises with Customer 40 and two other customers.

By December 2020, SCA was aware that Customer 40 was conducting suspicious transactions with other customers, including Customer 27. Customer 27 was a significant risk patron who engaged in possible loan sharking behaviour, and was banned by SCA in November 2021.

d. designated services provided to Customer 40 included substantial EGM activity at SCA;

Particulars

See paragraphs 352 and 353 above.

Between 29 August 2020 and 25 November 2021, Customer 40 gambled on EGMs at SCA. During this period, Customer 40's EGM activity was recorded as a turnover of over $7,741,651, with losses of $92,077.

e. in August 2018, a law enforcement agency shared information pertaining to Customer 40 with SCA;

Particulars

On 23 August 2018, SCA received information from a law enforcement agency that a prostitution syndicate would potentially be visiting SCA to launder their funds. Shortly after this on 27 August 2018, SCA formed the suspicion that Customer 40's associates were involved in the same prostitution syndicate.

f. Customer 40 had access to private gaming rooms at SCA;

Particulars

See paragraph 145(e) above.

Customer 40 had access to private gaming rooms at SCA, including the Platinum Room and the Grange Room.

g. following their ban in November 2021, Customer 40 continued to attend SCA on at least three occasions, and on at least one occasion conducted transactions; and

Particulars

On 26 November 2021, Customer 40 was banned from SCA at the direction of the AML team.

On 26 December 2021, Customer 40 attended SCA. SCA staff checked Customer 40's file and determined that they had been banned. Customer 40 was asked to leave the premises.

On 2 January 2022, Customer 40 attended SCA with another SCA customer. The other customer retrieved a bundle of $50 notes from their bag and gave several notes to Customer 40. Customer 40 then used this cash to gamble on an EGM. Over the next two hours, Customer 40 and the other customer continued to pass notes between each other and gamble on EGMs. An SCA VIP Host then approached Customer 40 and the other customer, while Customer 40 printed a TITO for $1,100 from the EGM. Customer 40 attended an SCA Cashier and exchanged the TITO for cash. The SCA VIP Host then accompanied Customer 40 to exit the premises. The VIP Host subsequently informed an SCA AML Compliance Analyst that Customer 40 had attended SCA while banned.

On 27 January 2022, Customer 40 again attended SCA. SCA staff checked Customer 40's file and determined that they had been banned. Customer 40 was asked to leave the premises.

h. SCA did not have adequate reason to believe that Customer 40's source of wealth or source of funds was sufficient to explain the high value gambling services (table 3, s 6 of the Act) provided to Customer 40 by SCA.

Particulars

See paragraph 516 above.

From 3 January 2018, when Customer 40 became a customer at SCA, until 1 November 2021, SCA recorded Customer 40's occupation in their Bally system as 'Waitress'.

By August 2018, SCA had formed a suspicion that some of Customer 40's known associates were part of a prostitution syndicate and were potentially attending SCA to launder money.

In December 2020 and August 2021, SCA reported in three SMRs given to the AUSTRAC CEO that Customer 40's level of gambling at SCA was not commensurate with their stated occupation as a waitress. SCA recorded in December 2020 that Customer 40's gambling activity indicated that they had access to funds well above

what could reasonably be earned on a waitress' salary: SMRs dated 11 December 2020, 28 January 2021 and 11 August 2021.

On 24 August 2021, SCA requested that Customer 40 complete a Source of Wealth Declaration. Customer 40 completed the Declaration on the same date. In the Declaration, Customer 40 stated that:

a. Customer 40's occupation was a homemaker;

b. Customer 40's ex-partner had come into SCA on the same day and provided documentation stating that they fully supported Customer 40's gambling. The documentation consisted of the ex-partner's income statement and superannuation withdrawals; and

c. Customer 40 gave all of their money to their relative overseas.

The supporting documentation provided by Customer 40 indicated that their ex-partner's annual income for the period from the 2019 financial year to the 2021 financial year ranged between approximately $4,700 and $94,600. It also suggested that Customer 40's relative was potentially conducting remittance to Australian residents, who then supplied Customer 40 with Australian currency.

On 2 November 2021, SCA reported in an SMR given to the AUSTRAC CEO that the Source of Wealth Declaration completed by Customer 40 in August 2021 provided minimal information regarding Customer 40's source of wealth. SCA recorded that Customer 40's stated occupation, and the lack of information surrounding Customer 40's source of wealth, created further concerns around the legitimacy of Customer 40's source of funds: SMR dated 2 November 2021.

On 25 November 2021, SCA reported in an SMR given to the AUSTRAC CEO that Customer 40 was conducting transactions on another customer's account, potentially to conceal their gaming actions due to source of wealth enquiries. SCA again recorded that Customer 40's source of wealth information and stated occupation raised concerns regarding the legitimacy of Customer 40's source of funds: SMR dated 25 November 2021. On 26 November 2021, SCA issued Customer 40 with a ban due to their inadequate source of wealth.

Between January 2018 and November 2021, SCA recorded that Customer 40 had a total cash buy-in exceeding $2,800,000. At no time was SCA's understanding of Customer 40's source of wealth or source of funds commensurate with the high value gambling services that they received at SCA.

SCA's determination of the ML/TF risks posed by Customer 40

1108. SCA was unable to identify or assess the ML/TF risks posed by Customer 40 appropriately because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 40.

a. On and from August 2018, Customer 40 should have been recognised by SCA as a high risk customer for the purpose of the Act and Rules for the reasons pleaded above: see *Customer 40's risk profile* above.

Particulars

Sections 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

b. It was not until 15 December 2020 that Customer 40 was rated high risk for the purpose of the Act and Rules by SCA.

Particulars

On or around 22 October 2021, Customer 40's risk rating was elevated to significant risk, which was high risk for the purpose of the Act and Rules.

Monitoring of Customer 40's transactions

1109. At no time did SCA apply appropriate transaction monitoring to Customer 40's transactions because SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

The review, update and verification of Customer 40's KYC information

1110. SCA did not review, update or verify Customer 40's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 40, including the nature, extent and purpose of Customer 40's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 40's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 40's risk profile* above, there were real risks that Customer 40's source of wealth and source of funds were not legitimate.

d. to the extent that SCA reviewed Customer 40's KYC information on and from 3 January 2018, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 40.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

Failure to apply appropriate due diligence suited to the high ML/TF risks

1111. Had SCA conducted ongoing customer due diligence on and from 3 January 2018 by:

a. appropriately identifying and assessing the ML/TF risks posed by Customer 40;

b. applying appropriate risk-based transaction monitoring to Customer 40; and

c. appropriately reviewing and updating Customer 40's KYC information, having regard to the high ML/TF risks,

SCA would have been required by the Act and Rules to apply the ECDD Program to Customer 40 at a time before the date of the ECDD triggers pleaded below: see *ECDD triggers in respect of Customer 40*.

ECDD triggers in respect of Customer 40

1112. SCA was required to apply the ECDD program to Customer 40 following any ECDD triggers in respect of Customer 40.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

1113. Customer 40 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 11 December 2020 and 25 November 2021, SCA gave the AUSTRAC CEO five SMRs relating to Customer 40.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 40* above.

1114. Each matter pleaded at paragraph 1113 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

1115. SCA did not conduct appropriate risk-based ECDD with respect to Customer 40 following an ECDD trigger because:

a. on each occasion prior to 26 November 2021 that SCA conducted ECDD in respect of Customer 40 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 40 and failed to appropriately consider whether the ML/TF risks posed by Customer 40 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

Transaction reviews

Between December 2020 and November 2021, SCA reviewed transactions involving Customer 40 at SCA on five occasions. These transactions were conducted between 7 December 2020 and 18 November 2021: see particulars to paragraph 1107.b above.

ECDD screening

On or around 7 January 2021, SCA conducted ECDD screening in respect of Customer 40. The screening recorded that:

a. Customer 40's occupation was as a waitress; and

b. Customer 40 had a number of known associates, including Customer 27.

The ECDD conducted by SCA did not have appropriate regard to Customer 40's higher ML/TF risks: see *Customer 40's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 40's source of funds or source of wealth.

By reason of the matters set out in *Customer 40's risk profile* above, there were real risks that Customer 40's source of wealth and source of funds were not legitimate.

However, it was not until 26 November 2021 that SCA issued a ban in respect of Customer 40.

b. on any occasion prior to 26 November 2021 that senior management considered the higher ML/TF risks posed by Customer 40 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 40 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

On or around 1 November 2021, after elevating Customer 40's risk rating to significant, an SCA AML Analyst prepared an internal memorandum for the SCA Chief Operating Officer and the SCA General Counsel and Company Secretary to determine whether SCA should continue a business relationship with Customer 40. The memorandum noted that:

a. Customer 40 had been unable to provide adequate information and documentation regarding their source of wealth;

b. since the creation of Customer 40's account at SCA in 2018, their occupation had been recorded as a waitress;

c. Customer 40 had provided a source of wealth declaration form in August 2021, which suggested that Customer 40's only source of wealth came from gifts;

d. Customer 40 had been the subject of three SMRs for attempting to structure cash outs and avoid reporting obligations;

e. in January 2019, Customer 40 stole $600 worth of chips from another SCA customer; and

f. there were concerns that Customer 40 was linked to an illegal prostitution syndicate and potentially had access to proceeds of crime.

The memorandum recommended that SCA discontinue its business relationship with Customer 40 until Customer 40 provided documentation which justified a legitimate source of wealth.

On 22 November 2021, SCA determined to terminate its business relationship with Customer 40 due to their inadequate source of wealth.

On 26 November 2021, SCA issued a ban in respect of Customer 40.

Contravention of s 36 of the Act in respect of Customer 40

1116. By reason of the matters pleaded at paragraphs 1104 to 1115 above, on and from 3 January 2018, SCA:

a. did not monitor Customer 40 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1117. By reason of the matters pleaded at paragraph 1116, SCA contravened s 36(1) of the Act on and from 3 January 2018 to 26 November 2021 with respect to Customer 40.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 41

1118. Customer 41 was a customer of SCA during the relevant period. Between 30 July 2018 and 9 December 2021, SCA recorded turnover exceeding $8,700,000 for Customer 41.

Particulars

Customer 41 was a customer of SCA from at least 30 July 2018.

On 9 December 2021, SCA issued a ban in respect of Customer 41 at the recommendation of the SCA AML team.

1119. SCA provided Customer 41 with designated services within the meaning of table 1 and table 3, s 6 of the Act during the relevant period.

Particulars

On 30 July 2018, SCA opened an FMA for Customer 41 which was closed on 9 December 2021 (item 11, table 3, s 6 of the Act).

See *Customer 41's risk profile* below.

1120. At all times from 30 July 2018, SCA was required to conduct ongoing customer due diligence in respect of Customer 41.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 41's risk profile

1121. On and from 30 July 2018, Customer 41, and the provision of designated services to Customer 41 by SCA, posed higher ML/TF risks because of the following red flags:

a. Customer 41 received high value gambling services (table 3, s 6 of the Act) at SCA other than through junket programs. Between 30 July 2018 and 9 December 2021, SCA

recorded an estimated buy in of $1,119,220, a high and escalating turnover of $8,775,740 for Customer 41, with cumulative losses of $228,346;

Particulars

In 2018, Customer 41's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $38,350, turnover of $85,325 and losses of $13.

In 2019, Customer 41's recorded individual rated gambling activity at SCA escalated to an estimated buy-in of $450,800 for table games, and for both table games and EGMs, turnover of $1,459,530 and losses of $104,000.

In 2020, despite closures related to the COVID-19 pandemic, Customer 41's recorded individual rated gambling activity at SCA escalated to an estimated buy-in of $630,070 for table games, and for both table games and EGMs, turnover of $3,449,387 and losses of $53,695.

In 2021, Customer 41's recorded individual rated gambling activity at SCA escalated to an estimated $1,336,395 for table games, and for both table games and EGMs, turnover of $3,781,497 and losses of $57,301.

From at least 18 November 2021, SCA was aware that most of Customer 41's gaming consisted of baccarat in the Grange Room.

b. Customer 41 was connected to other customers at SCA, including players who posed higher ML/TF risks such as Customer 40, Customer 42 and Customer 58 and other customers who SCA considered had acted suspiciously;

Particulars

From at least 31 July 2018, SCA was aware that Customer 41 was associated with Customer 42 and that the two individuals had attempted to cash out chips on behalf of a third individual who refused to provide identification.

On 27 August 2018, SCA formed the suspicion that Customer 41 and Customer 42 were part of a prostitution syndicate and were potentially attempting to launder funds at SCA.

On 20 December 2020, Customer 41 was identified exiting SCA with an individual who had been questioned by a law enforcement agency on the same day for attempting to use counterfeit notes (two $50 notes) at SCA.

c. designated services provided to Customer 41 included EGM activity at SCA;

Particulars

See paragraphs 352 and 353 above.

Between 2018 and 2021, Customer 41's turnover on EGMs was estimated to be $16,008 with a loss of $1,146.

d. Customer 41 transacted using large amounts of cash and cash that appeared suspicious at SCA, including large volumes of cash in small notes at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 31 July 2018 and 24 August 2021, SCA gave the AUSTRAC CEO three TTRs detailing outgoing chip and cash exchanges made by Customer 41 totalling $34,805.

Large and suspicious cash transactions in 2021

On 24 August 2021, Customer 41 was observed accepting 20 $100 notes ($2,000 in total) from an individual before using this cash to purchase chips. SCA suspected that this was an attempt by Customer 41 to help the individual avoid being identified.

e. Customer 41 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including structuring;

Particulars

See paragraph 24 above.

On the following occasions, Customer 41 was involved in transactions indicative of the ML/TF typology of structuring:

a. on 30 July 2018, Customer 41 attempted to exchange $5,000 worth of chips for cash, but was refused due to the chips belonging to another individual who refused to provide identification. Customer 41 and their associates repeatedly attempted to exchange chips for cash for up to a total of $11,000 on behalf of the same individual before SCA banned all of the individuals from SCA for 24 hours, with security escorting them off the premises. Shortly after being escorted out, Customer 41 and Customer 41's associates were observed re-entering the SCA premises; and

b. on 24 August 2021, another customer gave Customer 41 $2,000 comprised of $100 notes and then proceeded to make a cash buy-in of $2,000. Customer 41 then accepted what appeared to be $4,300 in cash chips, comprising four $1,000 and three $100 cash chips from the same person. Customer 41 proceeded to cash out $8,500 and then immediately handed the cash to the third party. Shortly afterwards, Customer 41 exchanged a further $2,300 in chips for cash.

In 2020, Customer 41 was included in an SCA internal report titled 'AML Unusual Changes in Betting'.

f. Customer 41 had access to private gaming rooms at SCA;

Particulars

See paragraph 145(e) above.

Customer 41 had access to private gaming rooms at SCA, including the Grange Room and the Black Room.

g. by 27 August 2018, SCA suspected that Customer 41 and their associates were involved in an illegal escort and prostitution syndicate; and

Particulars

On 23 August 2018, SCA received information from a law enforcement agency that an illegal escort and prostitution syndicate would potentially be visiting SCA to launder their funds.

On 27 August 2018, SCA formed the suspicion that Customer 41 and their associates were involved in the same illegal escort and prostitution syndicate.

h. SCA did not have adequate reason to believe that Customer 41's source of wealth or source of funds was sufficient to explain the high value gambling services (table 3, s 6 of the Act) provided to Customer 41 by SCA.

Particulars

See paragraph 516 above.

On 30 August 2018 and 25 June 2021, Customer 41 provided occupation details to SCA. On both of these occasions, Customer 41 stated that their occupation was 'home duties'. This source of wealth information was not consistent with Customer 41's escalating turnover on table games and EGMs, which was over $80,000 in 2018, over $1,000,000 in 2019, and over $3,000,000 in each of 2020 and 2021.

In 2018, SCA became aware that Customer 41 was involved in an illegal escort and prostitution syndicate which was suspected of laundering funds at SCA. Despite this, SCA took no steps to verify the source of wealth or source of funds information Customer 41 had provided to it.

Despite the above, it was not until 24 August 2021 that SCA sought source of wealth information from Customer 41. In response to this request, Customer 41 provided minimal information and claimed that their parent and ex-partner fully supported their gaming. The ex-partner provided an income statement indicating an annual income of approximately $84,000 and superannuation withdrawals totalling $49,000.

At no time was SCA's understanding of Customer 41's source of wealth or source of funds commensurate with the high value financial and gambling services that they received at SCA.

SCA's determination of the ML/TF risks posed by Customer 41

1122. SCA was unable to identify or assess the ML/TF risks posed by Customer 41 appropriately because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 41.

a. By August 2018, Customer 41 should have been recognised by SCA as a high risk customer for the purpose of the Act and Rules for the reasons pleaded above: see *Customer 41's risk profile* above.

Particulars

Sections 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

b. It was not until 31 December 2020 that Customer 41 was rated high risk for the purpose of the Act and Rules by SCA.

Particulars

On or around 18 November 2021, SCA escalated Customer 41's risk rating to significant risk, which was high risk for the purpose of the Act and Rules.

Monitoring of Customer 41's transactions

1123. At no time did SCA apply appropriate transaction monitoring to Customer 41's transactions because SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

The review, update and verification of Customer 41's KYC information

1124. SCA did not review, update or verify Customer 41's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 41, including the nature, extent and purpose of Customer 41's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 41's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 41's risk profile* above, there were higher ML/TF risks associated with Customer 41's source of wealth or source of funds.

d. to the extent that SCA reviewed Customer 41's KYC information on and from 30 July 2018, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 41.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

On 30 July 2018 and 27 August 2018, SCA performed due diligence in relation to Customer 41, which noted that:

a. on 30 July 2018, Customer 41 was banned from SCA for 24 hours following repeated attempts to exchange $5,000 worth of chips for cash, on behalf of another individual;

b. on 23 August 2018, a law enforcement agency supplied information to SCA indicating that a prostitution syndicate could potentially be visiting SCA to launder their funds; and

c. on 27 August 2018, SCA formed the suspicion that Customer 41 and Customer 41's associates formed part of the prostitution syndicate.

See paragraph 138(h) above.

Failure to apply appropriate due diligence suited to the high ML/TF risks

1125. Had SCA conducted ongoing customer due diligence on and from 30 July 2018 by:

a. appropriately identifying and assessing the ML/TF risks posed by Customer 41;

b. applying appropriate risk-based transaction monitoring to Customer 41; and

c. appropriately reviewing and updating Customer 41's KYC information, having regard to the high ML/TF risks,

SCA would have been required by the Act and Rules to apply the ECDD Program to Customer 41 at a time before the date of the ECDD triggers pleaded below: see *ECDD triggers in respect of Customer 41*.

ECDD triggers in respect of Customer 41

1126. SCA was required to apply the ECDD program to Customer 41 following any ECDD triggers in respect of Customer 41.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

1127. Customer 41 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 30 July 2018 and 9 December 2021, SCA gave the AUSTRAC CEO two SMRs with respect to or pertaining to Customer 41.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 41* above.

1128. Each matter pleaded at paragraph 1127 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

1129. SCA did not conduct appropriate risk-based ECDD with respect to Customer 41 following an ECDD trigger because:

a. on each occasion prior to 9 December 2021 that SCA conducted ECDD in respect of Customer 41 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 41 and failed to appropriately consider whether the ML/TF risks posed by Customer 41 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

On 24 August 2021, 9 December 2021 and 13 December 2021, SCA conducted ECDD in respect of Customer 41.

On 24 August 2021, the ECDD screening in respect of Customer 41 identified that:

a. Customer 41 exchanged cash chips with a third party and engaged in third-party structuring: see paragraph 1121.e; and

b. Customer 41's high gambling turnover was not commensurate with their occupation and source of wealth information: see paragraph 1121.h.

On 9 December 2021, the ECDD screening in respect of Customer 41 stated that SCA had determined to discontinue its business relationship with Customer 41, effective from 10 December 2021.

On 13 December 2021, the ECDD screening in respect of Customer 41 identified that:

a. Customer 41 did not have a plausible source of wealth to support their level of gambling activity;

b. Customer 41 refused to adequately explain their source of wealth and was unable to provide any documentation to support their claim of engaging in 'home duties' as an occupation; and

c. since the creation of Customer 41's account, Customer 41 was recorded to have lost $227,200 on table games and $1,146 on EGMs.

The ECDD conducted by SCA did not have appropriate regard to Customer 41's higher ML/TF risks: see *Customer 41's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 41's source of funds or source of wealth.

By reason of the matters set out in *Customer 41's risk profile* above, there were real risks that Customer 41's source of wealth and source of funds were not legitimate.

However, it was not until 9 December 2021 that SCA issued a ban in respect of Customer 41.

b. at no time prior to 9 December 2021 did senior management consider the higher ML/TF risks posted by Customer 41 in response to an ECDD trigger, or appropriately consider whether the ML/TF risks posed by Customer 41 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

On 9 December 2021, SCA determined to discontinue its business relationship with Customer 41.

On 9 December 2021, SCA issued a ban in respect of Customer 41.

Contravention of s 36 of the Act in respect of Customer 41

1130. By reason of the matters pleaded at paragraphs 1118 to 1129 above, on and from 30 July 2018, SCA:

a. did not monitor Customer 41 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1131. By reason of the matters pleaded at paragraph 1130, SCA contravened s 36(1) of the Act on and from 30 July 2018 to 9 December 2021 with respect to Customer 41.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 42

1132. Customer 42 was a customer of SCA during the relevant period. Between 7 December 2016 and 4 August 2021, SCA recorded turnover exceeding $4,100,000 for Customer 42.

Particulars

Customer 42 was a customer of SCA from at least 21 February 2016.

On 4 August 2021, SCA issued a ban in respect of Customer 42 at the direction of the SCA AML team.

1133. SCA provided Customer 42 with designated services within the meaning of table 3, s 6 of the Act during the relevant period.

Particulars

On 21 February 2016, SCA opened an FMA for Customer 42 which was closed on 8 October 2022 (item 11, table 3, s 6 of the Act).

See *Customer 42's risk profile* below.

1134. See *Customer 42's risk profile* below. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 42.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 42's risk profile

1135. On and from 7 December 2016, Customer 42, and the provision of designated services to Customer 42 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 42's risk profile prior to the relevant period

a. by 7 December 2016, Customer 42 had the following risk history:

i. SCA was aware that Customer 42 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

Between 1 June 2016 and 31 October 2016 SCA gave the AUSTRAC CEO 11 TTRs detailing incoming and outgoing payments by Customer 42 totalling $136,205, comprising:

a. three incoming TTRs totalling $36,300 in cash purchases of chips or tokens; and

b. eight outgoing TTRs totalling $99,905 in chip or token exchanges for cash.

ii. SCA was aware that designated services provided to Customer 42 included substantial EGM activity at SCA;

Particulars

See paragraphs 352 and 353 above.

Between 21 February 2016 and 28 November 2016, Customer 42's recorded individual rated gambling activity at SCA for EGMs was estimated as turnover of $208,046 and losses of $18,970.

Customer 42's risk profile during the relevant period

b. Customer 42 received high value gambling services (table 3, s 6 of the Act) at SCA other than through junket programs. Between 7 December 2016 and 2 August 2021, SCA recorded an estimated buy-in of $1,591,180, a turnover estimated at $4,154,311 for Customer 42, with cumulative losses of $178,145;

Particulars

In 2016, Customer 42's recorded individual rated gambling activity at SCA was estimated as a buy-in of $881,060 for table games, and for both table games and EGMs, turnover of $2,689,662 and losses of $86,016.

In 2017, Customer 42's recorded individual rated gambling activity at SCA was estimated as a buy-in of $842,400 for table games, and for both table games and EGMs, turnover of $2,024,784 and losses of $40,679.

In 2018, Customer 42's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $392,750, turnover of $1,017,063 and losses of $76,100.

Between January 2019 and July 2019, Customer 42's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $237,680, turnover of $888,401 and losses of $35,230.

Customer 42 did not game at SCA between August 2019 and June 2021 as they had applied to be excluded from SCA in late July 2019, and they were only permitted re-entry in July 2021.

In July 2021 and August 2021 (the only period in 2021 during which Customer 42 gambled at SCA), Customer 42's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $87,450, turnover of $153,063 and losses of $21,550.

c. SCA was aware that Customer 42 had engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

Particulars

Customer 42 was included in an internal report titled 'AML Unusual Changes in Betting – January' where SCA recorded Customer 42's turnover for January 2018.

On 30 July 2018, Customer 42 and three other SCA customers attempted to cash out $11,000 worth of chips between them. Three of the customers refused to show identification when requested, and surveillance showed that they passed the chips between them.

In August 2018, two other SCA customers passed Customer 42 $8,000 worth of chips under a table. Customer 42 then attempted to cash in the chips. When SCA did not allow the transaction Customer 42 passed the chips to another SCA customer.

In September 2018, SCA recorded that Customer 42 and two associates had engaged in possible structuring, and may have swapped chips between themselves.

d. Customer 42 was connected to other customers at SCA, including players who posed higher ML/TF risks such as Customer 41 and players who SCA considered had acted suspiciously;

Particulars

See *Customer 41's risk profile* above.

From at least 31 July 2018, SCA was aware that Customer 42 was an associate of Customer 41 and that the two individuals had attempted to cash out chips on behalf of a third individual who refused to provide identification.

On 27 August 2018, SCA formed the suspicion that Customer 42 and Customer 41 were part of a prostitution syndicate and were potentially attempting to launder funds at SCA.

e. Customer 42 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 23 January 2017 and 19 July 2021, SCA gave the AUSTRAC CEO 11 TTRs detailing incoming and outgoing payments made by Customer 42 totalling $138,865, which comprised:

a. 10 outgoing TTRs totalling $128,865 in cash purchases of chips or tokens; and

b. one incoming TTR totalling $10,000 in chip or token exchanges for cash.

f. Customer 42 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including structuring;

Particulars

See paragraph 24 above.

On 27 August 2018, Customer 42 was observed exchanging chips with two associates, before all three customers attempted to cash out chips just under the $10,000 threshold. SCA refused to complete the requested transactions as staff suspected that all the chips belonged to one of the associates.

See paragraph 1135.c above.

g. in August 2018, a law enforcement agency shared information pertaining to Customer 42 with SCA;

Particulars

On 23 August 2018, SCA received information from a law enforcement agency that a prostitution syndicate would potentially be visiting SCA to launder their funds. Shortly after this on 27 August 2018, SCA formed the suspicion that Customer 42 and their associates were involved in the same prostitution syndicate.

h. by 27 August 2018, SCA suspected that Customer 42 and their associates were involved in an illegal escort and prostitution syndicate;

Particulars

On 27 August 2018, SCA performed open source checks in relation to Customer 42 after Customer 42 was observed engaging in suspicious behaviour. The open source checks revealed that the phone number provided to SCA by Customer 42 was linked to numerous escort websites. Based on this, SCA formed the suspicion that Customer 42, Customer 41 and their associates were involved in an illegal escort and prostitution syndicate.

i. Customer 42 had access to a private gaming room at SCA; and

Particulars

See paragraph 145(e) above.

Customer 42 had access to the Grange Room, a private gaming room at SCA.

j. SCA did not have adequate reason to believe that Customer 42's source of wealth or source of funds was sufficient to explain the high value gambling services (table 3, s 6 of the Act) provided to Customer 42 by SCA.

Particulars

See paragraph 516 above.

Between at least June 2016 and August 2021 SCA recorded Customer 42's occupation as a beautician. In that time, Customer 42's buy-in on table games at SCA was $2,423,440 and their turnover on table games and EGMs was $6,592,339.

On 25 April 2017, a member of SCA staff recorded an entry in Customer 42's Player Notes on SCA's system that SCA needed to obtain a better description of Customer 42's occupation.

In 2018, SCA became aware that Customer 42 was involved with an illegal escort and prostitution syndicate which was suspected of laundering funds at SCA. From 2018 until Customer 42 was banned from SCA in August 2021, Customer 42's buy-in on table games at SCA was $717,880 and their turnover was $4,058,527.

Despite the above, at no time did request source of wealth or source of funds information from Customer 42.

At no time was SCA's understanding of Customer 42's source of wealth or source of funds commensurate with the high value gambling services that they received at SCA.

SCA's determination of the ML/TF risks posed by Customer 42

1136. SCA was unable to identify or assess the ML/TF risks posed by Customer 42 appropriately because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 42.

a. At all relevant times, Customer 42 should have been recognised by SCA as a high risk customer for the purpose of the Act and Rules for the reasons pleaded above: see *Customer 42's risk profile*.

Particulars

Sections 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

b. It was not until 28 August 2018 that Customer 42 was rated high risk for the purpose of the Act and Rules by SCA.

Monitoring of Customer 42's transactions

1137. At no time did SCA apply appropriate transaction monitoring to Customer 42's transactions because SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

The review, update and verification of Customer 42's KYC information

1138. SCA did not review, update or verify Customer 42's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 42, including the nature, extent and purpose of Customer 42's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 42's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 42's risk profile* above, there were real risks that Customer 42's source of wealth and source of funds were not legitimate.

d. to the extent that SCA reviewed Customer 42's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 42.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

In March 2017, Customer 42 was included in a spreadsheet created by SCA titled 'AntiMoney Laundering – February', which recorded KYC information as well as buy-in and bet information Customer 42's their play on table games in November 2016 and December 2016 and January 2017 and February 2017.

In February 2018, Customer 42 was included in an internal report titled 'AML Unusual Changes in Betting – January' where SCA recorded Customer 42's turnover for January 2018.

Failure to apply appropriate due diligence suited to the high ML/TF risks

1139. Had SCA conducted ongoing customer due diligence on and from 7 December 2016 by:

a. appropriately identifying and assessing the ML/TF risks posed by Customer 42;

b. applying appropriate risk-based transaction monitoring to Customer 42; and

c. appropriately reviewing and updating Customer 42's KYC information, having regard to the high ML/TF risks;

SCA would have been required by the Act and Rules to apply the ECDD Program to Customer 42 at a time before the date of the ECDD triggers pleaded below: see *ECDD triggers in respect of Customer 42*.

ECDD triggers in respect of Customer 42

1140. SCA was required to apply the ECDD program to Customer 42 following any ECDD triggers in respect of Customer 42.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

1141. Customer 42 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

On 27 August 2018, SCA gave the AUSTRAC CEO an SMR with respect to Customer 42.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 42* above.

1142. Each matter pleaded at paragraph 1141 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

1143. SCA did not conduct appropriate risk-based ECDD with respect to Customer 42 following an ECDD trigger because:

a. on each occasion prior to 4 August 2021 that SCA conducted ECDD in respect of Customer 42 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 42 and failed to appropriately consider whether the ML/TF risks posed by Customer 42 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

In August 2018, SCA conducted ECDD in respect of Customer 42.

On 9 August 2018, an SCA AML Analyst requested an historical review of an incident that occurred on 8 August 2018 with which Customer 42 was involved. The review concluded that Customer 42 and two associates cashed out amounts below the transaction reporting threshold, and chips may have been swapped between the players.

On 27 August 2018, an SCA AML Analyst requested an historical review of an incident with which Customer 42 was involved earlier that day.

On 27 August 2018, the ECDD screening in respect of Customer 42 identified that Customer 42 attempted to cash in chips that belonged to an associate.

Also on 27 August 2018, SCA conducted ECDD in respect of Customer 42. This ECDD consisted of open source checks to confirm Customer 42's source of funds. The checks identified that Customer 42's phone number was linked to the illegal escort and prostitution syndicate of which SCA had been informed by a law enforcement agency (see paragraph 1135.h above).

The ECDD conducted by SCA did not have appropriate regard to Customer 42's higher ML/TF risks: see *Customer 42's risk profile.*

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 42's source of funds or source of wealth.

By reason of the matters set out in *Customer 42's risk profile* above, there were real risks that Customer 42's source of wealth and source of funds were not legitimate.

It was not until 4 August 2021 that SCA issued a ban in respect of Customer 42.

b. at no time did prior to 4 August 2021 did senior management consider the higher ML/TF risks posed by Customer 42 in response to an ECDD trigger, or appropriately consider whether the ML/TF risks posed by Customer 42 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

It was not until 4 August 2021 that SCA issued a ban in respect of Customer 42.

Contravention of s 36 of the Act in respect of Customer 42

1144. By reason of the matters pleaded at paragraphs 1132 to 1143 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 42 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1145. By reason of the matters pleaded at paragraph 1144, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 4 August 2021 with respect to Customer 42.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 43

1146. Customer 43 was a customer of SCA during the relevant period. Between February 2017 and June 2022, SCA recorded turnover exceeding $31,000,000 for Customer 43.

Particulars

Customer 43 was a customer of SCA from at least 5 July 2015.

As at 28 October 2022, Customer 43 remained a customer of SCA and had not been banned.

1147. SCA provided Customer 43 with designated services within the meaning of tables 1 and 3, s 6 of the Act during the relevant period.

Particulars

Prior to 7 December 2016, SCA opened an FMA for Customer 43 which remained open as at November 2022 (item 11, table 3, s 6 of the Act).

While a customer of SCA, Customer 43 remitted funds to their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 43's risk profile* below.

1148. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 43.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 43's risk profile

1149. On and from 7 December 2016, Customer 43, and the provision of designated services to Customer 43 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 43's risk profile prior to the relevant period

a. by 7 December 2016, Customer 43 had the following risk history:

i. SCA had formed suspicions for the purposes of s 41 of the Act with respect to Customer 43;

Particulars

SCA gave the AUSTRAC CEO an SMR on two occasions, on 4 June 2001 and 23 February 2014.

Both SMRs reported that Customer 43 refused to provide identity documents to SCA staff upon request.

The SMR dated 23 February 2014 reported that Customer 43 attempted to cash out $10,000 worth of chips without providing identify documents. The transaction request was denied but Customer 43 returned five minutes later and attempted to cash out $9,500 worth of chips. Customer 43 again refused to provide identify documents and the transaction request was denied.

ii. SCA was aware that Customer 43 transacted using large amounts of cash at SCA; and

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 9 April 2014 and 18 July 2016, SCA gave the AUSTRAC CEO 24 TTRs detailing outgoing payments made by Customer 43 totalling $410,025 in chip and cash exchanges.

iii. Customer 43 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs;

Particulars

Between 5 February 2014 and 2 December 2016, Customer 43's recorded individual rated gambling activity for table games at SCA was estimated as a buy-in of $1,060,450, turnover of $2,959,608 and losses of $18,250.

Customer 43's risk profile during the relevant period

b. Customer 43 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs. Between February 2017 and June

2022, SCA recorded an estimated buy-in of $5,385,985, a high turnover estimated at $31,861,674 for Customer 43, with cumulative wins of $536,635;

Particulars

In 2017, Customer 43's recorded individual rated gambling activity at SCA for table games escalated to an estimated buy-in of $476,440, turnover of $2,103,852 and wins of $46,130.

In 2018, Customer 43's recorded individual rated gambling activity at SCA for table games escalated to an estimated buy-in of $950,505, turnover of $4,634,560 and wins of $450,205.

In 2019, Customer 43's recorded individual rated gambling activity at SCA escalated to an estimated as a buy-in of $1,594,610 for table games, and for both table games and EGMs, turnover of $7,437,185 and wins of $239,403.

In 2020, despite closures related to the COVID-19 pandemic, Customer 43's recorded individual rated gambling activity at SCA was estimated as a buy-in of $1,690,460 for table games, and for both table games and EGMs, turnover of $5,274,768 and losses of $101,800.

From 1 January 2021 to 30 June 2021, Customer 43's recorded individual rated gambling activity at SCA was estimated as a buy-in of $673,970 for table games, and for both table games and EGMs, turnover of $2,171,025 and losses of $128,183.

Between 1 July 2021 and 30 June 2022, Customer 43's recorded individual rated gambling activity at SCA was estimated as a turnover of $10,240,284.

c. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 43 by remitting large amounts of money into the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

Between February 2022 and July 2022, SCA received 110 telegraphic transfers totalling $552,010 from Customer 43's personal bank account in Australia, each of which was made available to Customer 43's FMA.

d. designated services provided to Customer 43 included EGM activity at SCA;

Particulars

See paragraphs 352 and 353 above.

In 2019, Customer 43 had a turnover of $14,110 on EGMs and losses of $1,307.

In 2020, despite closures related to the COVID-19 pandemic, Customer 43 had a turnover of $14,494 on EGMs and losses of $1,510.

In 2021, Customer 43 had a turnover of $6,722 on EGMs and losses of $2,003.

e. Customer 43 transacted using large amounts of cash and cash that appeared suspicious, including large volumes of cash in $100 notes bundled together with rubber bands, at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 6 March 2017 and 9 November 2022, SCA gave the AUSTRAC CEO 247 TTRs detailing transactions by Customer 43 totalling $4,703,041, which comprised:

a. 245 TTRs totalling $4,683,041 in chip and cash exchanges; and

b. two TTRs totalling $20,000 in account withdrawals.

Large and suspicious cash transactions in 2019

On 20 March 2019, Customer 43 presented at the Cage and counted cash in front of an SCA staff member. A surveillance review showed Customer 43 using bundles of cash held together with rubber bands in bundles of $100 notes.

f. in 2017, Customer 43 was the subject of law enforcement enquiries at SCA;

Particulars

On 31 August 2017 and 21 December 2017, SCA received requests from a law enforcement agency for information regarding Customer 43 in relation to an ongoing money laundering investigation in which Customer 43 was a person of interest.

g. in 2022, SCA received information from a law enforcement agency in respect of Customer 43;

Particulars

On 5 May 2022, a law enforcement agency informed SCA that it regarded Customer 43 as an established figure in organised crime, with a long history of association with drug trafficking and drug importation.

h. Customer 43 had access to private gaming rooms at SCA;

Particulars

See paragraph 145(e) above.

Customer 43 had access to private gaming rooms at SCA, including the Black Room, the Platinum Room and the Grange Room.

i. by 22 February 2021, SCA was aware of media articles reporting on Customer 43's criminal history; and

Particulars

On 22 February 2021, an open source Jade search performed by SCA staff identified media articles which reported that:

a. Customer 43 had convictions for drug offences dating back to 1983;

b. on 13 February 2001, Customer 43 and four associates were granted bail in an Australian court on charges relating to the sale and import of cannabis from Adelaide to Melbourne; and

c. in 2004, Customer 43 was sentenced to a period of imprisonment with a non-parole period of six years, after pleading guilty to involvement in the sale and shipping of cannabis.

j. SCA did not have adequate reason to believe that Customer 43's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 43 by SCA.

Particulars

See paragraph 516 above.

From 7 December 2016, SCA understood Customer 43 owned three businesses which they operated with their spouse.

Between 7 December 2016 and 23 September 2021, SCA took no steps to verify Customer 43's source of wealth or source of funds in circumstances where:

a. Customer 43's gambling activity escalated from 2016, and remaining high in 2020 and 2021, despite COVID-19 closures and restrictions;

b. SCA reported over 240 threshold transactions conducted by Customer 43 between 7 December 2016 and 19 August 2022, the total value of which exceeded $4,600,000;

c. SCA received a request from a law enforcement agency on 31 August 2017 in relation to a money laundering investigation involving Customer 43; and

d. SCA identified that Customer 43 had previous convictions for drug offences.

It was not until 23 September 2021, that Customer 43 submitted a Source of Wealth Declaration which declared an annual income of approximately $1,095,000 comprised of:

a. salary of $300,000 per annum as director of one of the businesses they owned and operated;

b. dividends of $295,000 per annum from shares in the same company; and

c. investment income of $500,000 per annum from undisclosed sources.

The only evidence Customer 43 provided in support of this declaration was a letter on letterhead of a company they owned, signed by Customer 43 themselves in their capacity as director.

In or about May 2022, SCA identified concerns that Customer 43's businesses involved the use of illicit funds, and SCA's AML team recommended that SCA obtain evidence to verify the information provided in Customer 43's Source of Wealth Declaration.

SCA's determination of the ML/TF risks posed by Customer 43

1150. On and from 17 April 2016, Customer 43 was appropriately rated by SCA as a high risk customer for the purpose of the Act and Rules.

Particulars

On 17 April 2016, Customer 43 was rated high risk.

On 1 June 2022, Customer 43's risk rating was elevated to significant risk, which was high risk for the purpose of the Act and Rules.

1151. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 43 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by it with respect to Customer 43.

Monitoring of Customer 43's transactions

1152. At no time did SCA apply appropriate transaction monitoring to Customer 43's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities; and

Particulars

Sections 36(1)(a) and (b) of the Act and rules 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 43 through the SCA Customer account channel, which was a high risk remittance channel.

Particulars

Section 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

1153. At no time did SCA apply appropriate transaction monitoring to Customer 43's transactions because SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

The review, update and verification of Customer 43's KYC information

1154. SCA did not review, update or verify Customer 43's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 43, including the nature, extent and purpose of Customer 43's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 43's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 43's risk profile* above, there were higher ML/TF risks associated with Customer 43's source of wealth or source of funds.

From 2017, Customer 43's turnover was high. This turnover was not proportionate to their source of wealth, suggesting that there were real ML/TF risks as to Customer 43's source of funds. SCA did not take steps to verify Customer 43's source of wealth or source of funds until 2021: see paragraph 1149.j above.

d. to the extent that SCA reviewed Customer 43's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 43.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

ECDD triggers in respect of Customer 43

1155. SCA was required to apply the ECDD program to Customer 43 following any ECDD triggers in respect of Customer 43.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1) and 15.10 of the Rules.

1156. Customer 43 was determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 43* above.

1157. The matter pleaded at paragraph 1156 was an ECDD trigger.

Particulars

See paragraphs 496 and 504 above.

1158. SCA did not conduct appropriate risk-based ECDD with respect to Customer 43 following an ECDD trigger because:

a. on each occasion that SCA conducted ECDD in respect of Customer 43 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 43 and failed to appropriately consider whether the ML/TF risks posed by Customer 43 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

Automatic alerts

Customer 43's transactions at SCA triggered 45 alerts between 6 March 2017 and 9 September 2021. SCA staff reviewed 34 of these alerts and determined that no further action was required. Ten of the alerts were not reviewed. For one alert dated 1 February 2021, SCA staff included Customer 43 in a report titled 'Five or More TTR Spreadsheet', which was provided to SCA's Table Games Senior Management for feedback.

Anti-money laundering report

Customer 43 was included in an internal report titled 'ADL AML Working Group – High Risk List 210824' where SCA recorded Customer 43's name, customer details and status as 'monitoring'.

2021

On 22 February 2021, SCA's customer screening system Jade identified that Customer 43 had a drug-related criminal history, including a 2004 conviction for involvement in the sale and shipping of cannabis in respect of which Customer 43 was sentenced to imprisonment with a non-parole period of six years.

On 21 July 2021, SCA conducted ECDD in respect of this screening. The ECDD report recommended that Customer 43 continue to be monitored within the business.

2022

On 1 June 2022, SCA's Financial Crime team prepared a significant risk escalation form and escalated Customer 43's risk rating to significant risk in response to information received from a law enforcement agency that it regarded Customer 43 as an established figure in organised crime (see paragraph 1149.g). The significant risk escalation form concluded that:

a. SCA was unable to verify Customer 43's declared financial position;

b. there was a risk that Customer 43's businesses had initially been funded with the proceeds of crime; and

c. any historical illicit wealth derived by Customer 43 has almost certainly been well integrated into their current financial holdings.

The General Manager of SCA's Financial Crimes team recommended that SCA independently verify the source of wealth information provided by Customer 43.

On 25 July 2022, SCA's Financial Crime team completed a second significant risk customer escalation form in respect of Customer 43. SCA's Financial Crime team undertook company and property checks in an attempt to independently verify information Customer 43 had provided in their Source of Wealth Declaration on 23 September 2021. The Financial Crime team stated that:

a. it had been unable to independently confirm the income generated from Customer 43's businesses;

b. however, Customer 43 had significant property holdings consistent with estimated annual rental returns of approximately $400,000;

c. it was possible that Customer 43 was using their wins of approximately $450,000 from 2018 and $240,000 from 2019 to fund their gambling activity in part;

d. it was almost certain that Customer 43 had historical access to illicit funds from their criminal offending prior to 2004; and

e. any illegal funds would be well integrated into their current financial holdings.

The Financial Crimes team did not consider whether Customer 43's income from property investments or historical wins was commensurate with their gambling activity, which had escalated to a turnover of $10,240,284 in the 2022 financial year.

The Financial Crimes team recommended that SCA senior management consider possible reputational risks of continuing a business relationship with Customer 43, particularly given that one of Customer 43's businesses supplied massage chairs to SCA. However, the report did not make any recommendations as to whether the ML/TF risks presented by Customer 43 could be adequately mitigated.

The ECDD conducted by SCA did not have appropriate regard to Customer 43's higher ML/TF risks: see *Customer 43's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 43's source of funds or source of wealth.

By reason of the matters set out in *Customer 43's risk profile* above, there were higher ML/TF risks associated with Customer 43's source of wealth or source of funds.

b. on any occasion that senior management considered the higher ML/TF risks posed by Customer 43 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 43 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

On 25 July 2022, after completing a second significant risk customer escalation form in respect of Customer 43, SCA's Financial Crime team emailed the SCA Chief Operating Officer to determine whether SCA should continue a business relationship with Customer 43.

On 8 August 2022, the SCA Chief Operating Officer determined that SCA should continue its business relationship with Customer 43. The SCA Chief Operating Officer observed that while Customer 43 was the subject of law enforcement investigations, they had not yet been charged with an offence and therefore there were no ML/TF requirements to exclude Customer 43. In their reasons for

determining that SCA should continue its business relationship with Customer 43, the SCA Chief Operating Officer recorded Customer 43's risk rating as high risk, despite the fact that Customer 43's risk rating was elevated to significant risk on 1 June 2022.

Contravention of s 36 of the Act in respect of Customer 43

1159. By reason of the matters pleaded at paragraphs 1146 to 1158 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 43 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1160. By reason of the matters pleaded at paragraph 1159, SCA contravened s 36(1) of the Act on and from 7 December 2016 with respect to Customer 43.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 44

1161. Customer 44 was a customer of SCA during the relevant period. Between 18 March 2017 and 13 January 2020, SCA recorded turnover exceeding $22,000,000 for Customer 44.

Particulars

Customer 44 was a customer of SCA from at least 18 March 2017.

On 29 March 2022, SCA issued a ban in respect of Customer 44.

1162. SCA provided Customer 44 with designated services within the meaning of table 1 and table 3, s 6 of the Act during the relevant period.

Particulars

On 18 March 2017, SCA opened an FMA for Customer 44 which was closed on 29 March 2022 (item 11, table 3, s 6 of the Act).

While a customer of SCA, Customer 44 remitted funds to and from their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 44's risk profile* below.

1163. At all times from 18 March 2017, SCA was required to conduct ongoing customer due diligence in respect of Customer 44.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 44's risk profile

1164. On and from 18 March 2017, Customer 44, and the provision of designated services to Customer 44 by SCA, posed higher ML/TF risks because of the following red flags:

a. Customer 44 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs. Between 2017 and 2020, SCA recorded an estimated buy-in of $3,597,600, a turnover estimated at $22,173,417 for Customer 44, with cumulative wins of $815,050;

Particulars

In 2017, Customer 44's recorded individual rated gambling activity at SCA was estimated as a buy-in of $3,357,800 for table games, and for both table games and EGMs turnover of $20,765,742 and wins of $844,050.

In 2018, Customer 44's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $158,800, turnover of $1,022,775 and wins of $38,200.

On 12 January 2020 and 13 January 2020, Customer 44's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $81,000, turnover of $384,900 and losses of $67,200. The last date that Customer 44 recorded gambling activity at SCA was 13 January 2020.

b. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 44 by remitting large amounts of money into, out of and within the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

SCA made money available to Customer 44 in the following transactions.

a. Between 13 November 2017 and 13 January 2020, SCA received 35 telegraphic transfers totalling $523,310, each of which was deposited into the SCA Cage account and made available to Customer 44's FMA.

SCA accepted instructions to transfer funds from Customer 44's accounts for the following transactions.

a. On 13 November 2017, Customer 44 transferred $20,000 from their SCA FMA to Customer 45's SCA FMA.

b. On 29 November 2017, Customer 44 was unable to transfer $20,000 to Customer 45's SCA FMA because Customer 44

was not onsite at the casino to sign a funds authorisation form: SMR dated 30 November 2017.

Remittances within the casino environment

On 13 January 2020, Customer 44 transferred $10,000 from their SCA FMA to their partner's SCA FMA.

c. SCA was aware that Customer 44 had engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

Particulars

On 23 September 2017, Customer 44 exchanged $8,000 in chips for cash and another customer exchanged $2,500 in chips for cash. The customer gave Customer 44 the $2,500 in cash. When an SCA staff member asked whether Customer 44's friend was cashing out for Customer 44, Customer 44 said they were just holding their friend's cash for them and became upset when they were asked again.

On 28 November 2017, SCA observed that Customer 44 shared funds with Customer 45: SMR dated 30 November 2017.

On 29 November 2017, after unsuccessfully attempting to transfer $20,000 to Customer 45, Customer 44 withdrew an unknown amount of cash from their FMA and commenced gaming. Later that day, Customer 44 handed $20,000 in chips to Customer 45: SMR dated 30 November 2017.

d. Customer 44 was connected to other customers at SCA, including players who posed higher ML/TF risks such as Customer 45 and players who SCA considered had acted suspiciously;

Particulars

See particulars to paragraphs 1164.b and 1164.c above.

Customer 44 and Customer 45 predominately played baccarat at SCA.

e. Customer 44 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 20 March 2017 and 15 January 2020, SCA gave the AUSTRAC CEO 69 TTRs detailing transactions made by Customer 44 totalling $1,993,435, which comprised:

a. 35 TTRs detailing cash and chip exchange transactions totalling $1,388,435;

b. 33 TTRs detailing account deposits totalling $585,000; and

c. one TTR detailing an account withdrawal of $20,000.

Large cash transactions in 2017

In 2017, SCA recorded that Customer 44 conducted significant cash transactions. For example:

a. on 12 September 2017, Customer 44 exchanged $100,015 in chips for cash;

b. on 30 September 2017, Customer 44 exchanged $85,000 in chips for cash;

c. on 15 October 2017, Customer 44 conducted two cash to chip exchange transactions totalling $20,000, each of which was for $10,000;

d. on 28 November 2017, Customer 44 exchanged $20,000 in chips for cash; and

e. on 29 November 2017, Customer 44 exchanged a $20,000 CPV for chips. A few hours later, Customer 44 exchanged $30,000 in chips for cash.

On 6 December 2017, Customer 44 deposited $30,000 in cash into the SCA Cage account.

f. Customer 44 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including quick turnover of money without betting;

Particulars

See paragraph 24 above.

For example, in 2017, Customer 44 conducted transactions indicative of the ML/TF typology of quick turnover of money without betting.

a. On 13 November 2017, Customer 44 deposited $200,000 in cash, and was provided a cheque for $150,000.

b. On 17 November 2017, a deposit of cash was made into Customer 44's FMA, and Customer 44 was then provided a cheque for $20,000.

g. in 2017, Customer 44 was the subject of a law enforcement enquiry on one occasion at SCA;

Particulars

On 29 November 2017, SCA received a request from a law enforcement agency regarding Customer 44 and Customer 45 in connection with an investigation into drug offences.

h. Customer 44 had access to a private gaming room at SCA;

Particulars

See paragraph 145(e) above.

Customer 44 had access to the Grange Room, which was a private gaming room at SCA.

i. by November 2017, SCA was aware that Customer 44's associate, Customer 45, was suspected of dealing with proceeds of crime;

Particulars

On 30 November 2017, SCA reported that it received information that Customer 45 was suspected of dealing with proceeds of crime worth over $1,000,000. SCA also reported that Customer 44 appeared to be sharing funds with Customer 45: SMR dated 30 November 2017.

j. by January 2018, SCA was aware that Customer 44's personal bank account had been closed; and

Particulars

On 17 January 2018, Customer 44 informed a VIP Host that Customer 44's personal bank account had been closed by their bank and their funds had been returned to them by bank cheque.

k. SCA did not have adequate reason to believe that Customer 44's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 44 by SCA.

Particulars

See paragraph 516 above.

On 20 March 2017, SCA recorded Customer 44's occupation as 'Working Holiday – Grape Picking'. On 5 September 2017, SCA updated Customer 44's occupation to 'Chef'.

On 30 November 2017, SCA reported that there was a discrepancy between Customer 44's play and their stated occupation as a chef: SMR dated 30 November 2017.

On 15 January 2020, SCA reported that Customer 44 had returned to SCA with their partner after an extended absence and was conducting cash transactions that did not align with their known source of wealth. SCA reported that Customer 44 was a chef and their partner was a student: SMR dated 15 January 2020.

At no time did SCA request source of wealth or source of funds information from Customer 44.

At no time was SCA's understanding of Customer 44's source of wealth or source of funds commensurate with the high value financial and gambling services that they received at SCA.

Between 18 March 2017 and 13 January 2020, SCA recorded an estimated buy-in of $3,597,600 for Customer 44.

SCA's determination of the ML/TF risks posed by Customer 44

1165. On and from 30 November 2017, Customer 44 was appropriately rated by SCA as a high risk customer for the purpose of the Act and Rules.

Particulars

On 30 November 2017, Customer 44 was rated high risk for the purpose of the Act and Rules.

On 25 March 2022, Customer 44 was rated significant risk, which was high risk for the purpose of the Act and Rules.

1166. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 44 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by it with respect to Customer 44.

Monitoring of Customer 44's transactions

1167. At no time did SCA apply appropriate transaction monitoring to Customer 44's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 44 through the SCA Customer account channel, which was a high risk remittance channel.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 44's KYC information

1168. SCA did not review, update or verify Customer 44's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 44, including the nature, extent and purpose of Customer 44's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update or verify Customer 44's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 44's risk profile* above, there were real risks that Customer 44's source of wealth and source of funds were not legitimate.

d. to the extent that SCA reviewed Customer 44's KYC information on and from 18 March 2017, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 44.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

On 23 September 2017, SCA conducted due diligence in respect of Customer 44 but did not have appropriate regard to their higher ML/TF risks: see *Customer 44's risk profile* above.

ECDD triggers in respect of Customer 44

1169. SCA was required to apply the ECDD program to Customer 44 following any ECDD triggers in respect of Customer 44.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

1170. Customer 44 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 30 November 2017 and 15 January 2020, SCA gave the AUSTRAC CEO two SMRs regarding Customer 44.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 44* above.

1171. Each matter pleaded at paragraph 1170 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

1172. SCA did not conduct appropriate risk-based ECDD with respect to Customer 44 following an ECDD trigger because:

a. on each occasion prior to 29 March 2022 that SCA conducted ECDD in respect of Customer 44 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 44 and failed to appropriately consider whether the ML/TF risks posed by Customer 44 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

On 17 January 2018, after becoming aware that Customer 44's bank account had been closed, SCA conducted a compliance investigation and identified that:

a. Customer 44 was previously reported to AUSTRAC for their association with suspected money launderer, Customer 45;

b. since March 2017, Customer 44's gambling activity and wins steadily increased;

c. SCA did not know why Customer 44's bank had decided to terminate its relationship with Customer 44; and

d. other than Customer 44's association with Customer 45, SCA held no concerns regarding Customer 44's behaviour.

On 5 December 2019, SCA conducted ECDD screening in respect of Customer 44. The screening recorded that:

a. Customer 44 had been reported to the AUSTRAC CEO for sharing funds with Customer 45;

b. Customer 44's occupation was recorded as a chef; and

c. SCA had been unable to find any open source information with respect to Customer 44.

The ECDD conducted by SCA did not have appropriate regard to Customer 44's higher ML/TF risks: see *Customer 44's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 44's source of funds or source of wealth.

By reason of the matters set out in *Customer 44's risk profile* above, there were real risks that Customer 44's source of wealth and source of funds were not legitimate.

It was not until 29 March 2022 that SCA issued a ban in respect of Customer 44.

b. on any occasion prior to 29 March 2022 that senior management considered the higher ML/TF risks posed by Customer 44 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 44 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

Customer 44 was named in a 'Transaction Monitoring Overview' report relating to the period 1 November 2017 and 1 February 2018 which was provided to the AML/CTF Senior Management Group for discussion at its meeting. The report noted that Customer 44 had received nine cheques at SCA.

It was not until 25 March 2022 that SCA's AML team rated Customer 44 significant risk and escalated Customer 44 to the Chief Operating Officer to determine whether to continue the business relationship.

On 27 March 2022, the Chief Operating Officer determined that SCA should discontinue its business relationship with Customer 44.

On 29 March 2022, SCA issued a ban in respect of Customer 44.

Contravention of s 36 of the Act in respect of Customer 44

1173. By reason of the matters pleaded at paragraphs 1161 to 1172 above, on and from 18 March 2017, SCA:

a. did not monitor Customer 44 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1174. By reason of the matters pleaded at paragraph 1173, SCA contravened s 36(1) of the Act on and from 18 March 2017 to 29 March 2022 with respect to Customer 44.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 45

1175. Customer 45 was a customer of SCA during the relevant period. Between October 2017 and July 2018, SCA recorded turnover exceeding $18,000,000 for Customer 45.

Particulars

Customer 45 was a customer of SCA from at least 10 October 2017.

On 18 July 2019, SCA issued a ban in respect of Customer 45.

1176. SCA provided Customer 45 with designated services within the meaning of table 1 and table 3, s 6 of the Act during the relevant period.

Particulars

On 10 October 2017, SCA opened an FMA for Customer 45 which remained open as 28 October 2022 (item 11, table 3, s 6 of the Act).

While a customer of SCA, Customer 45 remitted funds to their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 45's risk profile* below.

1177. At all times from 10 October 2017, SCA was required to conduct ongoing customer due diligence in respect of Customer 45.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 45's risk profile

1178. On and from 10 October 2017, Customer 45, and the provision of designated services to Customer 45 by SCA, posed higher ML/TF risks because of the following red flags:

a. Customer 45 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs From October 2017, SCA recorded an estimated buy-in of $3,768,600, a turnover estimated at $18,570,380 for Customer 45, with cumulative losses of $596,376;

Particulars

In 2017, Customer 45's recorded individual rated gambling activity at SCA was estimated as a buy-in of $2,686,400 for table games, and for both table games and EGMs, turnover of $12,921,322 and losses of $245,470.

In 2018, Customer 45's recorded individual rated gambling activity at SCA was estimated a buy-in of $1,062,200 for table games, and for both table games and EGMs, turnover of $5,649,058 and losses of $350,906.

b. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 45 by remitting large amounts of money into the casino environment, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

Between 11 November 2017 and 23 July 2018, SCA received 12 telegraphic transfers totalling $200,479, each of which was made available to Customer 45's SCA FMA.

c. Customer 45 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

Between 13 October 2017 and 27 July 2018, SCA gave the AUSTRAC CEO 61 TTRs detailing incoming and outgoing payments made by Customer 45 totalling $1,072,374, which comprised:

a. 40 TTRs totalling $571,875 in chip and cash exchanges;

b. 20 TTRs totalling $490,499 in account deposits; and

c. one TTR totalling $10,000 for an account withdrawal.

d. Customer 45 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including structuring;

Particulars

See paragraph 24 above.

On 8 November 2017, SCA staff observed that Customer 45 made three simultaneous cash buy-ins on different tables totalling $16,500. The buy-ins were in the amounts of $8,500, $7,000 and $1,500.

On 12 June 2018, Customer 45 transferred $9,999 and $8,000 to SCA's bank account: SMR dated 13 July 2018.

These transactions were indicative of the ML/TF typology of structuring.

e. Customer 45 was the subject of law enforcement enquiries on two occasions at SCA;

Particulars

On 29 November 2017, SCA received a request for information from a law enforcement agency and provided a response. SCA was advised that Customer 45 was suspected of dealing with proceeds of crime over $1,000,000.

On 10 July 2018, SCA was again contacted by a law enforcement agency for information concerning Customer 45 and their associates, including Customer 44.

f. SCA was aware of additional law enforcement interest in Customer 45;

Particulars

On 7 November 2017, SCA became aware that Customer 45 had been intercepted at an airport by a law enforcement agency and had a large amount of cash confiscated.

g. SCA was aware that Customer 45 had engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

Particulars

For example, on 29 November 2017, Customer 44 attempted to transfer $20,000 for Customer 45 via telegraphic transfer but was unable to do so because Customer 44 was not present at the casino to sign a funds authorisation form for the transfer. When Customer 44 attended the casino later that day they withdrew the funds from their account and gave Customer 45 $20,000 in chips: SMR dated 30 November 2017.

h. Customer 45 was connected to other customers at SCA, including players who posed higher ML/TF risks and players who SCA considered had acted suspiciously such as Customer 44;

Particulars

For example, in November 2017, Customer 44 and Customer 45 were observed sharing bankroll, and Customer 44 attempted to transfer funds to Customer 45's FMA: SMR dated 30 November 2017.

Customer 44 and Customer 45 predominately played baccarat.

SCA understood that Customer 44 and Customer 45 had met at SCA in October 2017. By November 2017 SCA was aware that Customer 44 and Customer 45 were transferring large amounts of money between each other and they had been observed sharing bankroll, despite having only met a month previously.

i. Customer 45 had access to a private gaming room at SCA; and

Particulars

See paragraph 145(e) above.

Customer 45 had access to the Platinum Room, a private gaming room at SCA.

j. SCA did not have adequate reason to believe that Customer 45's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 45 by SCA.

Particulars

See paragraph 516 above.

SCA recorded Customer 45's occupation as a student and business owner.

On and from October 2017, Customer 45's buy-in was high, exceeding $3,700,000. Customer 45's buy-in was not proportionate to

their source of wealth. From November 2017, SCA was aware that Customer 45 was suspected of dealing with proceeds of crime, suggesting that there were real ML/TF risks as to Customer 45's source of funds.

Despite this, at no time did SCA request source of wealth or source of funds information from Customer 45.

At no time was SCA's understanding of Customer 45's. source of wealth or source of funds commensurate with the high value financial and gambling services that they received at SCA.

SCA's determination of the ML/TF risks posed by Customer 45

1179. On and from 30 November 2017, Customer 45 was appropriately rated by SCA as a high risk customer for the purpose of the Act and Rules.

1180. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 45 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by it with respect to Customer 45.

Monitoring of Customer 45's transactions

1181. At no time did SCA apply appropriate transaction monitoring to Customer 45's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities;

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not carry out adequate due diligence on source of funds in respect of third party deposits for the benefit of Customer 45 into its bank accounts; and

Particulars

See paragraph 227 above.

c. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 45 through the SCA Customer account channel, which was a high risk remittance channel.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 45's KYC information

1182. SCA did not review, update or verify Customer 45's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 45, including the nature, extent and purpose of Customer 45's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 45's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 45's risk profile* above, there were higher ML/TF risks associated with Customer 45's source of wealth or source of funds.

On and from October 2017, Customer 45's buy-in was high, exceeding $3,700,000. Customer 45's buy-in was not proportionate to their source of wealth. From November 2017, SCA was aware that Customer 45 was suspected of dealing with proceeds of crime, suggesting that there were real ML/TF risks as to Customer 45's source of funds.

d. to the extent that SCA reviewed Customer 45's KYC information on and from 10 October 2017, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 45.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

ECDD triggers in respect of Customer 45

1183. SCA was required to apply the ECDD program to Customer 45 following any ECDD triggers in respect of Customer 45.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

1184. Customer 45 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 30 November 2017 and 14 January 2020, SCA gave the AUSTRAC CEO three SMRs with respect to Customer 45.

b. determined by SCA to be high risk for the purpose of the Act and Rules on 30 November 2017.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 45* above.

1185. Each matter pleaded at paragraph 1184 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

1186. SCA did not conduct appropriate risk-based ECDD with respect to Customer 45 following an ECDD trigger because:

a. on each occasion prior to 18 July 2019 that SCA conducted ECDD in respect of Customer 45 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 45 and failed to appropriately consider whether the ML/TF risks posed by Customer 45 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

In November 2017, SCA conducted ECDD in respect of Customer 45.

The ECDD revealed Customer 45 engaged in unusual transactions, and appeared to be connected to Customer 44.

On 20 July 2018, SCA's Cage Manager noted that they required updated occupation details for Customer 45 and that business owner was not a sufficient description.

On 1 May 2019, an SCA AML Analyst noted that they were aware that Customer 45 was suspected of money laundering funds in connection with a drug syndicate.

On 9 May 2019, SCA determined that there would be no further early release of funds for Customer 45.

The ECDD conducted by SCA did not have appropriate regard to Customer 45's higher ML/TF risks: see *Customer 45's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 45's source of funds or source of wealth.

By reason of the matters set out in *Customer 45's risk profile* above, there were higher ML/TF risks associated with Customer 45's source of wealth or source of funds.

However, it was not until 18 July 2019 that SCA issued a ban in respect of Customer 45.

b. on any occasion prior to 18 July 2019 that senior management considered the higher ML/TF risks posed by Customer 45 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 45 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

Customer 45 was named in a 'Transaction Monitoring Overview' report relating to the period 14 August 2017 to 1 November 2017 which was considered by SCA's Senior Management Group.

On or around 12 July 2018, SCA noted that a law enforcement agency advised that Customer 45 was a person of interest for drug trafficking. The fact that there had been a law enforcement agency request regarding Customer 45 was noted in the minutes of the SCA AML/CTF Senior Management Group meeting on 9 August 2018.

On or around 24 July 2018, SCA produced two Audit Reports which outlined suspicious activity regarding Customer 45's play. These reports were escalated to senior management who decided that this activity in conjunction with other information SCA had regarding Customer 45 justified barring Customer 45 from SCA. On 24 July 2018, Customer 45 was banned for three months from SCA.

It was not until 18 July 2019 that SCA issued a ban in respect of Customer 45.

Contravention of s 36 of the Act in respect of Customer 45

1187. By reason of the matters pleaded at paragraphs 1175 to 1186 above, on and from 10 October 2017, SCA:

a. did not monitor Customer 45 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1188. By reason of the matters pleaded at paragraph 1187, SCA contravened s 36(1) of the Act on and from 10 October 2017 to 18 July 2019 with respect to Customer 45.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 46

1189. Customer 46 was a customer of SCA during the relevant period. Between 7 December 2016 and 10 May 2021, SCA recorded turnover exceeding $20,000,000 for Customer 46.

Particulars

Customer 46 was a customer of SCA from at least 29 September 2015.

On 29 March 2022, SCA issued a ban in respect of Customer 46 at the direction of the AML Team.

1190. SCA provided Customer 46 with designated services within the meaning of table 3, s 6 of the Act during the relevant period.

Particulars

On 19 June 2015, SCA opened an FMA for Customer 46 which was closed on 29 March 2022 (item 11, table 3, s 6 of the Act).

See *Customer 46's risk profile* below.

1191. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 46.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 46's risk profile

1192. On and from 7 December 2016, Customer 46, and the provision of designated services to Customer 46 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 46's risk profile prior to the relevant period

a. by 7 December 2016, Customer 46 had the following risk history:

   i. Customer 46 received high value gambling services (table 3, s 6 of the Act) at SCA; and

Particulars

In 2015, Customer 46's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $176,200, turnover of $624,540 and wins of $135,200.

   ii. Customer 46 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 29 July 2013 and 25 November 2016, SCA gave the AUSTRAC CEO 23 TTRs detailing chip and cash exchanges made by Customer 46 totalling $372,100, which comprised:

a. two incoming transactions involving the issuance of chips or tokens totalling $23,500; and

b. 21 outgoing transactions involving cashing out chips or tokens totalling $348,600.

Customer 46's risk profile during the relevant period

b. Customer 46 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs. Between 7 December 2016 and 10 May 2021, SCA recorded an estimated buy-in of $3,034,200, a turnover estimated at $20,319,140 for Customer 46, with cumulative wins of $79,650;

Particulars

In 2016, Customer 46's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $331,550, turnover of $2,503,836 and wins of $30,350.

In 2017, Customer 46's recorded individual rated gambling activity at SCA for table games escalated to an estimated buy-in of $845,950, turnover of $6,862,909 and wins of $80,150.

In 2018, Customer 46's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $280,000, turnover of $3,023,861 and wins of $19,700.

In 2019, Customer 46's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $409,200, turnover of $1,895,299 and wins of $144,700.

In 2020, despite closures related to the COVID-19 pandemic, Customer 46's recorded individual rated gambling activity at SCA escalated to an estimated buy-in of $1,309,000 for table games, and for both table games and EGMs, turnover of $7,425,532 and losses of $194,950.

In 2021, Customer 46's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $177,850, turnover of $968,390 and wins of $22,250.

c. SCA was aware that Customer 46:

i. had engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

ii. had engaged in transactions that were indicative of ML/TF typologies and vulnerabilities, including structuring and disguising gaming play through the use of a third party associate; and

iii. was connected to another SCA customer, Person 25, and disguised their gaming through the use of Person 25's loyalty card;

Particulars

See paragraph 24 above.

On 31 May 2017, Customer 46 split $10,300 in cash chips with Person 25. Customer 46 then cashed out $5,300 and Person 25 cashed out $5,000. Person 25 handed over an amount of cash to Customer 46.

On 13 October 2017, Person 25 recorded turnover exceeding $125,000 on rapid roulette. SCA recorded that Customer 46 had been playing on the machine with Person 25's loyalty card inserted in the terminal. This had the effect of disguising Customer 46's gambling activity: SMR dated 16 October 2017.

On 17 September 2018, Customer 46 played rapid roulette with Person 25's loyalty card inserted in the terminal. Customer 46 received $10,200 in cash chips from this play. Customer 46 gave $5,000 in chips to Person 25 and kept the remaining $5,200 in chips. Customer 46 cashed out their chips, and shortly after Person 25 cashed out their chips. Customer 46 and Person 25 then returned to the rapid roulette terminals, where Customer 46 instructed Person 25 on where to place their bets. SCA recorded that this activity: SMR dated 18 September 2018. These transactions were indicative of the ML/TF typology of structuring, and had the effect of disguising Customer 46's gambling activity.

In September 2018, Customer 46 instructed SCA to close their loyalty account. After Customer 46's loyalty account was closed, SCA was not able to track Customer 46's visitation to SCA. However, Customer 46 still attended SCA after their loyalty card was closed: SMRs dated 23 January 2019 and 30 April 2019.

On 19 January 2019, Customer 46 and Person 25 cashed out a total of $14,613 in three separate transactions which were each under the reporting threshold. Two of the transactions were performed by Person 25 using chips that had been handed to them by Customer 46. Person 25 then gave the cash to Customer 46. On the same day, Customer 46 also made a $1,000 buy-in on an EGM terminal which had Person 25's loyalty card inserted. SCA suspected that a spike in recorded play on Person 25's card in November 2018 was due to Customer 46 using Person 25's loyalty card, and that Customer 46's play while not using Person 25's card was minimal and uncarded: SMR dated 23 January 2019.

On 29 April 2019, Customer 46 attempted to exchange $9,000 worth of chips to cash despite holding $11,850 worth of chips in total. When the SCA Cashier queried this, Customer 46 initially refused to present identification. SCA staff suspected that Customer 46 had attempted to engage in structuring: SMR dated 30 April 2019.

d. designated services provided to Customer 46 included substantial EGM activity at SCA;

Particulars

See paragraphs 352 and 353 above.

Between 25 July 2020 and 21 October 2020, Customer 46's turnover for EGMs was estimated to be $443,625 and losses were estimated to be $45,050.

e. Customer 46 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 28 December 2016 and 11 May 2021, SCA gave the AUSTRAC CEO 86 TTRs detailing incoming and outgoing payments made by Customer 46 totalling $1,763,700, which comprised:

a. 82 TTRs totalling $1,697,085 in chip and cash exchanges; and

b. four TTRs totalling $66,615 in EGM payouts.

f. in 2018, Customer 46 was the subject of law enforcement enquiries on one occasion at SCA; and

Particulars

On 22 February 2018, SCA received a request from a law enforcement agency for information on Customer 46.

The request identified that Customer 46 was suspected of involvement in money laundering.

g. SCA did not have adequate reason to believe that Customer 46's source of wealth or source of funds was sufficient to explain the high value gambling services (table 3, s 6 of the Act) provided to Customer 46 by SCA.

Particulars

See paragraph 516 above.

At all times, SCA understood that Customer 46 was a plumber.

From February 2018, SCA was aware that Customer 46 was suspected of involvement in money laundering. SCA continued to

provide designated services to Customer 46 until at least 10 May 2021.

At no time did SCA request any source of funds or source of wealth information from Customer 46.

At no time was SCA's understanding of Customer 46's source of wealth or source of funds commensurate with the high value financial and gambling services that they received at SCA.

Between 2016 and 2021, SCA recorded an estimated buy-in exceeding $3,000,000 for Customer 46.

SCA's determination of the ML/TF risks posed by Customer 46

1193. SCA was unable to identify or assess the ML/TF risks posed by Customer 46 appropriately because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 46.

a. On and from 7 December 2016, Customer 46 should have been recognised by SCA as a high risk customer for the purpose of the Act and Rules for the reasons pleaded above: see *Customer 46's risk profile.*

Particulars

Sections 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

b. It was not until 16 October 2017 that Customer 46 was rated high risk for the purpose of the Act and Rules by SCA.

Particulars

On 25 March 2022, Customer 46's risk rating was elevated to significant risk, which was high risk for the purpose of the Act and Rules.

Monitoring of Customer 46's transactions

1194. At no time did SCA apply appropriate transaction monitoring to Customer 46's transactions because SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

The review, update and verification of Customer 46's KYC information

1195. SCA did not review, update or verify Customer 46's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b)Sections 36(1)(a) and (b)

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 46, including the nature, extent and purpose of Customer 46's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update or verify Customer 46's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 46's risk profile* above, there were real risks that Customer 46's source of wealth and source of funds were not legitimate.

d. to the extent that SCA reviewed Customer 46's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 46.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

On 31 May 2017, SCA conducted a review of Customer 46's transactions earlier that day: see paragraph 1192.c above. An SCA AML Analyst was advised of the findings.

Failure to apply appropriate due diligence suited to the high ML/TF risks

1196. Had SCA conducted ongoing customer due diligence on and from 7 December 2016 by:

a. appropriately identifying and assessing the ML/TF risks posed by Customer 46;

b. applying appropriate risk-based transaction monitoring to Customer 46; and

c. appropriately reviewing and updating Customer 46's KYC information, having regard to the high ML/TF risks;

SCA would have been required by the Act and Rules to apply the ECDD Program to Customer 46 at a time before the date of the ECDD triggers pleaded below: see *ECDD triggers in respect of Customer 46*.

ECDD triggers in respect of Customer 46

1197. SCA was required to apply the ECDD program to Customer 46 following any ECDD triggers in respect of Customer 46.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

1198. Customer 46 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 16 October 2017 and 30 April 2019, SCA gave the AUSTRAC CEO four SMRs with respect to Customer 46.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 46* above.

1199. Each matter pleaded at paragraph 1198 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

1200. SCA did not conduct appropriate risk-based ECDD with respect to Customer 46 following an ECDD trigger because:

a. on each occasion prior to 29 March 2022 that SCA conducted ECDD in respect of Customer 46 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 46 and failed to appropriately consider whether the ML/TF risks posed by Customer 46 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

On 3 October 2019, SCA conducted ECDD screening in respect of Customer 46. The screening recorded that:

a. Customer 46 had been the subject of several SMRs, which identified that they had engaged in structuring and disguised their gaming by using an associate's loyalty card; and

b. Customer 46 was a plumber, and they were registered as a sole trader.

The ECDD conducted by SCA did not have appropriate regard to Customer 46's higher ML/TF risks: see *Customer 46's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 46's source of funds or source of wealth.

By reason of the matters set out in *Customer 46's risk profile* above, there were real risks that Customer 46's source of wealth and source of funds were not legitimate.

However, it was not until 29 March 2022 that SCA issued a ban in respect of Customer 46.

b. at no time prior to March 2022 did senior management consider the higher ML/TF risks posed by Customer 46 in response to an ECDD trigger, or appropriately consider whether the ML/TF risks posed by Customer 46 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

On 25 March 2022, the SCA General Manager AML endorsed a Significant Risk Elevation Form for Customer 46. An SCA AML Compliance Analyst then emailed the SCA Chief Operating Officer to determine whether SCA should continue a business relationship with Customer 46.

On 27 March 2022, the SCA Chief Operating Officer determined that SCA should discontinue its business relationship with Customer 46.

On 29 March 2022, SCA issued a ban in respect of Customer 46.

Contravention of s 36 of the Act in respect of Customer 46

1201. By reason of the matters pleaded at paragraphs 1189 to 1200 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 46 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1202. By reason of the matters pleaded at paragraph 1201, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 29 March 2022 with respect to Customer 46.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 47

1203. Customer 47 was a customer of SCA during the relevant period. Between 23 December 2016 and 6 January 2022, SCA recorded turnover exceeding $17,000,000 for Customer 47.

Particulars

Customer 47 was a customer of SCA from at least 1 July 2015.

On 1 June 2022, SCA issued a ban in respect of Customer 47 at the direction of the SCA AML team.

1204. SCA provided Customer 47 with designated services within the meaning of table 3, s 6 of the Act during the relevant period.

Particulars

By 7 December 2016, SCA opened an FMA for Customer 47 which was closed on 31 May 2022 (item 11, table 3, s 6 of the Act).

See *Customer 47's risk profile* below.

1205. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 47.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 47's risk profile

1206. On and from 7 December 2016, Customer 47, and the provision of designated services to Customer 47 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 47's risk profile prior to the relevant period

a. by 7 December 2016, Customer 47 had the following risk history:

i. SCA was aware that Customer 47 received high value gambling services (table 3, s 6 of the Act) at SCA other than through junket programs; and

Particulars

In 2015, Customer 47's recorded individual rated gambling activity at SCA was estimated as a buy-in of $164,115 for table games, and for both table games and EGMs, turnover of $895,621 and losses of $49,993.

ii. Customer 47 transacted using large amounts of cash at SCA.

Particulars

See paragraphs 376 to 381 above.

TTRs

On 14 December 2015, SCA gave the AUSTRAC CEO a TTR detailing a chip and cash exchange made by Customer 47 totalling $10,955.

Customer 47's risk profile during the relevant period

b. Customer 47 received high value gambling services (table 3, s 6 of the Act) at SCA other than through junket programs. Between 2016 and 2022, SCA recorded an estimated buy-in of $2,186,535, high turnover estimated at $19,582,782 for Customer 47, with cumulative losses of $617,301;

Particulars

In 2016, Customer 47's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $374,603, turnover of $2,181,819 and losses of $59,320.

In 2017, Customer 47's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $668,285, turnover of $5,351,080 and losses of $148,515.

In 2018, Customer 47's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $622,525, turnover of $4,733,844 and losses of $205,475.

In 2019, Customer 47's recorded individual rated gambling activity at SCA was estimated as a buy-in of $281,150 for table games, and for both table games and EGMs, turnover of $3,304,893 and losses of $98,550.

In 2020, despite closures related to the COVID-19 pandemic, Customer 47's turnover remained high. Customer 47's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $180,205, turnover of $903,508 and losses of $77,122.

In 2021, Customer 47's recorded individual rated gambling activity at SCA escalated to an estimated buy-in of $427,720 for table games, and for both table games and EGMs turnover of $3,079,738 and losses of $85,879.

In the period 1 January 2022 to approximately 6 January 2022, Customer 47's recorded individual rated gambling activity at SCA was estimated as a buy-in of $3,050 for table games, and for both table games and EGMs, turnover of $27,900 and losses of $960.

c. SCA was aware that Customer 47 had engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

Particulars

On 1 April 2017, Customer 47 exchanged a total of $11,600 in chips to cash in two transactions. The transactions were conducted on

behalf of another SCA customer, Person 30. Customer 47 was seen handing two bundles of cash to Person 30 while waiting for their vehicle.

On 29 December 2018, Customer 47 exchanged $5,000 in chips to cash at the Cage. Shortly after, another SCA customer exchanged $5,000 in chips to cash and then gave Customer 47 the cash.

d. Customer 47 was connected to other customers at SCA, including players who posed higher ML/TF risks such as Customer 31 and players who SCA considered had acted suspiciously such as Person 30;

Particulars

For example, SCA recorded that Customer 31 was a known associate of Customer 47 in Customer 47's iTrak profile.

e. from 2021, designated services provided to Customer 47 included substantial EGM activity at SCA;

Particulars

See paragraphs 352 and 353 above.

In 2021, Customer 47's turnover for EGMs was $314,513 with losses of $23,229.

In 2022, Customer 47's turnover for EGMs was $16,389 with losses of $810.

f. Customer 47 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 17 July 2017 and 11 February 2022, SCA gave the AUSTRAC CEO eight TTRs detailing transactions made by Customer 47 totalling $165,220, which comprised:

a. seven TTRs totalling $155,220 in chip and cash exchanges; and

b. one TTR totalling $10,000 for an account withdrawal.

g. Customer 47 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including structuring and quick turnover of money without betting;

Particulars

See paragraph 24 above.

Customer 47 was involved in transactions indicative of the ML/TF typology of structuring. For example:

a. on 1 April 2017, Customer 47 received $11,600 in chips from Person 30. Customer 47 cashed out the chips in two separate transactions of $6,600 and $5,000 in quick succession. SCA asked Customer 47 for identification but they refused, stating that the transaction was under the reporting threshold and that the earlier cash withdrawal was for a friend. Customer 47 then handed two bundles of cash to Person 30 before departing the casino;

b. on 29 December 2018, Customer 47 conducted at least four chip and cash exchanges with SCA and other customers totalling at least $28,000 that raised red flags indicative of ML/TF typologies:

i. Customer 47 removed seven $1,000 chips from their handbag, exchanged them for cash at a cashier and placed the cash back in their handbag. Customer 47 had not received any $1,000 chips from table play that day;

ii. Customer 47 handed an unknown amount of cash to another SCA customer;

iii. Customer 47 mixed chips won from table play with an additional six $1,000 chips from their handbag and exchanged them for $10,000 in $5,000 chips at a cashier;

iv. Customer 47 exchanged one $5,000 chip for cash and placed the cash in their handbag;

v. Customer 47 handed the second $5,000 chip to a second SCA customer along with an unknown amount of cash;

vi. The second SCA customer exchanged the $5,000 chip for cash and handed the cash back to Customer 47.

SCA noted that these transactions presented indicators of structuring and Customer 47 appeared to use the second customer as a runner to cash out on their behalf; and

c. Customer 47 was involved in transactions indicative of the ML/TF typology of quick turnover of money without betting. For example, on 20 August 2017, Customer 47 deposited $10,000 in cash into their FMA and withdrew the funds in cash on the same day.

h. Customer 47 had access to a private gaming room at SCA; and

Particulars

See paragraph 145(e) above.

Customer 47 had access to the Grange Room.

i. SCA did not have adequate reason to believe that Customer 47's source of wealth or source of funds was sufficient to explain the high value gambling services (table 3, s 6 of the Act) provided to Customer 47 by SCA.

Particulars

See paragraph 516 above.

From at least April 2017, SCA recorded Customer 47's occupation and source of wealth as a wholesaler and farmer.

On 19 May 2019, SCA recorded that it needed to obtain details regarding Customer 47's occupation and update their customer profile due to their level of play.

It was not until 4 September 2021 that SCA recorded further details concerning Customer 47's occupation.

In 2021, SCA recorded that it had requested further information regarding Customer 47's source of wealth. It also noted that, whilst Customer 47's average loss between the 2019 and 2021 financial years was $82,722 annually, SCA was aware that the manual ratings it recorded were never accurate.

At no point was SCA's understanding of Customer 47's source of wealth or source of funds commensurate with the high value gambling services that they received at SCA.

Between 2016 and 2022, SCA recorded buy-in exceeding $2,100,000 for Customer 47.

SCA's determination of the ML/TF risks posed by Customer 47

1207. On and from 17 June 2017, Customer 47 was appropriately rated by SCA as a high risk customer for the purpose of the Act and Rules.

1208. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 47 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by it with respect to Customer 47.

Monitoring of Customer 47's transactions

1209. At no time did SCA apply appropriate transaction monitoring to Customer 47's transactions because SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

The review, update and verification of Customer 47's KYC information

1210. SCA did not review, update or verify Customer 47's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 47, including the nature, extent and purpose of Customer 47's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update and verify Customer 47's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 47's risk profile* above, there were higher ML/TF risks associated with Customer 47's source of wealth or source of funds.

On and from 2017, Customer 47 recorded high and escalating turnover at SCA. At no point was Customer 47's buy-in commensurate with SCA's understanding of their source of wealth and source of funds.

From April 2017, SCA was aware that Customer 47 was involved in structuring.

d. to the extent that SCA reviewed Customer 47's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 47.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

ECDD triggers in respect of Customer 47

1211. SCA was required to apply the ECDD program to Customer 47 following any ECDD triggers in respect of Customer 47.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

1212. Customer 47 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 7 April 2017 and 28 September 2017, SCA gave the AUSTRAC CEO two SMRs with respect to Customer 47.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 47* above.

1213. Each matter pleaded at paragraph 1212 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

1214. SCA did not conduct appropriate risk-based ECDD with respect to Customer 47 following an ECDD trigger because:

a. on each occasion prior to 1 June 2022 that SCA conducted ECDD in respect of Customer 47 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 47 and failed to appropriately consider whether the ML/TF risks posed by Customer 47 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

At various times between December 2018 and January 2022 SCA conducted ECDD in respect of Customer 47.

Transaction and activity reviews

In December 2018, SCA identified that Customer 47 appeared to be engaging in transactions indicative of the typologies of refining and structuring, and was also using other SCA customers as runners to conduct transactions on their behalf.

On 8 January 2019, SCA reviewed Customer 47's transactions and concluded they were indicative of refining and structuring.

ECDD screening

On 5 March 2020, SCA conducted ECDD screening in respect of Customer 47. The ECDD screening identified that:

a. Customer 47's occupation, source of wealth and source of funds was their employment as a wholesaler and farmer;

b. Customer 47's known associates included other SCA customers about whom SCA had formed suspicions, including Person 30; and

c. Customer 47 was a Grange VIP player in respect of whom SCA had previously given SMRs to the AUSTRAC CEO for structuring.

Source of wealth reviews

SCA requested that Customer 47 provide information about their occupation and source of wealth on various occasions between September 2021 and January 2022.

On 21 January 2022, SCA reviewed information provided by Customer 47 in relation to their source of wealth and source of funds, and requested that they provide further information.

The ECDD conducted by SCA did not have appropriate regard to Customer 47's higher ML/TF risks: see *Customer 47's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 47's source of funds or source of wealth.

By reason of the matters set out in *Customer 47's risk profile* above, there were higher ML/TF risks associated with Customer 47's source of wealth or source of funds.

It was not until 1 June 2022 that SCA issued a ban in respect of Customer 47.

b. on any occasion prior to 1 June 2022 that senior management considered the higher ML/TF risks posed by Customer 47 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 47 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

On 12 January 2022, an AML Compliance Analyst escalated Customer 47 to the Senior Gaming Operations Shift Manager and noted that they could be a customer of interest.

It was not until 1 June 2022 that SCA issued a ban in respect of Customer 47.

Contravention of s 36 of the Act in respect of Customer 47

1215. By reason of the matters pleaded at paragraphs 1203 to 1214 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 47 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1216. By reason of the matters pleaded at paragraph 1215, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 1 June 2022 with respect to Customer 47.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 48

1217. Customer 48 was a customer of SCA during the relevant period. Between 2017 and 2021, SCA recorded a turnover exceeding $11,000,000 for Customer 48.

Particulars

Customer 48 was a customer of SCA from at least 3 July 2015.

On 9 August 2021, SCA issued a ban in respect of Customer 48 at the direction of the SCA AML team.

1218. SCA provided Customer 48 with designated services within the meaning of table 3, s 6 of the Act during the relevant period.

Particulars

Prior to 7 December 2016, SCA opened an FMA for Customer 48 which remained open as at 28 October 2022 (item 11, table 3, s 6 of the Act).

See *Customer 48's risk profile* below.

1219. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 48.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 48's risk profile

1220. On and from 7 December 2016, Customer 48, and the provision of designated services to Customer 48 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 48's risk profile prior to the relevant period

a. by 7 December 2016, Customer 48 had the following risk history:

i. Customer 48 transacted using large amounts of cash at SCA; and

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 17 May 2009 and 29 June 2016, SCA gave the AUSTRAC CEO 94 TTRs detailing chip and cash exchanges made by Customer 48 totalling $3,541,195.

ii. in 2015, Customer 48 received high value gambling services (tables 3, s 6 of the Act) at SCA other than through junket programs;

Particulars

In 2015, Customer 48's recorded individual rated gambling activity at SCA was estimated as a buy-in of $8,000 for table games, and for both table games and EGMs, turnover of $6,713 and losses of $3,500.

Customer 48's risk profile during the relevant period

b. Customer 48 received high value gambling services (table 3, s 6 of the Act) at SCA other than through junket programs. Between 2016 and 2021, SCA recorded an estimated buy-in of $4,120,450, turnover estimated at $11,395,094 for Customer 48, with cumulative losses of $339,725;

Particulars

In 2016, Customer 48's recorded individual rated gambling activity at SCA for both table games and EGMs was a buy-in of $89,900, turnover of $143,960 and wins of $650.

In 2017, Customer 48's recorded individual rated gambling activity at SCA for table games was a buy-in of $712,400, turnover of $2,069,614 and losses of $124,000.

In 2018, Customer 48's recorded individual rated gambling activity at SCA for table games escalated to a buy-in of $2,141,250, turnover of $5,800,760 and losses of $87,025.

In 2019, Customer 48's recorded individual rated gambling activity at SCA for table games was a buy-in of $223,700, turnover of $382,317 and losses of $11,600.

In 2020, despite closures related to the COVID-19 pandemic, Customer 48's recorded individual rated gambling activity at SCA for table games escalated to a buy-in of $437,300, turnover of $1,013,514 and losses of $69,000.

In 2021, Customer 48's recorded individual rated gambling activity at SCA for table games was a buy-in of $564,400, turnover of $2,073,213 and losses of $47,300.

c. SCA was aware that Customer 48 had engaged in:

   i. large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

   ii. transactions using large amounts of cash; and

   iii. transactions indicative of ML/TF typologies and vulnerabilities, including structuring; and

Particulars

See paragraphs 24, and 376 to 381 above.

TTRs

Between 28 March 2017 and 23 April 2019, SCA gave the AUSTRAC CEO 129 TTRs detailing transactions made by Customer 48 totalling $2,711,590, which comprised:

a. 121 TTRs totalling $2,481,590 in chip and cash exchanges; and

b. eight TTRs totalling $230,000 in account deposits.

Large and suspicious cash transactions

In 2017 and 2020, Customer 48 was included in internal reports produced by SCA titled 'AML Unusual Changes in Betting' on three occasions.

Between December 2016 and August 2021, Customer 48 conducted transactions indicative of the ML/TF typology of structuring:

a. on 26 December 2016, Customer 48 conducted two separate cash buy-ins of $5,000;

b. on 14 May 2017, Customer 48 conducted three separate cash buy-ins of $3,000, $6,000 and $1,500 respectively;

c. on 25 July 2017, Customer 48 conducted four cash buy-ins totalling $42,000;

d. on 26 July 2017, Customer 48 conducted four cash buy-ins totalling $28,500;

e. on 31 July 2017, Customer 48 conducted two cash buy-ins of $9,000 and $7,500 respectively;

f. between 24 January 2018 and 28 January 2018, Customer 48 conducted five cash buy-ins of $8,000 totalling $40,000;

g. between 10 March 2018 and 12 March 2018, Customer 48 conducted three cash buy-ins of $8,000 totalling $24,000;

h. on 24 March 2018, Customer 48 conducted two cash buy-ins totalling $10,000;

i. on 17 April 2019, Customer 48 conducted four cash buy-ins totalling $20,000, each valued between $2,000 and $8,000;

j. on 29 September 2019, Customer 48 conducted two cash buy-ins of $5,000;

k. on 6 April 2021, Customer 48 conducted two separate cash buy-ins totalling $10,000;

l. on 28 May 2021, Customer 48 conducted two cash buy-ins totalling $10,000;

m. on 26 June 2021, Customer 48 conducted two cash buy-ins totalling $9,400; and

n. on 2 August 2021, Customer 48 conducted three cash buy-ins totalling $13,000, each valued between $3,000 and $5,000.

Large and suspicious cash transactions in February 2018

In February 2018, Customer 48 conducted 12 cash buy-ins in amounts under the reporting threshold totalling $76,300. Customer 48 recorded a loss of $40,800 for the month.

In February 2018, SCA identified a discrepancy between the total value of outgoing reportable transactions versus the total value of incoming reportable transactions in relation to Customer 48. SCA had reported $313,070 in outgoing transactions and $221,000 in incoming transactions, which suggested that Customer 48 was on a winning streak, but this was not the case.

Between 10 February 2018 and 18 August 2018, Customer 48 received $270,000 into their SCA FMA in 10 separate cash transactions.

Suspicious transactions in July 2018

Between 20 July 2018 and 22 July 2018, SCA recorded that Customer 48 appeared to structure six separate transactions totalling $30,000. On 21 July 2018, Customer 48 bought in for $8,000. While those funds were being counted by SCA Customer 48 conducted a

buy-in at the next table for $2,000. On 20 July 2018 and 22 July 2018, Customer 48 made a series of cash buy-ins for $8,000, $2,000, $6,000 and $4,000: SMR dated 23 July 2018.

Between 24 July 2018 and 27 July 2018, Customer 48 repeated the same behaviour and conducted daily cash buy-ins of $2,000 and $8,000.

d. Customer 48 had access to private gaming rooms at SCA;

Particulars

See paragraph 145(e) above.

Customer 48 had access to private gaming rooms at SCA, including the Grange Room and the Platinum Room.

e. SCA did not have adequate reason to believe that Customer 48's source of wealth or source of funds was sufficient to explain the high value gambling services (table 3, s 6 of the Act) provided to Customer 48 by SCA.

Particulars

See paragraph 516 above.

By March 2017, SCA recorded that Customer 48's occupation was in construction, but did not record any further details.

By August 2021, SCA understood that:

a. Customer 48 was registered as a sole trader and worked in construction;

b. Customer 48's residential address was valued at $500,000; and

c. Customer 48's previous residential address was sold in June 2015 for $450,000.

On 9 August 2021, SCA requested further information about Customer 48's source of wealth. Customer 48 declined this request and was subsequently banned from SCA.

At no time was SCA's understanding of Customer 48's source of wealth or source of funds commensurate with their high gambling activity.

Between 2017 and 2021, SCA recorded that Customer 48's estimated buy-in exceeded $4,000,000.

SCA's determination of the ML/TF risks posed by Customer 48

1221. SCA was unable to identify or assess the ML/TF risks posed by Customer 48 appropriately because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 48.

a. On and from mid-2017, Customer 48 should have been recognised by SCA as a high risk customer for the purpose of the Act and Rules for the reasons pleaded above: see *Customer 48's risk profile* above.

Particulars

Sections 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

b. It was not until 7 March 2018 that Customer 48 was rated high risk for the purpose of the Act and Rules by SCA.

Monitoring of Customer 48's transactions

1222. At no time did SCA apply appropriate transaction monitoring to Customer 48's transactions because SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

The review, update and verification of Customer 48's KYC information

1223. SCA did not review, update or verify Customer 48's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Section 36(1)(a), (b) of the Act, rule 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 48, including the nature, extent and purpose of Customer 48's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, verify or update Customer 48's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 48's risk profile* above, there were higher ML/TF risks associated with Customer 48's source of wealth or source of funds.

SCA did not require Customer 48 provide evidence of their source of wealth until 9 August 2021, at which time SCA banned Customer 48.

d. to the extent that SCA reviewed Customer 48's KYC information on and from 7 December 2016 it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 48.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

Failure to apply appropriate due diligence suited to the high ML/TF risks

1224. Had SCA conducted ongoing customer due diligence on and from 7 December 2016 by:

a. appropriately identifying and assessing the ML/TF risks posed by Customer 48;

b. applying appropriate risk-based transaction monitoring to Customer 48; and

c. appropriately reviewing and updating Customer 48's KYC information, having regard to the high ML/TF risks;

SCA would have been required by the Act and Rules to apply the ECDD Program to Customer 48 at a time before the date of the ECDD triggers pleaded below: see *ECDD triggers in respect of Customer 48* below.

ECDD triggers in respect of Customer 48

1225. SCA was required to apply the ECDD program to Customer 48 following any ECDD triggers in respect of Customer 48.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

1226. Customer 48 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 7 March 2018 and 23 July 2018, SCA gave the AUSTRAC CEO two SMRs with respect to Customer 48.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 48 above*.

1227. Each matter pleaded at paragraph 1226 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

1228. SCA did not conduct appropriate risk-based ECDD with respect to Customer 48 following an ECDD trigger because:

a. at no time did SCA apply the ECDD program to Customer 48; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

By reason of the matters set out in *Customer 48's risk profile* above, there were real risks that Customer 48's source of wealth and source of funds were not legitimate.

It was not until 9 August 2021 that SCA issued a ban in respect of Customer 48.

b. at no time prior to 9 August 2021 did senior management consider the higher ML/TF risks posed by Customer 48 in response to an ECDD trigger, or appropriately consider whether the ML/TF risks posed by Customer 48 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

On 9 August 2021, SCA senior management were informed that Customer 48 would be requested to complete a source of wealth declaration, and would not be permitted to attend SCA until Customer 48 had returned the declaration and it had been assessed.

On 9 August 2021, SCA issued a ban in respect of Customer 48.

Contravention of s 36 of the Act in respect of Customer 48

1229. By reason of the matters pleaded at paragraphs 1217 to 1228 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 48 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1230. By reason of the matters pleaded at paragraph 1229, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 9 August 2021 with respect to Customer 48.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 49

1231. Customer 49 was a customer of SCA during the relevant period. Between 7 December 2016 and 10 December 2021, SCA recorded turnover exceeding $10,700,000 for Customer 49.

Particulars

Customer 49 was a customer of SCA from at least 19 June 2012.

On 10 December 2021, SCA issued a ban in respect of Customer 49 with the involvement of the SCA AML team.

1232. SCA provided Customer 49 with designated services within the meaning of table 1 and table 3, s 6 of the Act during the relevant period.

Particulars

On 19 June 2012, SCA opened an FMA for Customer 49 which was closed on 6 May 2016. On 5 May 2016, SCA opened a second FMA for Customer 49, which was closed 10 December 2021 (item 11, table 3, s 6 of the Act).

While a customer of SCA, Customer 49 remitted funds to and from their FMA (items 31 and 32, table 1, s 6 of the Act).

See particulars to *Customer 49's risk profile* below.

1233. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 49.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 49's risk profile

1234. On and from 7 December 2016, Customer 49, and the provision of designated services to Customer 49 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 49's risk profile prior to the relevant period

a. by 7 December 2016, Customer 49 had the following risk history:

i. SCA had formed suspicions for the purposes of s 41 of the Act with respect to Customer 49;

Particulars

SCA gave the AUSTRAC CEO an SMR pertaining to Customer 49 on 21 occasions between 19 June 2012 and 6 December 2016.

The SMRs reported:

a. Customer 49 had engaged in suspicious transactions including attempted structuring on multiple occasions, either individually

or with associates, in a suspected attempt to avoid the mandatory reporting threshold: SMRs dated 22 June 2012; 9 April 2013, 10 June 2013, 22 November 2013, 24 November 2013, 25 November 2013, 26 November 2013, 27 November 2013 and, 17 March 2014;

b. on multiple occasions, Customer 49 refused or was visibly reluctant to provide identification after making a transaction above the reporting threshold: SMRs dated 9 April 2013, and 16 April 2013; and

c. Customer 49 provided cash and chips to others so that they could conduct transactions on Customer 49's behalf: SMRs dated 26 November 2013 and 24 May 2014.

ii. Customer 49 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs;

A. between 19 June 2012 and 6 December 2016, SCA recorded a high turnover estimated at $13,564,251 for Customer 49, with cumulative losses of $223,705;

Particulars

In 2012, Customer 49's recorded individual rated gambling activity at SCA was estimated as a buy-in of $1,115,850 for table games, and for both table games and EGMs, turnover of $3,720,129 and losses of $87,399.

In 2013, Customer 49's recorded individual rated gambling activity at SCA for table games escalated to an estimated buy-in of $2,766,095, and a turnover of $6,553,095 and losses of $54,855.

In 2014, Customer 49's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $399,850, and a turnover of $1,505,416 and losses of $14,750.

In 2015, Customer 49's recorded individual rated gambling activity at SCA for table games escalated to an estimated buy-in of $586,900, and a turnover of $1,785,609 and losses of $66,700.

iii. Customer 49 transacted using large amounts of cash at SCA; and

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 21 June 2012 and 6 May 2016, SCA gave the AUSTRAC CEO 124 TTRs detailing incoming and outgoing payments made by Customer 49 totalling $1,876,919, which comprised:

a. 118 TTRs totalling $1,754,919 in chip and cash exchanges; and

b. six TTRs totalling $122,000 in account deposits.

iv. between 19 June 2012 and 6 December 2016, SCA received Jade alerts indicating that Customer 49 had completed five or more cash transactions above the reportable threshold in a single month;

Particulars

In June 2016, SCA received a Jade alert indicating that Customer 49 had completed five or more cash transactions above the reportable threshold in a single month. SCA did not consider this alert to raise any concerns regarding Customer 49 at the time.

Customer 49's risk profile during the relevant period

b. Customer 49 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs. Between 7 December 2016 and 10 December 2021, SCA recorded a high turnover estimated at $11,135,516 for Customer 49, with cumulative losses of $149,142;

Particulars

In 2016, Customer 49's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $231,950, turnover of $452,130 and losses of $19,300.

In 2017, Customer 49's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $36,700, turnover of $40,977 and losses of $15,300.

In 2018, Customer 49's recorded individual rated gambling activity at SCA for table games escalated to an estimated buy-in of $1,754,525, turnover of $5,080,953 and losses of $34,855.

In 2019, Customer 49's recorded individual rated gambling activity at SCA was estimated as a buy-in of $381,700 for table games, and for both table games and EGMs, turnover of $642,325 and wins of $26,240.

In 2020, despite closures related to the COVID-19 pandemic, Customer 49's recorded individual rated gambling activity at SCA escalated to an estimated buy-in of $671,700 for table games, and for both table games and EGMs, turnover of $3,067,158 and losses of $24,409.

In 2021, Customer 49's recorded individual rated gambling activity at SCA escalated to an estimated buy-in of $915,310 for table games, and for both table games and EGMs, turnover of $1,851,973 and losses of $105,118.

c. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 49 by remitting large amounts of money into the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

Between 1 January 2020 and 10 December 2021, SCA reported 11 incoming IFTIs totalling $80,700 where Customer 49 was named as the customer. SCA made these funds available to Customer 49's FMA.

d. Customer 49 was connected to other customers at SCA, including one player who SCA considered had acted suspiciously;

Particulars

From at least 11 January 2018, SCA was aware that Customer 49 and Customer 49's partner both had a history of attempting to structure transactions.

e. Customer 49 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 8 January 2018 and 16 June 2021, SCA gave the AUSTRAC CEO 110 TTRs detailing incoming and outgoing payments made by Customer 49 totalling $2,144,785, which comprised:

a. 92 TTRs totalling $1,755,185 in chip and cash exchanges; and

b. 18 TTRs totalling $389,600 in account deposits.

f. Customer 49 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including structuring;

Particulars

See paragraph 24 above.

For example, on 11 January 2018, Customer 49 and Customer 49's partner cashed out $9,500 and $9,570 respectively within a few minutes of each other. SCA suspected they were structuring their transactions to avoid the reporting threshold. SCA noted that Customer 49 had engaged in the majority of play prior to cashing out, and Customer 49 had held the majority of the chips that their partner cashed out.

g. Customer 49 had access to private gaming rooms at SCA; and

Particulars

See paragraph 145(e) above.

Customer 49 had access to private gaming rooms at SCA, including the Grange Room, the Black Room and the Platinum Room.

h. SCA did not have adequate reason to believe that Customer 49's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 49 by SCA.

Particulars

See paragraph 516 above.

By 7 December 2016, SCA was aware that:

a. Customer 49 had a total turnover of over $13,000,000, with cumulative losses of over $200,000; and

b. Customer 49's stated occupation was a mechanical engineer.

Throughout the relevant period, Customer 49's buy-in was consistently high, and escalated significantly in 2018.

Prior to 2021, SCA did not have any source of wealth or source of funds information for Customer 49.

In around 2021, Customer 49 provided overseas bank statements to SCA. When asked to provide further information, Customer 49 refused.

On 10 December 2021, SCA banked Customer 49 because it was not satisfied with the source of wealth information provided by Customer 49.

At no time was SCA's understanding of Customer 49's source of wealth or source of funds commensurate with the high value financial and gambling services that they received at SCA.

SCA's determination of the ML/TF risks posed by Customer 49

1235. SCA was unable to identify or assess the ML/TF risks posed by Customer 49 appropriately because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 49.

a. On and from 7 December 2016, Customer 49 should have been recognised by SCA as a high risk customer for the purpose of the Act and Rules for the reasons pleaded above: see *Customer 49's risk profile.*

Particulars

Sections 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

b. It was not until 12 January 2018 that Customer 49 was rated high risk for the purpose of the Act and Rules by SCA.

Monitoring of Customer 49's transactions

1236. At no time did SCA apply appropriate transaction monitoring to Customer 49's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 49 through the SCA Customer account channel, which was a high risk remittance channel.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 49's KYC information

1237. SCA did not review, update or verify Customer 49's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 49, including the nature, extent and purpose of Customer 49's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 49's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 49's risk profile* above, there were higher ML/TF risks associated with Customer 49's source of wealth or source of funds.

d. to the extent that SCA reviewed Customer 49's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 49.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

Failure to apply appropriate due diligence suited to the high ML/TF risks

1238. Had SCA conducted ongoing customer due diligence on and from 7 December 2016 by:

a. appropriately identifying and assessing the ML/TF risks posed by Customer 49;

b. applying appropriate risk-based transaction monitoring to Customer 49; and

c. appropriately reviewing and updating Customer 49's KYC information, having regard to the high ML/TF risks;

SCA would have been required by the Act and Rules to apply the ECDD Program to Customer 49 at a time before the date of the ECDD triggers pleaded below: see *ECDD triggers in respect of Customer 49*.

ECDD triggers in respect of Customer 49

1239. SCA was required to apply the ECDD program to Customer 49 following any ECDD triggers in respect of Customer 49.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

1240. Customer 49 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 7 December 2016 and 10 December 2021, SCA gave the AUSTRAC CEO one SMR with respect to Customer 49.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 49* above.

1241. Each matter pleaded at paragraph 1240 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

1242. SCA did not conduct appropriate risk-based ECDD with respect to Customer 49 following an ECDD trigger because:

a. on each occasion prior to 10 December 2021 that SCA conducted ECDD in respect of Customer 49 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 49 and failed to appropriately consider whether the ML/TF risks posed by Customer 49 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

On 12 January 2018 and 21 June 2021, SCA conducted ECDD in respect of Customer 49.

The ECDD screenings in respect of Customer 49 identified that:

a. Customer 49 had intentionally attempted to avoid threshold transactions;

b. Customer 49 and Customer 49's partner had engaged in structuring; and

c. Customer 49 and Customer 49's partner had previously been identified by SCA staff engaging in similar behaviour in the past on multiple occasions.

Between 2 January 2018 and 1 July 2021, SCA received 28 Jade alerts relating to cash transactions or other transactions made by Customer 49. SCA did not review 19 of the alerts. SCA resolved to take no further action with respect to nine alerts. At least nine of the alerts indicated that Customer 49 had made five or more cash transactions over the reportable threshold in a single month.

The ECDD conducted by SCA did not have appropriate regard to Customer 49's higher ML/TF risks: see *Customer 49's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 49's source of funds or source of wealth.

By reason of the matters set out in *Customer 49's risk profile* above, there were real risks that Customer 49's source of wealth and source of funds were not legitimate.

It was not until 10 December 2021 that SCA issued a ban in respect of Customer 49.

b. on any occasion prior to 10 December 2021 that senior management considered the higher ML/TF risks posed by Customer 49 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 49 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

In 2019, Customer 49 was mentioned in a 'Transaction Monitoring Overview' report for the period 1 August 2019 to 1 November 2019, which was provided to SCA's AML/CTF Senior Management Group for its consideration.

It was not until 10 December 2021 that SCA issued a ban in respect of Customer 49.

Contravention of s 36 of the Act in respect of Customer 49

1243. By reason of the matters pleaded at paragraphs 1231 to 1242 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 49 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1244. By reason of the matters pleaded at paragraph 1243, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 10 December 2021 with respect to Customer 49.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 50

1245. Customer 50 was a customer of SCA during the relevant period. Between 2017 and 2020, SCA recorded a high turnover exceeding $10,400,000 for Customer 50.

Particulars

Customer 50 was a customer of SCA from at least 2009.

On 10 May 2022, SCA issued a ban in respect of Customer 50.

1246. SCA provided Customer 50 with designated services within the meaning of table 3**,** s 6 of the Act during the relevant period.

Particulars

On 1 June 2016, SCA opened an FMA for Customer 50 which was closed on 6 May 2022 (item 11, table 3, s 6 of the Act).

See *Customer 50's risk profile* below.

1247. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 50.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 50's risk profile

1248. On and from 7 December 2016, Customer 50, and the provision of designated services to Customer 50 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 50's risk profile prior to the relevant period

a. by 7 December 2016, Customer 50 had the following risk history:

i. SCA formed suspicions for the purposes of s 41 of the Act with respect to Customer 50;

Particulars

SCA gave the AUSTRAC CEO an SMR on nine occasions between 14 May 2009 and 23 September 2013.

The SMRs reported that Customer 50 engaged in:

a. conduct indicative of the ML/TF typologies of structuring and utilising third parties to conduct transactions; and

b. other suspicious transactions involving SCA customers: see paragraph 1248.a.ii below.

ii. SCA was aware that Customer 50 had transacted using large amounts of cash at SCA, engaged in conduct indicative of the ML/TF typology of structuring, and was utilising third parties to disguise and structure transactions; and

Particulars

See paragraphs 24, and 376 to 381 above.

Customer 50 engaged in transactions indicative of the ML/TF typology of structuring on the following occasions:

a. 14 May 2009, SCA reported that Customer 50 utilised a third party to conduct two transactions in the amounts of $8,000 and $4,200. SCA noted that Customer 50 had divided their chips to avoid the reporting threshold;

b. on 7 March 2011, SCA reported that Customer 50 cashed out across four separate transactions within 20 minutes to avoid the reporting threshold;

c. on 27 June 2011, SCA reported that Customer 50 had staggered payouts a few minutes apart;

d. in May 2013, SCA reported that Customer 50 cashed out across three separate transactions within a few minutes of each other in the sums of $7,500, $2,500 and $3,500 to avoid the reporting threshold;

e. in August 2013, SCA reported that Customer 50 worked with their associate to structure transactions;

f. in September 2013, SCA reported that Customer 50 had structured two transactions within two hours, cashing out $9,990 in chips on each occasion; and

g. on 3 October 2013 and 27 October 2013, SCA reported instances where Customer 50 utilised third parties to structure

transactions and remain below the transaction reporting threshold amount. In each of those instances, SCA confirmed that all of the chips being cashed out by both Customer 50 and their associates belonged to Customer 50.

iii. Customer 50 received high value gambling services (table 3, s 6 of the Act) at SCA other than through junket programs;

Particulars

Customer 50's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $134,500 and turnover of $374,710 and losses of $15,200.

Customer 50's risk profile during the relevant period

b. Customer 50 received high value gambling services (table 3, s 6 of the Act) at SCA other than through junket programs. Between 2017 and 2020, SCA recorded an estimated buy in of $2,619,915, turnover estimated at $10,496,547 for Customer 50, with cumulative losses of $440,921;

Particulars

In 2017, Customer 50's recorded individual rated gambling activity at SCA escalated to an estimated buy-in of $1,511,585 for table games, and for both table games and EGMs, turnover of $4,835,618 and losses of $162,645.

In 2018, Customer 50's recorded individual rated gambling activity at SCA was estimated as a buy-in of $939,700 for table games, and for both table games and EGMs, turnover of $4,173,600 and losses of $189,682.

In 2019, Customer 50's recorded individual rated gambling activity at SCA was estimated as a buy-in of $152,780 for table games, and for both table games and EGMs, turnover of $1,374,575 and losses of $78,732.

Between January 2020 and March 2020, Customer 50's recorded individual rated gambling activity at SCA was estimated as a buy-in of $15,850 for table games, and for both table games and EGMs, turnover of $112,755 and losses of $9,862.

c. designated services provided to Customer 50 included substantial EGM activity at SCA;

Particulars

See paragraphs 352 and 353 above.

From 30 July 2017 to 4 March 2020, Customer 50's turnover on EGMs was estimated to be $637,274 and their total losses were estimated to be $1,429.

d. Customer 50 performed a number of transactions indicative of ML/TF typologies and vulnerabilities, including structuring, utilising third parties and cashing-in large value chips with no evidence of play;

Particulars

See paragraphs 24, and 376 to 381 above.

Transactions indicative of structuring

By May 2018, SCA was aware that Customer 50 appeared to be structuring their cash outs:

a. For example, on 19 May 2018, Customer 50 attempted to cash out $10,000 worth of cash chips at a cashier. When the cashier requested Customer 50's identification and casino membership, Customer 50 refused the request, claiming that they were not a member at SCA and that this was their first time attending SCA. Customer 50 withdrew their request to cash out and returned to the gaming tables. Customer 50 was a member of SCA, belonged to the highest membership tier (Grange Black) and was a frequent player at SCA:

b. SCA's transactional records showed that Customer 50 exclusively bought-in at tables in amounts under $10,000. For example, in May 2018, SCA recorded that since June 2016, Customer 50 had bought in at tables with approximately $1,200,000 in cash. Customer 50's transactions records showed that each of those buy-ins were under $10,000;

c. SCA had no record of Customer 50 cashing out at SCA; and

d. SCA only recorded cash outs over $10,000 to players' accounts, which meant that all Customer 50's cash outs occurred under the $10,000 limit: SMR dated 22 May 2018.

On the following occasions, Customer 50 was involved in transactions indicative of the ML/TF typology of structuring:

a. on 1 September 2018, Customer 50 cashed out $9,000 in chips at 10:48pm, entered the bathrooms, and then cashed out a further $2,000 in chips at 10:51pm;

b. on 2 September 2018, SCA frontline staff observed Customer 50 cash out $9,800, before going to the bathroom and then returning to the same Cashier to cash out a further $2,000;

c. on 7 September 2019, Customer 50 refused to provide their details when requested by SCA staff. Customer 50 had bought in for $10,000 without gaming and passed all the chips to their spouse. Once Customer 50's spouse ceased play, Customer 50 collected all their chips and attempted to cash out for $24,000;

d. on 6 November 2019, Customer 50's spouse passed them $15,000 worth of cash chips while they were playing together at a table. Customer 50 left the table and exchanged $9,700 worth of chips for cash. Customer 50 separated $700 in cash

which they placed in their wallet, and placed the remaining $9,000 in their bag. Customer 50 returned to the Baccarat Pavilion but did not recommence play. Approximately ten minutes later, Customer 50 returned to the main Cage and exchanged a further $6,500 in chips for cash. Customer 50 placed $500 of the cash in their wallet and placed the remaining $6,000 in their bag. Approximately 15 minutes later, Customer 50's spouse passed them $5,000 in chips, which Customer 50 immediately cashed out and placed in their bag. Six minutes later, the couple left the casino together. SCA concluded that Customer 50 and their spouse were structuring transactions to avoid reporting obligations: SMR dated 8 November 2019;

e. on 25 November 2019, Customer 50 and their spouse were passing cash chips between one another and cashing them out across various transactions before leaving SCA. Customer 50's spouse did not engage in any gaming. SCA considered that Customer 50 and their spouse were structuring transactions to avoid the reporting threshold: SMR dated 9 December 2019; and

f. on 10 December 2019, Customer 50 and their spouse were passing cash chips between one another and cashing them out across various transactions. Customer 50 achieved a win that, combined with the chips they had received from their spouse, exceeded the reporting threshold amount. Customer 50 conducted two cash out transactions of approximately $6,000 each within six minutes of each other. SCA recorded its suspicion that Customer 50 and their spouse were structuring transactions to avoid the transaction reporting threshold: SMR dated 12 December 2019.

Transaction reports

In 2017 and 2018, Customer 50 was included in internal SCA reports titled:

a. 'AntiMoney Laundering – February' where Customer 50's name, information and betting details are listed in the worksheets titled 'November Tables', 'January Tables' and 'February Tables'; and

b. 'AML Unusual Changes in Betting – December' where SCA recorded Customer 50's turnover for September to December 2018.

e. Customer 50 had access to private gaming rooms at SCA; and

Particulars

See paragraph 145(e) above.

Customer 50 had access to private gaming rooms at SCA including the Opal Room, the Grange Room the and Black Room.

SCA did not have adequate reason to believe that Customer 50's source of wealth or source of funds was sufficient to explain the high value gambling services (table 3, s 6 of the Act) provided to Customer 50 by SCA.

Particulars

See paragraph 516 above.

Since Customer 50 opened their account on 1 June 2016, SCA recorded their occupation as a farmer.

In May 2018, SCA recognised that Customer 50's source of funds was inconsistent with their high value gambling activities. SCA reported that Customer 50 had bought in at gaming tables with cash for approximately $1,200,000 since joining SCA in June 2016: SMR dated 22 May 2018.

In April 2019, SCA recorded Customer 50's occupation as a homemaker.

At no time did SCA request that Customer 50 provide source of wealth information.

SCA continued to provide designated services to Customer 50 until at least March 2020.

Between 2017 and 2020, SCA recorded buy-in exceeding $2,600,000 and turnover exceeding $10,800,000 for Customer 50.

At no time was SCA's understanding of Customer 50's source of wealth or source of funds commensurate with the high value gambling services that they received at SCA.

SCA's determination of the ML/TF risks posed by Customer 50

1249. SCA was unable to identify or assess the ML/TF risks posed by Customer 50 appropriately because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 50.

a. By 7 December 2016, Customer 50 should have been recognised by SCA as a high risk customer for the purpose of the Act and Rules for the reasons pleaded above: see *Customer 50's risk profile.*

Particulars

Sections 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

b. It was not until 22 May 2018 that Customer 50 was rated high risk for the purpose of the Act and Rules by SCA.

Particulars

On 3 February 2017, Customer 50 was rated medium risk for the purpose of the Act and Rules by SCA.

On 22 May 2018, Customer 50 was rated high risk for the purpose of the Act and Rules by SCA.

Monitoring of Customer 50's transactions

1250. At no time did SCA apply appropriate transaction monitoring to Customer 50's transactions because SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

The review, update and verification of Customer 50's KYC information

1251. SCA did not review, update or verify Customer 50's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 50, including the nature, extent and purpose of Customer 50's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 50's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 50's risk profile* above, there were real risks that Customer 50's source of wealth and source of funds were not legitimate.

SCA was aware that Customer 50's source of funds was inconsistent with their high value gambling activities: see *Customer 50's risk profile* above.

d. to the extent that SCA reviewed Customer 50's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 50.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

SCA maintained inconsistent identification records in respect of Customer 50: see paragraph 546 above.

SCA held two player profiles for Customer 50. Each player profile had different identification records, including different information about Customer 50's date of birth, home address, occupation and identification documents. SMRs were reported for Customer 50 against both player profiles. In addition, data from player profiles was combined in SCA's internal monitoring documents and ECDD reports in respect of Customer 50.

In May 2018, SCA recorded an incident where Customer 50 refused to show their identification at an SCA Cashier. The Compliance Team recorded that the instance was suspicious in light of the fact that there were inconsistencies in the information contained in Customer 50's player profile: SMR dated 22 May 2018.

Failure to apply appropriate due diligence suited to the high ML/TF risks

1252. Had SCA conducted ongoing customer due diligence on and from 7 December 2016 by:

a. appropriately identifying and assessing the ML/TF risks posed by Customer 50;

b. applying appropriate risk-based transaction monitoring to Customer 50; and

c. appropriately reviewing and updating Customer 50's KYC information, having regard to the high ML/TF risks;

SCA would have been required by the Act and Rules to apply the ECDD Program to Customer 50 at a time before the date of the ECDD triggers pleaded below: see *ECDD triggers in respect of Customer 50*.

ECDD triggers in respect of Customer 50

1253. SCA was required to apply the ECDD program to Customer 50 following any ECDD triggers in respect of Customer 50.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules

1254. Customer 50 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 22 May 2018 and 12 December 2019, SCA gave the AUSTRAC CEO 4 SMRs with respect to Customer 50.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 50* above.

1255. Each matter pleaded at paragraph 1254 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

1256. SCA did not conduct appropriate risk-based ECDD with respect to Customer 50 following an ECDD trigger because:

a. on each occasion prior to 10 May 2022 that SCA conducted ECDD in respect of Customer 50 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 50 and failed to appropriately consider whether the ML/TF risks posed by Customer 50 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

Between 7 June 2016 and 26 June 2021, SCA received six open source Dow Jones watchlist alerts in respect to Customer 50, but resolved to close the alerts.

SCA conducted ECDD in respect of Customer 50 on two occasions. On 10 April 2019, SCA conducted ECDD in respect of Customer 50 citing SMRs reported against one of their SCA player profiles.

On 19 December 2019, SCA conducted further ECDD in respect of Customer 50, citing the SMR reported in relation to Customer 50's second SCA player profile. The ECDD screenings identified:

a. at least ten transactions between April 2009 and May 2018 that were indicative of ML/TF typologies including structuring;

b. the inconsistent information in Customer 50's player profile and the suspicious incident where Customer 50 refused to show their identification at an SCA Cashier: SMR dated 22 May 2018; and

c. that Customer 50's occupation was not consistent with their gambling activity.

At no time was SCA's understanding of Customer 50's source of wealth or source of funds commensurate with the high value financial and gambling services that they received at SCA.

The ECDD conducted by SCA did not have appropriate regard to Customer 50's higher ML/TF risks: see *Customer 50's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 50's source of funds or source of wealth.

By reason of the matters set out in *Customer 50's risk profile* above, there were real risks that Customer 50's source of wealth and source of funds were not legitimate.

It was not until 10 May 2022 that SCA issued a ban in respect of Customer 50.

b. at no time prior to 10 May 2022 did senior management consider the higher ML/TF risks posed by Customer 50 in response to an ECDD trigger, or appropriately consider whether the ML/TF risks posed by Customer 50 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

It was not until 10 May 2022 that SCA issued a ban in respect of Customer 50.

Contravention of s 36 of the Act in respect of Customer 50

1257. By reason of the matters pleaded at paragraphs 1245 to 1256 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 50 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1258. By reason of the matters pleaded at paragraph 1257, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 10 May 2022 with respect to Customer 50.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 51

1259. Customer 51 was a customer of SCA during the relevant period. Between 2018 and 2021, SCA recorded turnover exceeding $9,100,000 for Customer 51.

Particulars

Customer 51 was a customer of SCA from at least 17 May 2018.

On 17 December 2021, SCA issued a ban in respect of Customer 51.

1260. SCA provided Customer 51 with designated services within the meaning of tables 1 and 3, s 6 of the Act during the relevant period.

Particulars

On 17 May 2018, SCA opened an FMA for Customer 51 which remained open as at 28 October 2022 (item 11, table 3, s 6 of the Act).

While a customer of SCA, Customer 51 remitted funds to their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 51's risk profile* below.

1261. At all times from 17 May 2018, SCA was required to conduct ongoing customer due diligence in respect of Customer 51.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 51's risk profile

1262. On and from 17 May 2018, Customer 51, and the provision of designated services to Customer 51 by SCA, posed higher ML/TF risks because of the following red flags:

a. Customer 51 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs. Between 2018 and 2021, SCA recorded an estimated buy-in of $2,192,440, turnover estimated at $9,108,578 for Customer 51, with cumulative losses of $219,009;

Particulars

In 2018, Customer 51's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $46,390, turnover of $153,125 and losses of $17,790.

In 2019, Customer 51's recorded individual rated gambling activity at SCA for table games escalated to an estimated buy-in of $81,605, turnover of $422,983 and losses of $13,248.

In 2020, despite closures related to the COVID-19 pandemic, Customer 51's recorded individual rated gambling activity at SCA significantly escalated to an estimated buy-in of $1,782,320 for table games, and for both table games and EGMs, turnover of $7,703,695 and losses of $218,571.

In 2021, Customer 51's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $282,125, turnover of $828,775 and wins of $30,600.

b. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 51 by remitting large amounts of money into the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

In a report dated October 2021, Bank 1 stated that, between 1 September 2019 and 31 May 2021, Customer 51 was the fourth highest SCA depositor by volume into SCA's bank account. Bank 1 identified that during this period, Customer 51 made at least 87 deposits totalling over $531,000.

Between 16 December 2019 and 20 March 2021, SCA received 125 telegraphic transfers totalling approximately $824,080, each of which was made available to Customer 51's FMA.

c. SCA was aware that Customer 51 had engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

Particulars

On 1 July 2020, Customer 51 attended SCA and made a cash buy-in at a table with $30,900. The cash was contained in four envelopes, and SCA staff noted that Customer 51 seemed unsure about the total amount of cash they had in the envelopes. Customer 51 then received a CPV for $58,000 from their FMA, and presented it for redemption. Customer 51 played for less than half an hour, and then presented $90,000 in cash chips in exchange for cash. SCA considered that Customer 51's buy-in was considerably higher than normal.

On 6 August 2020, Customer 51 attended SCA and handed another SCA customer an unknown amount of cash. That customer then immediately went to a Cashier and exchanged $10,000 in $50 notes for two $5,000 cash chips and proceeded to use them for gaming. Customer 51 bought in separately for $7,000 in cash at the Cashier.

On 11 December 2020, an SCA AML Advisor emailed a Table Games – VIP Manager regarding an SCA customer performing a number of large cash transactions on behalf of other customers, including Customer 51. The AML Advisor noted that they were not comfortable with the customer acting as a runner on behalf of other customers for such significant transactions, and they placed a note on the customer's account advising the Cage not to allow them to perform such transactions.

On 9 February 2021, Customer 51 attended SCA with two other SCA customers. Customer 51 attended a Cashier and removed an envelope from their satchel. The envelope contained $15,000 in $100 notes. Customer 51 exchanged the cash for fifteen $1,000 cash

chips. Customer 51 then re-joined the other two customers and gave the chips to one of them. The two customers left Customer 51 and attended the Grange Room. The customer who had received the chips from Customer 51 then commenced play using the chips. The customer gave some of the cash chips to the second customer: SMR dated 10 February 2021.

d. Customer 51 was connected to other customers at SCA, including players who posed higher ML/TF risks such as Customer 18 and players who SCA considered had acted suspiciously, including Person 26;

Particulars

In or around September 2021, Person 26 presented bank statements for their personal bank account (which had since been closed) to SCA as source of wealth evidence. SCA's review of Person 26's bank statement indicated that, between 20 June 2020 and 15 April 2021, the customer sent approximately $108,400 in 10 transactions to Customer 51. During this period, Person 26 also made a number of transactions to other SCA customers' accounts. Based on these transactions, SCA considered that Customer 51 was potentially using the customer to layer funds through multiple bank accounts to avoid detection. SCA also considered that Person 26 may have been utilised as a money mule for a network of money laundering or money concealing activities: SMR dated 5 October 2021.

See *Customer 18's risk profile* above.

e. Customer 51 transacted using large amounts of cash and chips at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 3 July 2020 and 29 March 2021, SCA gave the AUSTRAC CEO 108 TTRs detailing incoming and outgoing payments made by Customer 51 totalling $1,907,780, which comprised:

a. five TTRs totalling $83,600 in account withdrawals;

b. 29 TTRs totalling $470,800 in account deposits; and

c. 74 TTRs totalling $1,353,380 in chip and cash exchanges.

Large and suspicious cash transactions in 2020

From July to December 2020, SCA frequently recorded that Customer 51 made significant buy-ins or cash outs at SCA. For example:

a. on 1 July 2020, Customer 51 exchanged $30,900 in cash for chips. Within a short time, Customer 51 also redeemed a $58,000 CPV, and then exchanged $90,000 in chips for cash;

b. on 7 August 2020, Customer 51 exchanged $12,000 in cash chips for cash. Customer 51 then exchanged $10,000 in cash and received chips. Less than an hour later, Customer 51 exchanged $18,020 in chips for cash. Several hours later, Customer 51 bought in with $10,000 in cash;

c. between 17 August 2020 and 18 August 2020, Customer 51 deposited a total of $35,000 in cash into their FMA, made cash and chip exchanges totalling $31,000, and withdrew $10,000 in cash from their FMA;

d. between 15 September 2020 and 21 September 2020, Customer 51 withdrew a total of $28,500 in cash and chips from their FMA and made cash and chip exchanges totalling $54,010;

e. between 28 November 2020 and 30 November 2020, Customer 51 deposited a total of $62,000 in cash and chips into their FMA, withdrew $40,000 in cash from their FMA, and made a cash buy-in of $10,000; and

f. on 9 December 2020, Customer 51 exchanged $35,000 in cash for chips. Less than an hour later, Customer 51 exchanged $15,000 in chips for cash. Two hours later, Customer 51 exchanged $13,000 in chips for cash.

Large and suspicious cash transactions in 2021

Between January 2021 and March 2021, SCA frequently recorded that Customer 51 made significant buy-ins or cash outs at SCA. For example:

a. on 18 January 2021, Customer 51 made a cash buy-in of $42,300 and received chips. Approximately 20 minutes later, Customer 51 exchanged $50,000 in chips for cash;

b. between 22 January 2021 and 25 January 2021, Customer 51 made a number of cash and chip exchanges totalling $184,000;

c. on 28 January 2021, Customer 51 bought in with $30,000 in cash and received chips. Approximately 20 minutes later, Customer 51 exchanged $35,500 in chips for cash;

d. on 31 January 2021, Customer 51 exchanged $10,300 in chips for cash. Later that day, Customer 51 bought in with $15,000 in cash and received chips. Ten minutes later, Customer 51 exchanged $15,000 in chips for cash and withdrew $5,000 from their account in cash. They then exchanged $10,000 in cash for chips;

e. on 7 February 2021, Customer 51 withdrew $45,000 from their account in chips. Less than an hour later, Customer 51

exchanged $45,000 in chips for cash. Customer 51 then made two cash withdrawals totalling $20,000 from their FMA; and

f. between 20 March 2021 and 21 March 2021, Customer 51 withdrew $30,000 from their account in chips and made cash and chip exchanges totalling $70,925.

f. Customer 51 and persons associated with them engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including structuring, cashing-in large value chips with no evidence of play, and layering;

Particulars

See paragraph 24 above.

See particulars to paragraphs 1262.c, 1262.d and 1262.e above.

On the following occasions, Customer 51 was involved in transactions indicative of ML/TF typologies:

a. on 30 November 2020, Customer 51 presented $10,000 in cash to an SCA Cashier. The cash was processed in two separate transactions, as a $9,000 FMA deposit and a $1,000 chip sale. These transactions were indicative of the ML/TF typology of structuring.

b. between 27 November and 2 December 2020, Customer 51 regularly attended SCA with plastic bags containing a large number of notes of mixed denominations. Customer 51 would exchange the cash for chips, and within 45 minutes would cash out a significant amount of the chips and receive $100 notes in return. During this period, Customer 51 also purchased at least $54,100 in chips and deposited $87,800 into their FMA. These transactions were indicative of the ML/TF typologies of refining and cashing-in large value chips with no evidence of play.

c. on 6 December 2020, an SCA customer made a cash buy-in for $26,200 in the Grange Room. Less than two hours later, the customer cashed out $35,300. SCA noted that the customer had no play on the table and had told staff that they were a runner and bodyguard for Customer 51 and another person who was also a customer of SCA. The buy-in and cash out were recorded under the name of the customer who claimed to be a bodyguard. Less than five minutes after the cash out, Customer 51 bought a $1,000 chip with cash and then left SCA with the other two customers. These transactions were indicative of the ML/TF typology of cashing-in large value chips with no evidence of play. SCA considered that the sharing of funds between Customer 51 and their two associates was unusual, but did not think there was anything to suggest any criminal activity was occurring. It considered

the customer's explanation that they were Customer 51's runner and bodyguard to be plausible.

d. on 28 January 2021, Customer 51 presented $30,000 in cash at SCA and exchanged the funds for chips. The cash was comprised of $50 notes. Customer 51 then engaged in play, and recorded a turnover of $9,825 with a win of $5,500. Customer 51 then returned to the Cashier and presented $35,500 in chips. Customer 51 exchanged the chips for $100 notes. These transactions were indicative of the ML/TF typology of refining.

e. on 31 January 2021, Customer 51 made a telegraphic transfer of $5,000 to their SCA account and withdrew the funds as cash. Customer 51 then took $15,000 in chips from their pocket and cashed them out. SCA staff noted that Customer 51 had engaged in minimal play at the time of the transaction. These transactions were indicative of the ML/TF typology of cashing in large value chips with no evidence of play.

f. on 7 February 2021, Customer 51 made five telegraphic transfers to their SCA FMA totalling $73,000. The transfers came from different banks, which SCA considered unusual. Customer 51 then withdrew $45,000 from their account in gaming chips. Less than an hour later, Customer 51 exchanged the chips for $50 notes. SCA table games staff reported that Customer 51 had not recorded any play in the interim. Customer 51 then made three cash withdrawals from their FMA totalling $28,000. SCA recorded that throughout this period Customer 51 was agitated and constantly using their mobile phone. SCA queried Customer 51 regarding these transactions and their lack of gaming. Customer 51 informed staff that the funds and transfers were facilitating the purchase of a house overseas, and their agitated demeanour was due to the cut-off for the house purchase having been on 6 February 2021: SMR dated 10 February 2021. These transactions were indicative of the ML/TF typology of cashing-in large value chips with no evidence of play.

g. in 2020, Customer 51 was the subject of law enforcement enquiries on one occasion at SCA;

Particulars

On 22 October 2020, SCA received a request from a law enforcement agency regarding Customer 51's gaming records and transactions from 1 January 2020 to the date of the notice. The notice also requested information regarding a specific TTR.

h. by at least February 2021, SCA held suspicions that Customer 51 was involved in underground banking or unregistered hawala activity;

Particulars

By 10 February 2021, SCA suspected that Customer 51 was using SCA to circumvent foreign capital controls or to act as an underground bank for foreign nationals in Australia: SMR dated 10 February 2021.

See particulars to paragraphs 1262.c to 1262.f above.

i. Customer 51 had access to private gaming rooms at SCA; and

Particulars

See paragraph 145(e) above.

Customer 51 had access to private gaming rooms at SCA, including the Black Room and the Platinum Room.

j. SCA did not have adequate reason to believe that Customer 51's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 51 by SCA.

Particulars

See paragraph 516 above.

By at least 24 November 2020, SCA understood that Customer 51 was a property developer. SCA identified that Customer 51's contact number was linked to a residential property development company and a flooring company. SCA also noted that Customer 51's social media account listed them as a director of a large multi-level marketing company.

By October 2020, SCA had been contacted by a law enforcement agency in respect of Customer 51. In February 2021, SCA developed suspicions that Customer 51 was involved in underground banking.

Until December 2021, SCA took no steps to obtain any information regarding Customer 51's source of wealth.

On or around 17 December 2021, SCA sent Customer 51 a letter asking them to complete a Source of Wealth Declaration. On the same date, SCA banned Customer 51 from attending the casino until they had provided the source of wealth information.

When SCA did obtain a source of wealth declaration and supporting documentation from Customer 51, in April 2022, it identified a number of issues with the information provided by Customer 51, including:

a. SCA could not reconcile Customer 51's stated salary from a property development company based on the documents Customer 51 had provided, including payslips;

b. SCA could not verify that Customer 51 derived any wealth from three companies for which they claimed to be the sole director and shareholder;

c. in respect of one of the companies for which Customer 51 claimed they were the sole director and shareholder, SCA identified inconsistencies between the different financial documents Customer 51 provided, and determined that it was unable to reconcile these differences; and

d. Customer 51 failed to provide evidence of any shareholding in respect of another company of which Customer 51 claimed they were sole director and shareholder.

By April 2022, SCA had recorded buy-in for Customer 51 exceeding $2,100,000. SCA's understanding of Customer 51's source of wealth or source of funds was not commensurate with the high value financial gambling services that they received at SCA,

After considering Customer 51's Source of Wealth Declaration and the supporting documents, SCA concluded that it could not verify the information Customer 51 had provided regarding their source of wealth. Based on these concerns, as well as suspicions that Customer 51 was involved in underground banking or unregistered hawala activity, SCA determined that it could not be confident that Customer 51's gaming funds were from legitimate sources: SMR dated 29 April 2022.

SCA therefore decided to keep the ban in respect of Customer 51 in place.

SCA's determination of the ML/TF risks posed by Customer 51

1263. On and from 7 September 2020, Customer 51 was appropriately rated by SCA as a high risk customer for the purpose of the Act and Rules.

1264. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 51 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by it with respect to Customer 51.

Monitoring of Customer 51's transactions

1265. At no time did SCA apply appropriate transaction monitoring to Customer 51's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 51 through the SCA Customer account channel, which was a high risk remittance channel.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 51's KYC information

1266. SCA did not review, update or verify Customer 51's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 51, including the nature, extent and purpose of Customer 51's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 51's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 51's risk profile* above, there were higher ML/TF risks associated with Customer 51's source of wealth or source of funds.

d. to the extent that SCA reviewed Customer 51's KYC information on and from 17 May 2018, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 51.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

On 1 July 2020, SCA surveillance staff conducted a review of Customer 51's transactions that day and an SCA Legal & Compliance Advisor and an SCA AML Advisor were advised of the findings.

ECDD triggers in respect of Customer 51

1267. SCA was required to apply the ECDD program to Customer 51 following any ECDD triggers in respect of Customer 51.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

1268. Customer 51 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 10 February 2021 and 29 April 2022, SCA gave the AUSTRAC CEO three SMRs with respect to or pertaining to Customer 51.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 51* above.

1269. Each matter pleaded at paragraph 1268 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

1270. SCA did not conduct appropriate risk-based ECDD with respect to Customer 51 following an ECDD trigger because:

a. on each occasion prior to 17 December 2021 that SCA conducted ECDD in respect of Customer 51 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 51 and failed to appropriately consider whether the ML/TF risks posed by Customer 51 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

On several occasions between 24 November 2020 and 2 November 2021, SCA conducted ECDD in respect of Customer 51.

Watchlist alerts

Between 10 July 2020 and 16 July 2021, SCA received three open source Dow Jones watchlist alerts in respect of Customer 51.

Transaction reviews

Between December 2020 and February 2021, SCA conducted a surveillance review of Customer 51's transactions at SCA on three occasions. On each occasion, SCA AML Advisors were advised of the findings.

ECDD screenings

On 24 November 2020 and 3 September 2021, SCA conducted ECDD in respect of Customer 51. The ECDD consisted of reviews of:

a. Customer 51's occupation and source of wealth, which was listed as a property developer;

b. open source searches, which revealed that Customer 51 was linked to a property development company, a flooring company and an international multi-level marketing company;

c. Customer 51's known associates at SCA; and

d. SMRs in respect of Customer 51 given to the AUSTRAC CEO between July 2020 and February 2021.

Following the ECDD conducted on 3 September 2021, SCA recommended that a completed Source of Wealth Declaration be obtained from Customer 51. However, SCA did not request this form from Customer 51 until December 2021: see particulars to paragraph 1262.j above.

Other ECDD

On or around 18 December 2020, SCA prepared a document setting out Customer 51's known associates and their account details and addresses.

On or around 2 November 2021, SCA completed a review of all transactions conducted on SCA customer accounts between 4 September 2019 and 5 October 2021. The results of the review were sent to an SCA AML Compliance Manager and an SCA AML Analyst. One of the findings from the review was that Customer 51 engaged in repetitive behaviour that was indicative of the ML/TF typology of structuring.

The ECDD conducted by SCA did not have appropriate regard to Customer 51's higher ML/TF risks: see *Customer 51's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 51's source of funds or source of wealth.

By reason of the matters set out in *Customer 51's risk profile* above, there were higher ML/TF risks associated with Customer 51's source of wealth or source of funds.

On 17 December 2021, SCA issued a ban in respect of Customer 51.

b. on any occasion prior to 17 December 2021 that senior management considered the higher ML/TF risks posed by Customer 51 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 51 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

Between February and May 2021, Customer 51 was mentioned in two 'Transaction Monitoring Overview' reports which were provided to the AML/CTF Senior Management Group for discussion at their meetings. One of these reports noted that Customer 51 had been added to the '5 or more TTR's Report' and the 'Unusual Changes in Betting Habits Report' due to a series of telegraphic transfers they had conducted and chips they had purchased without commensurate gambling activity.

On 17 December 2021, SCA issued a ban in respect of Customer 51.

Contravention of s 36 of the Act in respect of Customer 51

1271. By reason of the matters pleaded at paragraphs 1259 to 1270 above, on and from 17 May 2018, SCA:

a. did not monitor Customer 51 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1272. By reason of the matters pleaded at paragraph 1271, SCA contravened s 36(1) of the Act on and from 17 May 2018 to 17 December 2021 with respect to Customer 51.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 52

1273. Customer 52 was a customer of SCA during the relevant period. Between December 2016 and June 2022, SCA recorded turnover exceeding $7,684,398 for Customer 52.

Particulars

Customer 52 was a customer of SCA from at least 6 February 2014.

On 31 May 2022, SCA issued a ban in respect of Customer 52 at the direction of the SCA AML team.

1274. SCA provided Customer 52 with designated services within the meaning of table 1 and table 3, s 6 of the Act during the relevant period.

Particulars

Prior to 7 December 2016, SCA opened an FMA for Customer 52 which was closed on 31 May 2022 (item 11, table 3, s 6 of the Act).

While a customer of SCA, Customer 52 remitted funds to and from their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 52's risk profile* below.

1275. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 52.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 52's risk profile

1276. On and from 7 December 2016, Customer 52, and the provision of designated services to Customer 52 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 52's risk profile prior to the relevant period

a. by 7 December 2016, Customer 52 had the following risk history:

   i. SCA had formed suspicions for the purposes of s 41 of the Act with respect to Customer 52;

Particulars

SCA gave the AUSTRAC CEO an SMR on 16 May 2016 which reported SCA's concerns that Customer 52's high spend at the casino was not commensurate with their stated source of funds. SCA reported that:

   a. between February 2014 and April 2016, Customer 52 made cash transactions totalling $2,011,480;

   b. Customer 52 asked an SCA Cashier if they could cash in smaller amounts or put their chip value on their reward card to avoid AML detection;

   c. Customer 52 lost approximately $80,011 in two and a half years and their explanation as to the source of funds, particularly cash, was questionable; and

   d. Customer 52 used funds from Person 27, who was a banned SCA customer and suspected money launderer.

   ii. Customer 52 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 26 March 2014 and 10 May 2016, SCA gave the AUSTRAC CEO 59 TTRs detailing transactions made by Customer 52 totalling $935,380, which comprised:

a. 50 TTRs totalling $789,420 in chip and cash exchanges;

b. one TTR totalling $29,500 for an account deposit; and

c. eight TTRs totalling $116,460 in account withdrawals.

iii. senior management at SCA were aware that Person 27, whom it suspected of being involved in money laundering, was supplying Customer 52 with cash; and

Particulars

On 18 May 2016, an internal memorandum was circulated to SCEG's General Counsel and Chief Risk Officer, SCA's AML Compliance Officer and General Manager Legal, Compliance & Regulatory Affairs, and the Acting General Manager, Adelaide, seeking approval regarding whether SCA should continue its business relationship with an associate of Customer 52, Person 27, who had been rated 'significant' risk. The memorandum stated that Person 27 had been supplying money to Customer 52 and noted that Customer 52 had asked SCA Cashiers how to avoid AML detection.

iv. Customer 52 received high value gambling services (table 3, s 6 of the Act) at SCA other than through junket programs;

Particulars

Between 1 July 2015 and 6 December 2016, SCA recorded a high turnover estimated at $3,061,631 for Customer 52, with total buy-in of $338,260 and losses of $24,555.

Customer 52's risk profile during the relevant period

b. Customer 52 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs. Between 2016 and 2022, SCA recorded an estimated buy-in of $439,740, turnover estimated at $7,684,398 for Customer 52, with cumulative losses of $242,871;

Particulars

In 2016, Customer 52's recorded individual rated gambling activity at SCA was a buy-in of $250,380 for table games, and for both table games and EGMs, turnover of $2,845,822 and losses of $55,045.

In 2017, Customer 52's recorded individual rated gambling activity at SCA was a buy-in of $257,945 for table games, and for both table games and EGMs, turnover of $2,867,213 and losses of $83,644.

In 2018, Customer 52's recorded individual rated gambling activity at SCA was estimated as a buy-in of $12,675 for table games, and for both table games and EGMs turnover of $132,476 and losses of $14,894.

In 2019, Customer 52's recorded individual rated gambling activity at SCA was estimated as a buy-in of $4,700 for table games, and for both table games and EGMs turnover of $2,479,953 and wins of $6,903.

In 2020, despite closures related to the COVID-19 pandemic, Customer 52's recorded individual rated gambling activity at SCA was estimated as a buy-in of $3,000 for table games, and for both table games and EGMs turnover of $561,127 and losses of $29,925.

In 2021, Customer 52's recorded individual rated gambling activity at SCA was estimated as a buy-in of $700 for table games, turnover of $922,326 and losses of $21,677 for both table games and EGMs.

c. designated services provided to Customer 52 included substantial EGM activity at SCA;

Particulars

See paragraphs 352 and 353 above.

Between 7 December 2016 and January 2022, Customer 52's total turnover for EGM activity totalled $5,928,149 with losses of $73,229.

In 2016, Customer 52's turnover for EGMs was $1,991,421.

In 2017, Customer 52's turnover for EGMs was $1,745,347.

In 2018, Customer 52's turnover for EGMs was $91,258.

In 2019, Customer 52's turnover for EGMs was $2,469,553.

In 2020, despite closures related to the COVID-19 pandemic, Customer 52's turnover for EGMs was $543,212.

In 2021, Customer 52's turnover for EGMs was $853,841.

Between 2 January 2022 and 13 January 2022, Customer 52's turnover for EGMs was $55,320.

On 15 July 2019, Customer 52 was issued a cheque for $37,745 for an EGM win.

On 22 October 2021, Customer 52 won $10,000 on EGMs and was recorded as a significant player on table games.

On 2 December 2021, Customer 52 lost $5,000 on EGMs and was recorded as a significant player on table games.

d. Customer 52 was connected to other customers at SCA, including customers who posed higher ML/TF risks such as Person 27 and Person 28, who SCA considered had acted suspiciously;

Particulars

SCA was aware that Customer 52 was a close associate of Person 27, a significant risk customer, who was banned from the casino on 22 March 2022. SCA suspected Person 27 of structuring and using

runners to conduct cash outs on their behalf. SCA was aware that Person 27 had been charged with drug and firearm offences: SMRs dated 31 March 2014, 6 April 2014, 19 July 2014, 22 July 2014, 2 August 2014, 7 August 2014, 13 August 2014, 14 August 2014 and 16 May 2016.

SCA believed that Person 27 was providing Customer 52 with large amounts of cash to fund their gaming. After Person 27 was banned in April 2016 (the ban imposed in 2016 expired in June 2018), Customer 52's attendance and gaming dropped: SMR dated 21 December 2016.

SCA was aware that Customer 52 was also a known associate of Person 28 who was banned from the casino on 10 May 2022.

e. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 52 by remitting large amounts of money into and out of the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

Between 29 March 2017 and 9 January 2022, SCA received eight telegraphic transfers totalling $11,030, each of which was made available to Customer 52's FMA.

Between 8 April 2021 and 2 December 2021, Customer 52 received refunds totalling $6,940 from their SCA FMA via telegraphic transfer in 11 separate transactions.

f. Customer 52 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

Between 8 December 2016 and 20 October 2021, SCA recorded a cash buy-in of totalling $408,640 for table games for Customer 52, including a cash buy-in for table games totalling $243,745 in 2017.

TTRs

Between 9 December 2016 and 17 July 2019, SCA gave the AUSTRAC CEO 29 TTRs detailing transactions made by Customer 52 totalling $427,980, which comprised:

a. 19 TTRs totalling $251,730 in chip and cash exchanges; and

b. 10 TTRs totalling $176,250 in account withdrawals.

Large FMA cash deposits

In 2017, Customer 52 deposited $10,946 into their SCA FMA across 32 cash transactions.

In 2019, Customer 52 deposited $19,540 into their SCA FMA across 11 cash transactions.

In 2020, Customer 52 deposited $11,220 into their SCA FMA across eight cash transactions.

In 2021, Customer 52 deposited $12,730 into their SCA FMA across eight cash transactions.

g. Customer 52 engaged in other transactions indicative of ML/TF typologies and vulnerabilities;

Particulars

See paragraph 24 above.

For example, on 21 December 2016, SCA recorded its concerns that Customer 52 was receiving funds from a third party, Person 27, and that Person 27 was using Customer 52 to disguise their play.

h. Customer 52 had access to private gaming rooms at SCA; and

Particulars

See paragraph 145(e) above.

Customer 52 had access to private gaming rooms at SCA, including the Platinum Room and the Grange Room.

i. SCA did not have adequate reason to believe that Customer 52's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 52 by SCA.

Particulars

See paragraph 516 above.

By 7 December 2016, SCA recorded that the only information it had concerning Customer 52's source of wealth and source of funds was that they were employed as a bus driver, and this did not correspond with the high value financial and gambling services they received: SMR dated 16 May 2016.

Between May 2017 and February 2019, SCA recorded its concerns that Customer 52's high spend at the casino was not commensurate with their stated source of funds and did not align with their gaming patterns.

At no time did SCA request source of wealth or source of funds information from Customer 52.

At no time was SCA's understanding of Customer 52's source of wealth and source of funds commensurate with the high value financial and gambling services that they received at SCA.

Between 2016 and 2022, SCA recorded a buy-in exceeding $400,000 and turnover exceeding $7,600,000 for Customer 52.

SCA's determination of the ML/TF risks posed by Customer 52

1277. On and from 7 December 2016, Customer 52 was appropriately rated by SCA as a high risk customer for the purpose of the Act and Rules.

Particulars

Section 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

1278. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 52 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by it with respect to Customer 52.

Monitoring of Customer 52's transactions

1279. At no time did SCA apply appropriate transaction monitoring to Customer 52's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 52 through the SCA Customer account channel, which was a high risk remittance channel.

Particulars

Sections 36(1)(a), (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 52's KYC information

1280. SCA did not review, update or verify Customer 52's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 52, including the nature, extent and purpose of Customer 52's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update or verify Customer 52's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 52's risk profile* above, there were higher ML/TF risks associated with Customer 52's source of wealth or source of funds.

d. to the extent that SCA reviewed Customer 52's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 52.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

ECDD triggers in respect of Customer 52

1281. SCA was required to apply the ECDD program to Customer 52 following any ECDD triggers in respect of Customer 52.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

1282. Customer 52 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

On 21 December 2016, SCA gave the AUSTRAC CEO one SMR with respect to Customer 52.

b. determined by SCA to be high risk for the purpose of the Act and Rules prior to the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 52* above.

1283. Each matter pleaded at paragraph 1282 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

1284. SCA did not conduct appropriate risk-based ECDD with respect to Customer 52 following an ECDD trigger because:

a. on each occasion prior to 31 May 2022 that SCA conducted ECDD in respect of Customer 52 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 52 and failed to appropriately consider whether the ML/TF risks posed by Customer 52 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

At various times between December 2016 and August 2021, SCA conducted ECDD screenings in respect of Customer 52 which identified that:

a. SCA was concerned about Customer 52's high spending at its casino;

b. Customer 52's known associate, Person 27, was a suspected money launderer and was banned from SCA. Customer 52 was seen receiving funds from Person 27 on 20 December 2016;

c. Person 28 was one of Customer 52's known associates; and

d. SCA had conducted open source searches in respect of Customer 52 but concluded that it did not have any information regarding Customer 52's source of wealth or source of funds.

The ECDD conducted by SCA did not have appropriate regard to Customer 52's higher ML/TF risks: see *Customer 52's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 52's source of funds or source of wealth.

By reason of the matters set out in *Customer 52's risk profile* above, there were higher ML/TF risks associated with Customer 52's source of wealth or source of funds.

It was not until 31 May 2022 that SCA issued a ban in respect of Customer 52.

b. on any occasion prior to 31 May 2022 that senior management considered the higher ML/TF risks posed by Customer 52 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 52 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

On 22 August 2019, Customer 52 was mentioned in a 'Transaction Monitoring Overview' report for the period 1 May 2019 to

1 August 2019, which was provided to the AML/CTF Senior Management Group for discussion at its meeting.

On 17 May 2022, the SCEG AML/CFT Compliance and Intelligence Manager New Zealand advised SCA's AML General Manager that Customer 52 was to be rated significant after an ECDD refresh process.

On 31 May 2022, SCA issued a ban in respect of Customer 52.

Contravention of s 36 of the Act in respect of Customer 52

1285. By reason of the matters pleaded at paragraphs 1273 to 1284 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 52 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1286. By reason of the matters pleaded at paragraph 1285, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 31 May 2022 with respect to Customer 52.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 53

1287. Customer 53 was a customer of SCA during the relevant period. Between 7 December 2016 and 8 September 2021, SCA recorded turnover exceeding $5,800,000 for Customer 53.

Particulars

Customer 53 was a customer of SCA from at least 3 April 2001.

On 8 September 2021, SCA issued a ban in respect of Customer 53.

1288. SCA provided Customer 53 with designated services within the meaning of tables 1 and 3, s 6 of the Act during the relevant period.

Particulars

Prior to 1 July 2015, SCA opened an FMA for Customer 53 which remained open as at 28 October 2022 (item 11, table 3, s 6 of the Act).

While a customer of SCA, Customer 53 remitted funds to and from their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 53's risk profile* below.

1289. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 53.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 53's risk profile

1290. On and from 7 December 2016, Customer 53, and the provision of designated services to Customer 53 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 53's risk profile prior to the relevant period

a. by 7 December 2016, Customer 53 had the following risk history:

   i. SCA was aware that Customer 53 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs; and

Particulars

Between 2001 and 6 December 2016, Customer 53's recorded individual rated gambling activity at SCA was estimated as a buy-in of $907,466 for table games, and for both table games and EGMs, turnover of $4,542,959 and wins of $355,684.

   ii. Customer 53 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

On 22 May 2011 and 23 December 2015, SCA gave the AUSTRAC CEO a TTR detailing outgoing payments made by Customer 53 totalling $21,000, which comprised of exchanging cash for chips or tokens.

Customer 53's risk profile during the relevant period

b. Customer 53 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs. Between 7 December 2016 and 8 September 2021, SCA recorded an estimated buy-in at $1,267,045, turnover estimated at $5,810,641 for Customer 53, with cumulative wins of $108,364;

Particulars

In 2016, Customer 53's recorded individual rated gambling activity at SCA was estimated as a buy-in of $76,485 for table games, and for both table games and EGMs turnover of $439,443 and losses of $9,045.

In 2017, Customer 53's recorded individual rated gambling activity at SCA was estimated as a buy-in of $43,870 for table games, and for both table games and EGMs turnover of $182,076 and losses of $25,240.

In 2018, Customer 53's recorded individual rated gambling activity at SCA significantly escalated to an estimated buy-in of $227,230 for table games, and for both table games and EGMs turnover of $1,054,787 and wins of $96,068.

In 2019, Customer 53's recorded individual rated gambling activity at SCA was estimated as a buy-in of $206,055 for table games, and for both table games and EGMs turnover of $1,315,494 and wins of $89,096.

In 2020, despite closures related to the COVID-19 pandemic, Customer 53's recorded individual rated gambling activity at SCA significantly escalated to an estimated buy-in of $532,275 for table games, and for both table games and EGMs turnover of $2,097,017 and wins of $4,629.

In 2021, Customer 53's recorded individual rated gambling activity at SCA was estimated as a buy-in of $256,375 for table games, and for both table games and EGMs, turnover of $1,155,949 and losses of $55,901.

c. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 53 by remitting large amounts of money into and out of the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

On 23 November 2018, SCA received a telegraphic transfer of $13,000 from Customer 53, which it made available to Customer 53's FMA.

On 5 March 2019, SCA accepted instructions to transfer $1,000 from Customer 53's FMA to an account outside the casino environment.

d. SCA was aware that Customer 53 had engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

Particulars

For example, Customer 53 was included in an internal report titled 'AML Unusual Changes in Betting – August' where SCA recorded Customer 53's turnover in May 2018 to August 2018.

e. designated services provided to Customer 53 included substantial EGM activity at SCA;

Particulars

See paragraphs 352 and 353 above.

In 2018, Customer 53 had an EGM turnover of $134,195.

In 2019, Customer 53's EGM turnover escalated to $277,429.

In 2020, Customer 53 had an EGM turnover of $280,156.

In 2021, Customer 53's EGM turnover escalated to $420,477.

f. Customer 53 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 28 November 2018 and 2 March 2021, SCA gave the AUSTRAC CEO 14 TTRs detailing outgoing payments made by Customer 53 totalling $192,045, which comprised:

a. 13 TTRs totalling $180,000 in chip or token cash outs; and

b. one TTR totalling $12,045 in an EGM payout.

g. in 2019, Customer 53 was the subject of a law enforcement enquiry on one occasion at SCA;

Particulars

On 12 March 2019, SCA received and responded to a request from a law enforcement agency seeking information about Customer 53.

h. Customer 53 had access to private gaming rooms at SCA; and

Particulars

See paragraph 145(e) above.

Customer 53 had access to private gaming rooms at SCA including the Black Room, the Grange Room, the Opal Room and the Platinum Room.

i. SCA did not have adequate reason to believe that Customer 53's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 53 by SCA.

Particulars

See paragraph 516 above.

From at least 24 October 2019, SCA recorded Customer 53's occupation as retired. However, SCA did not record any further information as to Customer 53's source of wealth or source of funds.

In September 2021, SCA VIP staff attempted to obtain a completed Source of Wealth Declaration and documentation from Customer 53. Customer 53 advised they were collecting some form of government welfare payment. SCA considered that Customer 53's level of gaming and access to cash appeared to be incompatible with dependence on any form of welfare payment: SMR dated 9 September 2021. SCA issued a ban in respect of Customer 53 on 8 September 2021.

From December 2016 to September 2021, Customer 53's buy-in at SCA exceeded $1,200,000.

At no time was SCA's understanding of Customer 53's source of wealth or source of funds commensurate with the high value financial and gambling services that they received at SCA.

SCA's determination of the ML/TF risks posed by Customer 53

1291. SCA was unable to identify or assess the ML/TF risks posed by Customer 53 appropriately because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 53.

a. On and from December 2018, Customer 53 should have been recognised by SCA as a high risk customer for the purpose of the Act and Rules due to their escalating gaming and for the reasons pleaded above: see *Customer 53's risk profile.*

Particulars

Sections 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

b. It was not until 11 September 2019 that Customer 53 was rated high risk by SCA for the purpose of the Act and Rules.

Monitoring of Customer 53's transactions

1292. At no time did SCA apply appropriate transaction monitoring to Customer 53's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 53 through the SCA Customer account channel, which was a high risk remittance channel.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 53's KYC information

1293. SCA did not review, update or verify Customer 53's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b)Sections 36(1)(a) and (b)

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 53, including the nature, extent and purpose of Customer 53's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 53's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 53's risk profile* above, there were higher ML/TF risks associated with Customer 53's source of wealth or source of funds.

d. to the extent that SCA reviewed Customer 53's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 53.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

Customer 53 was named in a 'Transaction Monitoring Overview' report for the period 1 August 2018 to 1 November 2018 which was provided to SCA's Senior Management Group for discussion at its meeting.

Failure to apply appropriate due diligence suited to the high ML/TF risks

1294. Had SCA conducted ongoing customer due diligence on and from 7 December 2016 by:

a. appropriately identifying and assessing the ML/TF risks posed by Customer 53;

b. applying appropriate risk-based transaction monitoring to Customer 53; and

c. appropriately reviewing and updating Customer 53's KYC information, having regard to the high ML/TF risks;

SCA would have been required by the Act and Rules to apply the ECDD Program to Customer 53 at a time before the date of the ECDD triggers pleaded below: see *ECDD triggers in respect of Customer 53*.

ECDD triggers in respect of Customer 53

1295. SCA was required to apply the ECDD program to Customer 53 following any ECDD triggers in respect of Customer 53.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

1296. Customer 53 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 13 August 2019 and 9 September 2021, SCA gave the AUSTRAC CEO two SMRs with respect to Customer 53.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 53* above.

1297. Each matter pleaded at paragraph 1296 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

1298. SCA did not conduct appropriate risk-based ECDD with respect to Customer 53 following an ECDD trigger because:

a. on each occasion prior to 8 September 2021 that SCA conducted ECDD in respect of Customer 53 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 53 and failed to appropriately consider whether the ML/TF risks posed by Customer 53 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

On 12 March 2021, SCA conducted ECDD in respect of Customer 53. The ECDD compiled information regarding Customer 53, such as

KYC information and the details reported in the SMR given to the AUSTRAC CEO on 13 August 2019.

The ECDD conducted by SCA did not have appropriate regard to Customer 53's higher ML/TF risks: see *Customer 53's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 53's source of funds or source of wealth.

By reason of the matters set out in *Customer 53's risk profile* above, there were real risks that Customer 53's source of wealth and source of funds were not legitimate.

On 8 September 2021, SCA issued a ban in respect of Customer 53.

b. at no time did senior management appropriately consider whether the ML/TF risks posed by Customer 53 in response to an ECDD trigger, or appropriately consider whether the ML/TF risks posed by Customer 53 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

It was not until 8 September 2021 that SCA issued a ban in respect of Customer 53.

Contravention of s 36 of the Act in respect of Customer 53

1299. By reason of the matters pleaded at paragraphs 1287 to 1298 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 53 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1300. By reason of the matters pleaded at paragraph 1299, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 8 September 2021 with respect to Customer 53.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 54

1301. Customer 54 was a customer of SCA during the relevant period. Between 7 December 2016 and 9 August 2021, SCA recorded turnover exceeding $5,100,000 for Customer 54.

Particulars

Customer 54 was a customer of SCA from at least 21 May 2016.

On 9 August 2021, SCA issued a ban in respect of Customer 54 at the direction of the SCA AML team.

1302. SCA provided Customer 54 with designated services within the meaning of table 3, s 6 of the Act during the relevant period.

Particulars

On 29 May 2016, SCA opened an FMA for Customer 54 which remained open as at 28 October 2022 (item 11, table 3, s 6 of the Act).

See Customer 54's risk profile below.

1303. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 54.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 54's risk profile

1304. On and from 7 December 2016, Customer 54, and the provision of designated services to Customer 54 by SCA, posed higher ML/TF risks because of the following red flags:

a. Customer 54 received high value gambling services (table 3, s 6 of the Act) at SCA other than through junket programs. Between 7 December 2016 and 9 August 2021, SCA recorded an estimated buy-in of $936,185 for table games, turnover estimated at $5,132,700 for Customer 54, with cumulative losses of $232,974;

Particulars

Between 7 December 2016 to 30 June 2017, Customer 54's recorded individual rated gambling activity at SCA was estimated as a buy-in of $27,790 for table games, a turnover of $55,027 for EGMs and for both table games and EGMs, wins of $13,332.

In the 2018 financial year, Customer 54's recorded individual rated gambling activity at SCA was estimated as a buy-in of $60,980 for table games, and for both table games and EGMs, turnover of $452,609 and losses of $25,147.

In the 2019 financial year, Customer 54's recorded individual rated gambling activity at SCA was estimated as a buy-in of $75,850 for table games, and for both table games and EGMs, turnover of $525,121 and losses of $42,275.

In the 2020 financial year, despite closures due to COVID-19, Customer 54's recorded individual rated gambling activity at SCA escalated to an estimated buy-in of $236,420 for table games, and for

both table games and EGMs, turnover of $867,759 and losses of $68,848.

In the 2021 financial year, Customer 54's recorded individual rated gambling activity at SCA further escalated to an estimated buy-in of $509,130 for table games, and for both table games and EGMs, turnover of $3,045,572 and losses of $105,689.

Between 1 July 2021 to 9 August 2021, Customer 54's recorded individual rated gambling activity at SCA was estimated as a buy-in of $26,015 for table games, and for both table games and EGMs, turnover of $186,283 and losses of $4,347.

b. designated services provided to Customer 54 included substantial EGM activity at SCA;

Particulars

See paragraphs 352 and 353 above.

Between 7 December 2016 and 5 August 2021, Customer 54 had turnover of $647,352 on EGMs, with losses of $42,854.

c. Customer 54 had engaged in unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose, including:

   i. transactions that were indicative of ML/TF typologies and vulnerabilities, including structuring; and

   ii. transactions with other customers at SCA, including players who posed higher ML/TF risks such as Customer 55 and players who SCA considered had acted suspiciously;

Particulars

See paragraph 24 above.

On 21 March 2020, Customer 54 attended SCA with Customer 55. Customer 54 retrieved $5,000 in cash from their bag and handed it to Customer 55, who used the cash to buy-in to a game. Shortly after, an unknown customer arrived at the table and spoke to Customer 54. Customer 54 and the unknown customer sat down at another gaming table together, and they were then joined at the table by Customer 55 who started playing.

Over the next few hours, Customer 54, Customer 55 and the unknown customer exchanged cash or chips on multiple occasions.

a. Customer 55 left the table briefly and the unknown customer began playing with Customer 55's chips. Customer 55 then sat back down and resumed playing with their chips.

b. Customer 54 then handed the unknown customer a $1,000 cash chip, after which the unknown customer handed Customer 54 a $1,000 chip from their pocket.

c. Several hours later, Customer 54 handed the unknown customer a $5,000 cash chip. The unknown customer immediately cashed

out the $5,000 chip. They tried to hand the cash to Customer 54, but Customer 54 did not take it and the unknown customer put the cash into their jacket pocket.

d. Ten minutes later, Customer 54 handed all the chips they had in front of them to the unknown customer. The customer immediately cashed out $8,150 in chips.

e. The unknown customer then handed an unknown amount of cash to Customer 54, which Customer 54 placed into their bag.

f. SCA staff observed that Customer 54 appeared to be the ringleader, with Customer 55 and the unknown customer both giving funds to, and receiving funds from, Customer 54 over the course of the night.

g. Based on the above transactions, SCA considered that Customer 54 and Customer 55 were working together to structure their cash out transactions to avoid the reporting threshold.

On 1 August 2020:

a. an SCA customer exchanged four $1,000 cash chips and eight $100 cash chips for $4,800 in cash, which the customer placed into their pocket. The customer met Customer 54 near the Baccarat Pavilion and handed them an unknown amount of cash from their pocket. Customer 54 then handed the customer an unknown amount of chips. The customer returned to the window and exchanged one $5,000 chip and one $1,000 chip for $6,000 in cash, which they placed in their pocket;

b. several minutes after, Customer 54 met the customer, who handed Customer 54 a valet ticket. Customer 54 presented the valet ticket to staff at the casino entrance and sat down with the customer to wait for their vehicle. While seated, the customer handed Customer 54 an unknown amount of cash, which Customer 54 placed in their bag. The pair then left the casino;

c. SCA staff observed that Customer 54 appeared to be directing the other customer to act on their behalf to avoid scrutiny over transactions below the reporting threshold. SCA noted that it was worth placing this relatively small transaction into the larger context of Customer 54's ongoing suspicious behaviours; and

d. SCA considered that Customer 54 and the other customer had engaged in conduct involving the structuring of transactions to avoid reporting thresholds. SCA noted that it had previously reported concerns about Customer 54 engaging in structuring and utilising third parties to avoid detection: SMR dated 4 August 2020.

On 12 December 2020:

a. an SCA customer, Person 22, exchanged two $25 chips and one $5 cash chip for $55 in cash. Person 22 retained the $55 cash;

b. Customer 54 then approached Person 22 and gave them five $1,000 chips. Person 22 exchanged the five chips for $5,000 in cash, which they handed to Customer 54;

c. Customer 54 then exchanged five $1,000 cash chips for $5,000 in cash, which they retained;

d. SCA was not aware of the nature of the relationship between Customer 54 and the other customer; and

e. SCA considered that the conduct demonstrated structuring of transactions by Customer 54 in order to avoid reporting requirements, as well as the use of a third party to avoid scrutiny. SCA noted that it had previously reported its suspicions about Customer 54 structuring transactions and deliberately avoiding reporting requirements. SCA stated that all parties would continue to be monitored: SMR dated 17 December 2020.

d. Customer 54 transacted using large amounts of cash at SCA; and

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 18 April 2017 and 30 December 2020, SCA gave the AUSTRAC CEO three TTRs detailing incoming and outgoing payments made by Customer 54 totalling $32,956, which comprised:

a. two TTRs totalling $20,000 in chip and cash exchanges; and

b. one TTR totalling $12,956 for an EGM payout.

e. SCA did not have adequate reason to believe that Customer 54's source of wealth or source of funds was sufficient to explain the high value gambling services (table 3, s 6 of the Act) provided to Customer 54 by SCA.

Particulars

See paragraph 516 above.

Prior to January 2020, SCA did not have any information regarding Customer 54's source of funds and source of wealth. Between December 2016 and January 2020, Customer 54 had a total buy-in of $271,870 and cumulative losses of $86,030.

On 15 January 2020, SCA recorded Customer 54's occupation as a 'Factory Worker'.

SCA continued to provide Customer 54 with designated services and took no further steps to understand Customer 54's source of funds or source of wealth until 9 August 2021. On that date, SCA requested source of wealth information and issued a ban in respect of Customer 54 until they provided that information.

Customer 54 did not provide the source of wealth information.

Between December 2016 and August 2021, when they were banned, Customer 54 had a recorded buy-in of $936,185 and turnover exceeding $5,000,000.

At no time was SCA's understanding of Customer 54's source of wealth or source of funds commensurate with the high value gambling services that they received at SCA.

SCA's determination of the ML/TF risks posed by Customer 54

1305. On and from 23 March 2020, Customer 54 was appropriately rated by SCA as a high risk customer for the purposes of the Act and Rules.

Particulars

On 23 March 2020, Customer 54 was rated high risk.

1306. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 54 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by it with respect to Customer 54.

Monitoring of Customer 54's transactions

1307. At no time did SCA apply appropriate transaction monitoring to Customer 54's transactions because SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

The review, update and verification of Customer 54's KYC information

1308. SCA did not review, update or verify Customer 54's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 54, including the nature, extent and purpose of Customer 54's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 54's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 54's risk profile* above, there were higher ML/TF risks associated with Customer 54's source of wealth or source of funds.

d. to the extent that SCA reviewed Customer 54's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 54.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

ECDD triggers in respect of Customer 54

1309. SCA was required to apply the ECDD program to Customer 54 following any ECDD triggers in respect of Customer 54.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(3) and 15.10 of the Rules.

1310. Customer 54 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 23 March 2020 and 17 December 2020, SCA gave the AUSTRAC CEO 3 SMRs with respect to Customer 54.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 54* above.

1311. Each matter pleaded at paragraph 1310 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

1312. SCA did not conduct appropriate risk-based ECDD with respect to Customer 54 following an ECDD trigger because:

a. on each occasion prior to August 2021 that SCA conducted ECDD in respect of Customer 54 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 54 and failed to appropriately consider whether the ML/TF risks posed by Customer 54 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

On 27 October 2020, SCA conducted ECDD in respect of Customer 54. No further action was taken after this ECDD.

The ECDD conducted by SCA did not have appropriate regard to Customer 54's higher ML/TF risks: see *Customer 54's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 54's source of funds or source of wealth.

By reason of the matters set out in *Customer 54's risk profile* above, there were higher ML/TF risks associated with Customer 54's source of wealth or source of funds.

It was not until 9 August 2021 that SCA issued a ban in respect of Customer 54.

b. at no time prior to 9 August 2021 did senior management consider the higher ML/TF risks posed by Customer 54 in response to an ECDD trigger, or appropriately consider whether the ML/TF risks posed by Customer 54 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

It was not until 9 August 2021 that SCA issued a ban in respect of Customer 54.

Contravention of s 36 of the Act in respect of Customer 54

1313. By reason of the matters pleaded at paragraphs 1301 to 1312 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 54 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1314. By reason of the matters pleaded at paragraph 1313, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 9 August 2021 with respect to Customer 54.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 55

1315. Customer 55 was a customer of SCA during the relevant period. Between January 2019 and June 2021, SCA recorded turnover exceeding $3,400,000 for Customer 55.

Particulars

Customer 55 was a customer of SCA from at least 16 January 2019.

On 22 March 2022, SCA issued a ban in respect of Customer 55 at the direction of the SCA AML team.

1316. SCA provided Customer 55 with designated services within the meaning of table 3, s 6 of the Act during the relevant period.

Particulars

On 16 January 2019, SCA opened an FMA for Customer 55 which was closed on 22 March 2022 (item 11, table 3, s 6 of the Act).

See *Customer 55's risk profile* below.

1317. At all times from 16 January 2019, SCA was required to conduct ongoing customer due diligence in respect of Customer 55.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 55's risk profile

1318. On and from 16 January 2019, Customer 55, and the provision of designated services to Customer 55 by SCA, posed higher ML/TF risks because of the following red flags:

a. Customer 55 received high value gambling services (table 3, s 6 of the Act) at SCA other than through junket programs. Between January 2019 and 29 June 2021, SCA recorded an estimated buy-in of $901,365, turnover estimated at $3,474,086 for Customer 55, with cumulative wins of $65,035;

Particulars

In 2019, Customer 55's recorded individual rated gambling activity was estimated as turnover of $5,750 and wins of $10,000.

In 2020, despite closures related to the COVID-19 pandemic, Customer 55's recorded individual rated gambling activity escalated significantly and was estimated as a buy-in of $463,815, turnover of $1,390,401 and losses of $25,515.

In 2021, Customer 55's recorded individual rated gambling activity was estimated as a buy-in of $437, turnover of $2,077,935 and wins of $80,550.

b. SCA was aware that Customer 55 had engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

Particulars

By January 2019, SCA was aware that Customer 55 used third parties to conduct structured cash outs to avoid the reporting threshold on multiple occasions: SMRs dated 24 January 2019, 14 February 2020, 12 March 2020, 18 March 2020 and 23 March 2020.

a. Between 19 January 2019 and 20 January 2019, Customer 55 conducted multiple chip cash outs totalling $30,500. Each chip cash out was under the reporting threshold and conducted across multiple Cage locations within SCA. Customer 55 refused to provide identification and stated that they did not need to provide identification for transactions less than $10,000. The Cashier was able to obtain Customer 55's identification details and created an uncarded account for Customer 55: SMR dated 24 January 2019.

b. On 11 February 2020, Customer 55 split chips in their possession and gave half to an unidentified customer. The customer exchanged $5,000 in chips for cash, whilst Customer 55 exchanged $7,400 in chips for cash. The customer handed the $5,000 in cash to Customer 55 before exiting the casino with them. An SCA Cashier overheard Customer 55 tell the player 'if under $9,900 then no problems': SMR dated 14 February 2020.

c. Between 7 March 2020 and 10 March 2020, SCA was aware that Customer 55 used third parties to assist with cash outs. SCA noted that Customer 55's low gambling activity did not match the cash outs conducted: SMR dated 12 March 2020.

d. On 17 March 2020, Customer 55 cashed out $9,700 in chips. Customer 55 then began playing before they were approached by a known associate. Five minutes later, Customer 55 and their associate entered the toilets. Their associate then cashed out $9,000 in chips and handed an undetermined amount of cash to Customer 55 before exiting the casino: SMR dated 18 March 2020.

e. On 21 March 2020, Customer 55 assisted their known associate, Customer 54, and an unidentified customer to

conduct multiple cash outs below the reporting threshold. The unidentified customer cashed out $8,150 in chips and handed an unknown amount of cash to Customer 54: SMR dated 23 March 2020.

SCA had no record of Customer 55 buying in for any amount during 2019, and recorded an estimated turnover of $5,750 and wins of $10,000 for Customer 55 in the same period.

c. Customer 55 was connected to other customers at SCA, including players who posed higher ML/TF risks such as Customer 54 and players who SCA considered had acted suspiciously;

Particulars

SCA recorded that Customer 55's known associates included Customer 54.

See paragraphs 1318.e below.

d. Customer 55 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 16 January 2019 and 28 June 2021, SCA gave the AUSTRAC CEO 25 TTRs detailing chip and cash exchanges made by Customer 55 totalling $388,500.

e. Customer 55 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including structuring; and

Particulars

See paragraph 24 above.

See the particulars to paragraph 1318.b above.

On the following occasions, Customer 55 was involved in transactions indicative of the ML/TF typology of structuring:

a. on 19 January 2019, Customer 55 conducted three separate chip cash outs below the reporting threshold: SMR dated 24 January 2019;

b. on 20 January 2019, Customer 55, Person 29 and their associate conducted six cash outs below the reporting threshold. Customer 55 and two associates also had four transactions refused for not complying with identification requests. Customer 55 conducted three cash outs totalling $10,300. Person 29 conducted three cash outs totalling $15,000. All chips presented by Person 29 belonged to Customer 55: SMR dated 24 January 2019;

c. on 10 March 2020, Customer 55 won $12,000 in chips and passed $5,000 of these chips to Person 29. SCA refused Person 29's request to cash out the $5,000 in chips until the customer to whom it belonged came to the Cage themselves. Customer 55 later entered the toilets and was followed by another associate. The associate subsequently emerged from the toilets and attempted to cash out $5,000 in chips but was also refused. Customer 55 later cashed out $5,000 in chips; and

d. on 17 March 2020, Customer 55 had $20,000 in chips in their possession, lost a $300 bet and cashed out $9,700 in chips. Customer 55 followed an associate into the toilets and then took a seat at a gaming table but did not play. The associate cashed out $9,000 in chips and handed the cash to Customer 55. SCA staff observed that Customer 55 had $19,000 in chips when Customer 55 cashed out. SCA noted that Customer 55 was known for avoiding the reporting threshold: SMR dated 18 March 2020.

f. SCA did not have adequate reason to believe that Customer 55's source of wealth or source of funds was sufficient to explain the high value gambling services (table 3, s 6 of the Act) provided to Customer 55 by SCA.

Particulars

See paragraph 516 above.

By January 2019, SCA recorded Customer 55's occupation as being the owner of two businesses dealing in homewares and linen.

By 2021, SCA recorded that the ABN for one of these businesses was cancelled.

From January 2019, immediately after Customer 55 became a customer of SCA, SCA identified that they were engaging in transactions that were indicative of the ML/TF typology of structuring. In 2019, SCA recorded that Customer 55's buy in was $0, despite also recording turnover and wins for Customer 55.

At no time did SCA request source of wealth or source of funds information from Customer 55.

At no time did SCA have a basis to understand whether Customer 55's source of wealth or source of funds was commensurate with their gambling activity.

At no time did SCA have a basis to understand whether Customer 55's source of wealth and source of funds was legitimate.

Between January 2019 and June 2021, SCA recorded individual rated turnover exceeding $3,400,000 for Customer 55.

SCA's determination of the ML/TF risks posed by Customer 55

1319. On and from 16 September 2019, Customer 55 was appropriately rated by SCA as a high risk customer for the purpose of the Act and Rules.

Particulars

On 16 September 2019, Customer 55 was rated high risk for the purpose of the Act and Rules.

1320. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 55 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by it with respect to Customer 55.

Monitoring of Customer 55's transactions

1321. At no time did SCA apply appropriate transaction monitoring to Customer 55's transactions because SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

The review, update and verification of Customer 55's KYC information

1322. SCA did not review, update or verify Customer 55's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 55, including the nature, extent and purpose of Customer 55's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, verify or update Customer 55's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 55's risk profile* above, there were higher ML/TF risks associated with Customer 55's source of wealth or source of funds.

From January 2019, SCA formed suspicions that Customer 55 was structuring and avoiding the transaction threshold, and recorded transactions which were not consistent with their gambling activity.

d. to the extent that SCA reviewed Customer 55's KYC information on and from 16 January 2019, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 55.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

ECDD triggers in respect of Customer 55

1323. SCA was required to apply the ECDD program to Customer 55 following any ECDD triggers in respect of Customer 55.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

1324. Customer 55 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 24 January 2019 and 18 March 2020, SCA gave the AUSTRAC CEO five SMRs with respect to Customer 55.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 55* above.

1325. Each matter pleaded at paragraph 1324 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

1326. SCA did not conduct appropriate risk-based ECDD with respect to Customer 55 following an ECDD trigger because:

a. on each occasion prior to 22 March 2022 that SCA conducted ECDD in respect of Customer 55 in response to an ECDD trigger, it failed to appropriately consider the

ML/TF risks posed by Customer 55 and failed to appropriately consider whether the ML/TF risks posed by Customer 55 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

Between 2019 and 2021, SCA reviewed open source information concerning Customer 55 and their businesses.

The ECDD conducted by SCA did not have appropriate regard to Customer 55's higher ML/TF risks: see *Customer 55's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 55's source of funds or source of wealth.

By reason of the matters set out in *Customer 55's risk profile* above, there were higher ML/TF risks associated with Customer 55's source of wealth or source of funds.

However, it was not until 22 March 2022 that SCA issued a ban in respect of Customer 55.

b. on any occasion prior to 22 March 2022 that senior management considered the higher ML/TF risks posed by Customer 55 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 55 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

It was not until 22 March 2022 that SCA issued a ban in respect of Customer 55 on the basis of their associates, and the fact that SCA had submitted five or more SMRs relating to Customer 55.

Contravention of s 36 of the Act in respect of Customer 55

1327. By reason of the matters pleaded at paragraphs 1315 to 1326 above, on and from 16 January 2019, SCA:

a. did not monitor Customer 55 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1328. By reason of the matters pleaded at paragraph 1327, SCA contravened s 36(1) of the Act on and from 16 January 2019 to 22 March 2022 with respect to Customer 55.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 56

1329. Customer 56 was a customer of SCA during the relevant period. Between 22 December 2015 and 31 October 2019, SCA recorded turnover exceeding $3,900,000 for Customer 56.

Particulars

Customer 56 was a customer of SCA from at least 22 December 2015.

On 29 March 2022, SCA issued a ban in respect of Customer 56 following investigations by the AML team, based on Customer 56's failure to disclose their occupation in 2017.

1330. SCA provided Customer 56 with designated services within the meaning of table 3, s 6 of the Act during the relevant period.

Particulars

On 22 December 2015, SCA opened an FMA for Customer 56 which was closed on 29 March 2022 (item 11, table 3, s 6 of the Act).

See *Customer 56's risk profile* below.

1331. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 56.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 56's risk profile

1332. On and from 7 December 2016, Customer 56, and the provision of designated services to Customer 56 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 56's risk profile prior to the relevant period

a. by 7 December 2016, Customer 56 had the following risk history:

   i. between 22 December 2015 and 22 March 2016, SCA recorded an escalating turnover estimated at $1,647,862 for Customer 56, with cumulative losses of $65,799; and

Particulars

In 2015, Customer 56's recorded individual rated gambling activity at SCA was estimated as a buy-in of $17,800, turnover of $152,250 and losses of $7,500.

In 2016, Customer 56's recorded individual rated gambling activity at SCA was estimated as a buy-in of $253,980, turnover of $1,495,612 and losses of $58,299.

ii. Customer 56 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

On 25 February 2016, SCA gave the AUSTRAC CEO a TTR detailing an incoming payment made by Customer 56 totalling $10,000, which comprised of an exchange of cash for chips or tokens.

Customer 56's risk profile during the relevant period

b. Customer 56 received high value gambling services (table 3, s 6 of the Act) at SCA other than through junket programs. Between 10 April 2017 and 31 October 2019, SCA recorded an estimated buy-in of $36,000, turnover estimated at $2,290,223 for Customer 56, with cumulative losses of $64,504;

Particulars

In 2017, Customer 56's recorded individual rated gambling activity at SCA was estimated as a buy-in of $402,790 for table games, and for both table games and EGMs, turnover of $1,632,809 and losses of $43,602.

In 2018, Customer 56's recorded individual rated gambling activity at SCA was estimated as a buy-in of $53,700 for table games, and for both table games and EGMs, turnover of $311,811 and losses of $26,306.

In 2019, Customer 56's recorded individual rated gambling activity at SCA was estimated as a buy-in of $45,300 for table games, and for both table games and EGMs, turnover of $345,603 and wins of $5,404.

c. designated services provided to Customer 56 included substantial EGM activity at SCA;

Particulars

See paragraphs 352 and 353 above.

In 2017, Customer 56 had an estimated turnover of $119,740 for EGMs.

d. Customer 56 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

For example, between 9 May 2017 and 26 July 2018, SCA gave the AUSTRAC CEO three TTRs detailing incoming and outgoing

payments made by Customer 56 totalling $34,725, which comprised of cash and chip exchanges.

e. Customer 56 engaged in transactions indicative of ML/TF typologies and vulnerabilities, including structuring; and

Particulars

See paragraph 24 above.

For example, on 9 August 2017, SCA gave the AUSTRAC CEO an SMR reporting that Customer 56 bought in at tables just under the threshold reporting obligation.

f. SCA did not have adequate reason to believe that Customer 56's source of wealth or source of funds was sufficient to explain the high value gambling services (table 3, s 6 of the Act) provided to Customer 56 by SCA.

Particulars

See paragraph 516 above.

SCA recorded Customer 56's occupation as unemployed. At no time did SCA obtain source of wealth or source of funds information from Customer 56.

On 9 August 2017, SCA gave the AUSTRAC CEO an SMR reporting Customer 56's failure to produce a valid identification that matched their supplied state of residence, Customer 56's refusal to supply occupation details and Customer 56's insistence that they were unemployed.

Between 10 April 2017 and 31 October 2019, SCA recorded an estimated buy-in of $36,000 for Customer 56.

At no time was SCA's understanding of Customer 56's source of wealth or source of funds commensurate with the high value financial and gambling services that they received at SCA.

SCA's determination of the ML/TF risks posed by Customer 56

1333. SCA was unable to identify or assess the ML/TF risks posed by Customer 56 appropriately because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 56.

a. On and from 9 August 2017, Customer 56 should have been recognised by SCA as a high risk customer for the purpose of the Act and Rules for the reasons pleaded above: see *Customer 56's risk profile.*

Particulars

Sections 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

b. It was not until 18 October 2017 that Customer 56 was rated by SCA as high risk for the purpose of the Act and Rules and not until 25 March 2022 that Customer 56 was rated significant risk, based on their failure to disclose their occupation in 2017.

Monitoring of Customer 56's transactions

1334. At no time did SCA apply appropriate transaction monitoring to Customer 56's transactions because SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

The review, update and verification of Customer 56's KYC information

1335. SCA did not review, update or verify Customer 56's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 56, including the nature, extent and purpose of Customer 56's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 56's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 56's risk profile* above, there were higher ML/TF risks associated with Customer 56's source of wealth or source of funds.

d. to the extent that SCA reviewed Customer 56's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 56.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

Failure to apply appropriate due diligence suited to the high ML/TF risks

1336. Had SCA conducted ongoing customer due diligence on and from 7 December 2016 by:

a. appropriately identifying and assessing the ML/TF risks posed by Customer 56;

b. applying appropriate risk-based transaction monitoring to Customer 56; and

c. appropriately reviewing and updating Customer 56's KYC information, having regard to the high ML/TF risks;

SCA would have been required by the Act and Rules to apply the ECDD Program to Customer 56 at a time before the date of the ECDD triggers pleaded below: see *ECDD triggers in respect of Customer 56*.

ECDD triggers in respect of Customer 56

1337. SCA was required to apply the ECDD program to Customer 56 following any ECDD triggers in respect of Customer 56.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(3) and 15.10 of the Rules.

1338. Customer 56 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

On 9 August 2017, SCA gave the AUSTRAC CEO an SMR with respect to Customer 56.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 56* above.

1339. Each matter pleaded at paragraph 1338 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

1340. SCA did not conduct appropriate risk-based ECDD with respect to Customer 56 following an ECDD trigger because:

a. on each occasion prior to 29 March 2022 that SCA conducted ECDD in respect of Customer 56 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 56 and failed to appropriately consider whether the ML/TF risks posed by Customer 56 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

On 9 August 2017, 19 December 2019 and 27 September 2021, SCA conducted ECDD in respect of Customer 56.

Each ECDD screening in respect of Customer 56 consisted of watchlist screening and did not return any results.

By August 2017, SCA had concerns in relation to Customer 56's source of funds and source of wealth, which were reported in an SMR given to the AUSTRAC CEO. In 2016 and 2017, Customer 56 had a high turnover that was not consistent with SCA's understanding of Customer 56's occupation, which was recorded as unemployed.

The ECDD conducted by SCA did not have appropriate regard to Customer 56's higher ML/TF risks: see *Customer 56's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 56's source of funds or source of wealth.

By reason of the matters set out in *Customer 56's risk profile* above, there were real risks that Customer 56's source of wealth and source of funds were not legitimate.

It was not until 29 March 2022 that SCA issued a ban in respect of Customer 56.

b. at no time prior to March 2022 did senior management consider the higher ML/TF risks posed by Customer 56 in response to an ECDD trigger, or appropriately consider whether the ML/TF risks posed by Customer 56 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

On 25 March 2022, SCA escalated Customer 56's risk rating to significant.

On 29 March 2022 SCA issued a ban in respect of Customer 56.

Contravention of s 36 of the Act in respect of Customer 56

1341. By reason of the matters pleaded at paragraphs 1329 to 1340 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 56 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1342. By reason of the matters pleaded at paragraph 1341, SCA contravened s 36(1) of the Act on and from 9 August 2017 to 29 March 2022 with respect to Customer 56.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 57

1343. Customer 57 was a customer of SCA during the relevant period. Between 9 June 2017 and 8 September 2021, SCA recorded turnover exceeding $3,600,000 for Customer 57.

Particulars

Customer 57 was a customer of SCA from at least 2007.

On 9 June 2012, SCA issued a temporary ban in respect of Customer 57. The ban lapsed on 9 June 2017.

On 8 September 2021, SCA issued another ban in respect of Customer 57.

1344. SCA provided Customer 57 with designated services within the meaning of table 1 and table 3, s 6 of the Act during the relevant period.

Particulars

Prior to 7 December 2016, SCA opened an FMA for Customer 57 which remained open as at 28 October 2022 (item 11, table 3, s 6 of the Act).

While a customer of SCA, Customer 57 remitted funds to their FMA (items 31 and 32, table 1, s 6 of the Act).

See *Customer 57's risk profile* below.

1345. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 57.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 57's risk profile

1346. On and from 7 December 2016, Customer 57, and the provision of designated services to Customer 57 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 57's risk profile prior to the relevant period

a. by 7 December 2016, Customer 57 had the following risk history:

   i. Customer 57 had received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs;

Particulars

Between 2007 and 9 June 2012, Customer 57's recorded individual rated gambling activity at SCA was estimated as a buy-in of $20,550 for table games, and for both table games and EGMs, turnover of $151,698 and losses of $17,253.

ii. designated services provided to Customer 57 included EGM activity at SCA; and

Particulars

See paragraphs 352 and 353 above.

Across 2011 and 2012, Customer 57 had a turnover of $39,154 on EGMs and losses of $6,523.

iii. in 2012, Customer 57 was arrested at SCA by a law enforcement agency for dealing drugs and was banned from SCA;

Particulars

On 9 June 2012, SCA reported Customer 57 to a law enforcement agency after they were captured on CCTV with another associate selling illicit substances on SCA premises. The law enforcement agency attended SCA and arrested Customer 57 after finding them to be in possession of a large amount of money. Customer 57 was then charged with drug dealing. Following this incident, SCA issued a ban in respect of Customer 57.

On 26 April 2014, SCA staff observed Customer 57 on the premises. Customer 57 advised SCA that they thought their ban had expired.

On 8 March 2016, SCA staff observed that Customer 57 was gaming on an EGM despite being banned from the premises. SCA informed a law enforcement agency, who attended and escorted Customer 57 off the premises.

The 2012 ban lapsed on 9 June 2017.

Customer 57's risk profile during the relevant period

b. Customer 57 received high value financial and gambling services (tables 1 and 3, s 6 of the Act) at SCA other than through junket programs. Between 2017 and 2021, SCA recorded an estimated buy-in of $460,690, turnover estimated at $3,699,102 for Customer 57, with cumulative losses of $205,870;

Particulars

In 2017, Customer 57's recorded individual rated gambling activity at SCA was estimated as a buy-in of $27,150 for table games, and for both table games and EGMs, turnover of $154,657 and losses of $8,971.

In 2018, Customer 57's recorded individual rated gambling activity at SCA was estimated as a buy-in of $2,700 for table games, and for both table games and EGMs, turnover of $257,484 and losses of $25,613.

In 2019, Customer 57's recorded individual rated gambling activity at SCA significantly escalated to an estimated buy-in of $272,890 for table games, and for both table games and EGMs, turnover of $2,025,930 and losses of $114,791.

Between 17 August 2019 and 15 May 2021, SCA did not record any individual rated gambling activity for Customer 57.

From 15 May 2021 to December 2021, Customer 57's recorded individual rated gambling activity at SCA was estimated as a buy-in of $157,950 for table games, and for both table games and EGMs, turnover of $1,261,031 and losses of $56,495.

On 26 June 2021, Customer 57 was recorded as a significant table and EGM player due to their gambling activity around that date.

c. SCA provided designated services (items 31 and 32, table 1, s 6 of the Act) to Customer 57 by remitting large amounts of money into the casino environment via their accounts, including through high risk remittance channels;

Particulars

See paragraphs 232 to 312 above.

Remittances through the SCA customer account channel

SCA made money available to Customer 57 in the following transactions.

a. Between 16 June 2019 and 19 July 2019, SCA received ten telegraphic transfers totalling $98,500 from an unknown account, each of which was made available to Customer 57's FMA.

b. Between 5 August 2019 and 30 December 2019, SCA received three telegraphic transfers totalling $3,000 from Customer 57's personal bank account in Australia, each of which was made available to Customer 57's FMA.

d. SCA was aware that Customer 57 and their associates had engaged in large and unusual transactions and patterns of transactions, which had no apparent economic or visible lawful purpose;

Particulars

On 26 June 2021, Customer 57 gave $10,000 in cash to another SCA customer in the Grange Room. The other customer attended the Grange Cage window and sought to exchange the cash for chips. While the transaction was being processed, Customer 57 came up to the counter. Customer 57 spoke with the Cashier and stated that the cash was theirs and they had asked the other customer to purchase the chips for them. Customer 57 then took the $10,000 in cash chips. Both Customer 57 and the other customer left the room, and Customer 57 recommenced gaming in another room. SCA noted that

Customer 57 appeared to have used the other customer as a runner for the transaction while Customer 57 continued to game.

On 22 July 2019, SCA authorised an early release of $50,000. SCA identified that Customer 57 conducted the following transactions using the funds:

a. on 22 July 2019, Customer 57 received a $5,000 TITO from an EGM. Customer 57 gave this TITO to another SCA customer, who then cashed it out and retained the funds. SCA noted that it could not determine why Customer 57 gave the TITO to the other customer;

b. later in the evening of 22 July 2019, Customer 57 received two further TITOs for $5,000 each at EGMs. Customer 57 gave the TITOs to a Gaming Machines Host, and the two TITOs were processed as separate transactions. SCA noted that it could not determine why the transactions were split up by the host;

c. on 23 July 2019, Customer 57 made six withdrawals of $2,000 each in cash from their FMA. SCA considered that Customer 57 may have conducted these eCash transactions, rather than finding a Cashier, for convenience, as they were meeting their partner in the Black Room where there was no Cashier present; and

d. between 22 July 2019 and 23 July 2019, Customer 57 received a total of $35,902 in cash from TITO redemptions. Customer 57 placed all of the cash either into their bag or into their pocket.

e. designated services provided to Customer 57 included substantial EGM activity at SCA;

Particulars

See paragraphs 352 and 353 above.

See particulars to paragraph 1346.f below.

Between 2017 and 2021, Customer 57 had a turnover of $1,118,913 on EGMs and losses of $45,854.

On 26 June 2021, SCA considered Customer 57 to be a significant EGM player based on their play around that date.

f. Customer 57 transacted using large amounts of cash and cash that appeared suspicious at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 25 June 2019 and 30 June 2021, SCA gave the AUSTRAC CEO 22 TTRS detailing incoming and outgoing payments made by Customer 57 totalling $376,163, which comprised:

a. eight TTRs totalling $102,105 in chip and cash exchanges;

b. nine TTRs totalling $189,000 in account deposits;

c. one TTR totalling $14,410 for an account withdrawal; and

d. four TTRs totalling $70,739 in EGM payouts.

Large and suspicious cash transactions

For example, on or around 29 June 2021, Customer 57 received a $50,000 TITO redemption at SCA following an EGM win. Customer 57 cashed out $40,000, and deposited the remaining $10,000 into their FMA.

g. Customer 57 engaged in other transactions indicative of ML/TF typologies and vulnerabilities, including structuring;

Particulars

See paragraph 24 above.

See particulars to paragraph 1346.d above.

For example, Customer 57 was involved in transactions indicative of the ML/TF typology of structuring on the following occasions:

a. on 22 July 2019, SCA recorded that Customer 57 was structuring transactions with another SCA customer to avoid the reporting threshold;

b. on 23 July 2019, Customer 57 made six cash withdrawals from their FMA totalling $12,000.

h. in 2019, Customer 57 was the subject of law enforcement interest on at least one occasion;

Particulars

See particulars to paragraph 778.c above.

i. between May 2019 and August 2019, SCA staff observed that Customer 57's gambling activity increased significantly;

Particulars

From May 2019 to 7 August 2019, Customer 57 had presented approximately $168,000 for buy-in and recorded losses of approximately $104,000. The majority of these losses occurred in July 2019. These figures represented a significant increase in Customer 57's gambling activity. This was of concern to SCA due to the limited information it had about Customer 57's source of funds: SMR dated 7 August 2019.

j. Customer 57 had access to private gaming rooms at SCA;

Particulars

See paragraph 145(e) above.

Customer 57 had access to private gaming rooms at SCA, including the Black Room, the Grange Room, the Opal Room and the Platinum Room.

k. from 2019, Customer 57 had an outstanding debt of $50,000 owed to SCA; and

Particulars

On 22 July 2019, Customer 57 transferred $50,000 from their personal bank account in Australia to their SCA FMA. The SCA General Manager authorised an early release of the funds to Customer 57. Customer 57 subsequently withdrew the funds over a 48-hour period.

By 24 July 2019, Customer 57's deposit had not appeared in SCA's account. SCA commenced a review to determine where the money was. On 1 August 2019, Customer 57 informed SCA staff that they had been approached by a law enforcement agency about their recent bank transactions and potential associates. Customer 57 advised SCA that their bank accounts had been frozen by the law enforcement agency pending an investigation: SMR dated 7 August 2019.

On 2 August 2019, SCA conducted a review of Customer 57's transactions on 22 July 2019 and 23 July 2019. The review concluded that it appeared that Customer 57 departed SCA on 23 July 2019 with $31,202 in cash withdrawn from their FMA.

In December 2020, SCA informed Customer 57 that they still had an outstanding debt of $47,000 owed to SCA.

By 12 June 2021, Customer 57 had only paid off $6,000 of the debt.

On 21 June 2021, Customer 57 paid off the remaining amount of their debt in cash to SCA. SCA believed that Customer 57 had spent two years saving to pay back this debt. SCA noted that Customer 57 would be monitored for future large cash transactions, and SCA would not release funds early to Customer 57.

l. SCA did not have adequate reason to believe that Customer 57's source of wealth or source of funds was sufficient to explain the high value financial and gambling services (tables 1 and 3, s 6 of the Act) provided to Customer 57 by SCA.

Particulars

See paragraph 516 above.

At all times, SCA was aware that Customer 57 had been arrested on SCA's premises in 2012 and charged with dealing drugs.

Between July 2019 and June 2021, Customer 57 had a debt owing to SCA in the amount of $47,000. Customer 57 cleared the debt, Customer 57 repaid at least $41,000 of the debt in cash on 21 June 2021.

On 7 August 2019, Customer 57 informed SCA that their occupation was a senior marketing manager. However, open source searches conducted by SCA failed to verify this information: SMR dated 7 August 2019.

In 2021, SCA became aware that the ABN for the business that Customer 57 claimed they worked for had been cancelled since 13 January 2020.

On 29 June 2021, Customer 57 provided SCA with the following details regarding their occupation:

a. Customer 57 stated they were a 'FIFO' worker who worked as a subcontractor for open cut mines;

b. however, Customer 57 stated that their main source of income was from trading in gold bullion. They said they had been running their gold bullion trading business for about seven years;

c. Customer 57 informed SCA that their annual business turnover was approximately $5,000,000, with profits of approximately $700,000;

d. Customer 57 also noted that they had received an inheritance three years earlier; and

e. Customer 57 stated that they also made money buying cars at auctions, doing them up and then selling them.

Customer 57 did not provide any evidence to support their purported source of wealth.

On 30 June 2021, SCA asked Customer 57 to complete a Source of Wealth Declaration. SCA advised Customer 57 that they could not attend the casino until the completed form and any supporting documentation had been provided and assessed by SCA. Customer 57 did not complete the form.

On 8 September 2021, following Customer 57's refusal to provide their source of wealth information, SCA issued a ban in respect of Customer 57.

From at least 2019, SCA's understanding of Customer 52's source of wealth or source of funds was not commensurate with the high value gambling services that they received at SCA.

At no time did SCA take appropriate steps to determine whether Customer 52's source of wealth or source of funds was legitimate, in circumstances where SCA had previously detected Customer 52

dealing drugs on SCA's premises and reported them to law enforcement.

SCA's determination of the ML/TF risks posed by Customer 57

1347. SCA was unable to identify or assess the ML/TF risks posed by Customer 57 appropriately because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 57.

a. On and from 7 December 2016, Customer 57 should have been recognised by SCA as a high risk customer for the purpose of the Act and Rules for the reasons pleaded above: see *Customer 57's risk profile.*

Particulars

Sections 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

b. It was not until 7 August 2019 that Customer 57 was rated high risk for the purpose of the Act and Rules by SCA.

Monitoring of Customer 57's transactions

1348. At no time did SCA apply appropriate transaction monitoring to Customer 57's transactions because:

a. SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities; and

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

b. SCA did not apply appropriate risk-based transaction monitoring to designated services provided to Customer 57 through the SCA Customer account channel, which was a high risk remittance channel.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 477 to 487 above.

The review, update and verification of Customer 57's KYC information

1349. SCA did not review, update or verify Customer 57's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 57, including the nature, extent and purpose of Customer 57's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 57's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 57's risk profile* above, there were real risks that Customer 57's source of wealth and source of funds were not legitimate.

In August 2019, Customer 57's turnover was high and escalated significantly. SCA was unable to verify Customer 57's source of wealth information, suggesting that there were real ML/TF risks as to Customer 57's source of funds (see paragraph 1346.l). In 2021, SCA became aware that the ABN for the business that Customer 57 said that they worked for had been cancelled since 13 January 2020.

d. to the extent that SCA reviewed Customer 57's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 57.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

On 3 December 2018 and 24 July 2019, SCA conducted due diligence in respect of Customer 57, but did not have appropriate regard to their higher ML/TF risks: see *Customer 57's risk profile* above.

On 2 August 2019, surveillance staff conducted a review of Customer 57's transactions at SCA between 22 July 2019 and 23 July 2019 and an SCA AML Analyst (Advisor) was advised of the findings: see particulars to paragraph 778.c above.

It was not until 8 September 2021 that SCA issued a ban in respect of Customer 57.

Failure to apply appropriate due diligence suited to the high ML/TF risks

1350. Had SCA conducted ongoing customer due diligence on and from 7 December 2016 by:

a. appropriately identifying and assessing the ML/TF risks posed by Customer 57;

b. applying appropriate risk-based transaction monitoring to Customer 57; and

c. appropriately reviewing and updating Customer 57's KYC information, having regard to the high ML/TF risks;

SCA would have been required by the Act and Rules to apply the ECDD Program to Customer 57 at a time before the date of the ECDD triggers pleaded below: see *ECDD triggers in respect of Customer 57*.

ECDD triggers in respect of Customer 57

1351. SCA was required to apply the ECDD program to Customer 57 following any ECDD triggers in respect of Customer 57.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1), 15.9(3) and 15.10 of the Rules.

1352. Customer 57 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

On 7 August 2019, SCA gave the AUSTRAC CEO an SMR with respect to Customer 57.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 57* above.

1353. Each matter pleaded at paragraph 1352 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

1354. SCA did not conduct appropriate risk-based ECDD with respect to Customer 57 following an ECDD trigger because:

a. on each occasion prior to 8 September 2021 that SCA conducted ECDD in respect of Customer 57 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 57 and failed to appropriately consider whether the ML/TF risks posed by Customer 57 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

On 23 June 2021, 28 June 2021, 30 June 2021 and 8 August 2021, SCA conducted ECDD in respect of Customer 57.

On 23 June 2021, ECDD screening in respect of Customer 57 identified that:

a. SCA had previously questioned the legitimacy of the funds presented by Customer 57;

b. in 2012, Customer 57 was reported to a law enforcement agency after they were captured on CCTV selling illicit substances on SCA premises. SCA banned Customer 57 from the premises following this event;

c. Customer 57's gambling activity at SCA had significantly increased in May 2019;

d. Customer 57 had been shown to be an untrustworthy patron due to a fraudulent EFT receipt presented on 22 July 2019 in support of their request for an early release of funds; and

e. SCA had conducted further investigations the businesses Customer 57's claimed to own and operate, which revealed that their ABN's had been cancelled since 2 January 2020. Further, the ABN for the business Customer 57 claimed they were employed by had been cancelled since 31 December 2017.

On 28 June 2021, an SCA AML Analyst requested a review of a transaction conducted by Customer 57 on 26 June 2021: see particulars to paragraph 1346.d above. On 29 June 2021, a review was conducted by surveillance staff and an SCA AML Analyst was advised of the findings.

On 30 June 2021, SCA asked Customer 57 to complete a Source of Wealth Declaration and provide supporting documentation.

On 1 July 2021, screening in respect of Customer 57 for the period 1 May 2021 to 1 July 2021 identified that on or around 29 June 2021, Customer 57 received a $50,000 TITO redemption at SCA following an EGM win. Customer 57 cashed out $40,000, and deposited the remaining $10,000 into their FMA.

On 8 September 2021, SCA conducted a review of its customer relationships and determined that it should discontinue its relationship with Customer 57.

The ECDD conducted by SCA did not have appropriate regard to Customer 57's higher ML/TF risks: see *Customer 57's risk profile* above.

The ECDD conducted by SCA did not have appropriate regarding to the higher ML/TF risks posed by Customer 57's source of funds or source of wealth.

By reason of the matters set out in *Customer 57's risk profile* above, there were real risks that Customer 57's source of wealth and source of funds were not legitimate.

On 8 September 2021, SCA issued a ban in respect of Customer 57.

b. on any occasion prior to 8 September 2021 that senior management considered the higher ML/TF risks posed by Customer 57 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 57 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

On 22 July 2019, the SCA General Manager approved the early release of $50,000 for Customer 57, after Customer 57 provided a receipt of the transfer. In doing so, the SCA General Manager did not have appropriate regard to Customer 57's higher ML/TF risks: see *Customer 57's risk profile* above.

It was not until 8 September 2021 that SCA issued a ban in respect of Customer 57.

Contravention of s 36 of the Act in respect of Customer 57

1355. By reason of the matters pleaded at paragraphs 1343 to 1354 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 57 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1356. By reason of the matters pleaded at paragraph 1355, SCA contravened s 36(1) of the Act on and from 9 June 2017 to 8 September 2021 with respect to Customer 57.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 58

1357. Customer 58 was a customer of SCA during the relevant period. Between 10 April 2017 and 16 June 2021, SCA recorded turnover exceeding $1,900,000 for Customer 58.

Particulars

Customer 58 was a customer of SCA from at least 10 April 2017.

On 16 June 2021, SCA issued a ban in respect of Customer 58 at the direction of the SCA AML team.

1358. SCA provided Customer 58 with designated services within the meaning of table 3, s 6 of the Act during the relevant period.

Particulars

On 10 April 2017, SCA opened an FMA for Customer 58 which remained open as at 28 October 2022 (item 11, table 3, s 6 of the Act).

See *Customer 58's risk profile* below.

1359. At all times from 10 April 2017, SCA was required to conduct ongoing customer due diligence in respect of Customer 58.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 58's risk profile

1360. On and from 10 April 2017, Customer 58 and the provision of designated services to Customer 58 by SCA, posed higher ML/TF risks because of the following red flags:

a. Customer 58 received high value gambling services (table 3, s 6 of the Act) at SCA other than through junket programs. Between April 2017 and June 2021, SCA recorded an estimated buy-in of $712,800, turnover estimated at $1,969,095 for Customer 58, with cumulative losses of $26,231;

Particulars

In 2017, Customer 58's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $18,800, turnover of $42,771 and losses of $3,700.

From February 2018 to May 2018, Customer 58's recorded individual rated gambling activity at SCA for table games escalated to an estimated buy-in of $42,100, turnover of $73,629 and losses of $14,800.

SCA did not record any gambling activity for Customer 58 from June 2018 to March 2019.

From April 2019 to December 2019, Customer 58's recorded individual rated gambling activity at SCA for table games further escalated to an estimated buy-in of $227,900, turnover of $560,356 and losses of $13,000.

From January 2020 to March 2020, Customer 58's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $6,600, and for both table games and EGMs, turnover of $44,414 and losses of $5,531. SCA did not record any gambling activity for Customer 58 between April 2020 and March 2021.

From April 2021 to June 2021, Customer 58's recorded individual rated gambling activity at SCA escalated to an estimated buy-in of

$417,400 for table games, turnover of $1,247,925 and wins of $10,800.

b. Customer 58 engaged in transactions indicative of ML/TF typologies and vulnerabilities, including structuring;

Particulars

Between 9 April 2021 and 10 April 2021, SCA reported that Customer 58 attempted to structure transactions to avoid the threshold reporting requirements by passing an unknown amount of chips to another SCA customer playing at the same table as them in the Baccarat Pavilion.

Customer 58 subsequently presented $7,000 in cash chips for cash out, and the other SCA customer presented $9,000 in cash chips for cash out at the next Cage. When questioned, Customer 58 advised that the chips were all theirs.

The Cage staff combined the chips presented by Customer 58 and the other customer and recorded a cash out for cash chips of $16,000 in Customer 58's account. Customer 58 retained the $16,000 cash.

c. Customer 58 was connected to other customers at SCA including players who posed higher ML/TF risks and players who SCA considered had acted suspiciously;

Particulars

For example, on 21 May 2021, SCA reported that Customer 58 provided another customer with $5,000 in cash to buy-in for chips at the Cashier. The relationship between Customer 58 and the customer was not known. The customer retained the funds. SCA was aware that the customer was convicted of an offence related to dealing with proceeds of crime in January 2019.

d. Customer 58 transacted using large amounts of cash at SCA; and

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 11 April 2017 and 16 June 2021, SCA gave the AUSTRAC CEO 19 TTRs detailing chip and cash exchanges by Customer 58 totalling $253,217, which comprised:

a. six incoming transactions involving the issuance of chips or tokens totalling $62,000; and

b. 13 outgoing transactions involving cashing out chips or tokens totalling $191,217.

Large cash transactions

On 7 June 2021, Customer 58 made four separate threshold transactions, totalling $57,000. SCA also recorded that Customer 58

had a cumulative cash buy-in of approximately $31,900 on the same day.

e. SCA did not have adequate reason to believe that Customer 58's source of wealth or source of funds was sufficient to explain the high value gambling services (table 3, s 6 of the Act) provided to Customer 58 by SCA.

Particulars

See paragraph 516 above.

SCA recorded Customer 58's occupation as 'Unemployed' until April 2017.

On 15 April 2017, SCA updated Customer 58's occupation to 'Travel/Unemployed' based on information received from a frontline staff member at SCA. SCA noted that the residential address provided by Customer 58 was the location of a hotel and a restaurant. When SCA spoke with Customer 58 regarding their address, Customer 58 said they were not sure of their address and would have to check.

By October 2019, Customer 58's gambling activity had escalated significantly and remained inconsistent with SCA's understanding of Customer 58's source of wealth and their occupation.

On 10 June 2021, Customer 58 completed a Source of Wealth Declaration at SCA's request:

a. Customer 58 first listed their occupation as 'Unemployed' but it was crossed out to state 'Home Duties';

b. Customer 58 stated they had outright ownership of an apartment in central Adelaide, valued at $400,000. The property did not have tenants; and

c. Customer 58 stated their source of wealth was 'Funds from savings account' overseas.

On 11 June 2021, SCA requested that Customer 58 complete a Source of Wealth Declaration. SCA reviewed the residential address provided by Customer 58 in the Source of Wealth Declaration using open source checks and noted that the address appeared to be a commercial building.

On 11 June 2021, Customer 58 told an SCA staff member that:

a. Customer 58 had not worked for 30 years and had been supported by their spouse before they divorced; and

b. Customer 58 did not want to provide details of their overseas bank account, or their overseas address details because they were concerned that SCA would investigate a person who sent money to their overseas bank account, and that

investigation would affect the person due to their political background.

On 19 July 2021, after SCA issued a ban with respect to Customer 58, Customer 58 provided SCA with a photo of two letters from their Australian bank, showing funds of $70,000 and $100,000 being credited from an overseas bank on 4 June 2021 and 23 June 2021 respectively. On the same day, SCA concluded that the documents did not contribute anything meaningful to a source of wealth assessment.

At no time was SCA's understanding of Customer 58's source of wealth or source of funds commensurate with the high value financial and gambling services that they received at SCA.

SCA's determination of the ML/TF risks posed by Customer 58

1361. SCA was unable to identify or assess the ML/TF risks posed by Customer 58 appropriately because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by SCA with respect to Customer 58.

a. From October 2019, Customer 58 should have been recognised by SCA as a high risk customer for the purpose of the Act and Rules for the reasons pleaded above: see *Customer 58's risk profile.*

Particulars

Sections 36(1)(a) and (b) of the Act and Chapter 15 of the Rules.

On 15 June 2021, SCA escalated Customer 58's risk rating to significant, which was high risk for the purpose of the Act and Rules.

b. It was not until 20 April 2021 that Customer 58 was rated high risk for the purpose of the Act and Rules by SCA.

Monitoring of Customer 58's transactions

1362. At no time did SCA apply appropriate transaction monitoring to Customer 58's transactions because SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

The review, update and verification of Customer 58's KYC information

1363. SCA did not review, update or verify Customer 58's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 58, including the nature, extent and purpose of Customer 58's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 58's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 58's risk profile* above, there were real risks that Customer 58's source of wealth and source of funds were not legitimate.

d. to the extent that SCA reviewed Customer 58's KYC information on and from 10 April 2017, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 58.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

ECDD triggers in respect of Customer 58

1364. SCA was required to apply the ECDD program to Customer 58 following any ECDD triggers in respect of Customer 58.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(3) and 15.10 of the Rules.

1365. Customer 58 was:

a. the subject of suspicions formed by SCA for the purposes of s 41 of the Act during the relevant period; and

Particulars

Between 19 April 2021 and 16 June 2021, SCA gave the AUSTRAC CEO two SMRs with respect to Customer 58.

b. determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 58* above.

1366. Each matter pleaded at paragraph 1365 was an ECDD trigger.

Particulars

See paragraphs 496, 504 and 506 above.

1367. SCA did not conduct appropriate risk-based ECDD with respect to Customer 58 following the ECDD triggers:

a. on each occasion prior to 16 June 2021 that SCA conducted ECDD in respect of Customer 58 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 58 and failed to appropriately consider whether the ML/TF risks posed by Customer 58 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

In May 2021, SCA conducted ECDD in respect of Customer 58 following an SMR reporting Customer 58's involvement in structuring given by SCA to the AUSTRAC CEO.

On 7 June 2021, when Customer 58 requested a cash out of $20,000 in chips, Customer 58 was not able to confirm the street number of their residential address after multiple guesses. Customer 58 stated that they moved apartments regularly as they were short stay apartments in the same complex. On 8 June 2021, SCA noted that Customer 58's recent turnover indicated an increased ML/TF risk.

The ECDD conducted by SCA did not have appropriate regard to Customer 58's higher ML/TF risks: see *Customer 58's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 58's source of funds or source of wealth.

By reason of the matters set out in *Customer 58's risk profile* above, there were real risks that Customer 58's source of wealth and source of funds were not legitimate

However, it was not until 16 June 2021 that SCA issued a ban in respect of Customer 58.

b. on any occasion prior to 16 June 2021 that senior management considered the higher ML/TF risks posed by Customer 58 in response to an ECDD trigger, senior management failed to appropriately consider whether the ML/TF risks posed by Customer 58 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

On 1 May 2019, Customer 58 was included in SCA's ''Transaction Monitoring Overview'' dated 1 May 2019, for the period 1 February 2019 to 1 May 2019. The report observed that Customer 58 had unusual changes in betting habits. SCA recorded that it would continue to monitor Customer 58.

In a 'Transaction Monitoring Overview' report dated 1 August 2019, relating to the period 1 May 2019 to 1 August 2019, SCA noted that Customer 58 had not attended SCA since April 2019. The concern raised in the report dated 1 May 2019 was recorded as resolved. These reports were provided to the AML/CTF Senior Management Group for consideration at its meeting.

On 15 June 2021, after elevating Customer 58's risk rating to significant, an SCA AML Compliance Analyst emailed the SCA Chief Operating Officer to determine whether SCA should continue a business relationship with Customer 58.

On 15 June 2021, the SCA Chief Operating Officer determined that SCA should discontinue its business relationship with Customer 58 until such a time that SCA is satisfied that their source of wealth is legitimate and commensurate with their gambling activity.

It was not until 16 June 2021 that SCA issued a ban in respect of Customer 58.

Contravention of s 36 of the Act in respect of Customer 58

1368. By reason of the matters pleaded at paragraphs 1357 to 1367 above, on and from 10 April 2017, SCA:

a. did not monitor Customer 58 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1369. By reason of the matters pleaded at paragraph 1368, SCA contravened s 36(1) of the Act on and from 10 April 2017 to 16 June 2021 with respect to Customer 58.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customer 59

1370. Customer 59 was a customer of SCA during the relevant period. Between 7 December 2016 and 27 July 2018, SCA recorded turnover exceeding $220,000 for Customer 59.

Particulars

Customer 59 was a customer of SCA from at least 10 February 2011.

On 22 October 2021, SCA issued a ban in respect of Customer 59 at the direction of the SCA AML team.

1371. SCA provided Customer 59 with designated services within the meaning of table 3, s 6 of the Act during the relevant period.

Particulars

On 10 February 2011, SCA opened an FMA for Customer 59 which remained open as at 28 October 2022 (item 11, table 3, s 6 of the Act).

See *Customer 59's risk profile* below.

1372. At all times from 7 December 2016, SCA was required to conduct ongoing customer due diligence in respect of Customer 59.

Particulars

Section 36(1) of the Act and rr 9.1.3, 9.1.4 and 15.2 to 15.11 of the Rules.

Customer 59's risk profile

1373. On and from 7 December 2016, Customer 59, and the provision of designated services to Customer 59 by SCA, posed higher ML/TF risks because of the following red flags:

Customer 59's risk profile prior to the relevant period

a. by 7 December 2016, Customer 59 had the following risk history:

   i. SCA had formed suspicions for the purposes of s 41 of the Act with respect to Customer 59;

Particulars

SCA gave the AUSTRAC CEO an SMR on 21 January 2014.

The SMR reported that Customer 59 tried to buy-in with $10,000 in cash without a valid identification document. Customer 59 then bought in using small amounts on the gaming floor and was eventually instructed that no further buy-ins were allowed until they presented a valid identification document.

   ii. From 10 February 2011 to 7 December 2016, Customer 59 had a high turnover estimated at $2,034,746, with cumulative losses of $35,100; and

Particulars

In 2011, Customer 59's recorded individual rated gambling activity at SCA was estimated as a buy-in of $172,450, turnover of $557,817 and losses of $20,650.

In 2012, Customer 59's recorded individual rated gambling activity at SCA was estimated as a buy-in of $163,600 for table games, and for

both table games and EGMs, turnover of $807,845 and wins of $8,100.

In 2013, Customer 59's recorded individual rated gambling activity at SCA was estimated as a buy-in of $72,750, turnover of $278,187 and losses of $5,550.

In 2014, Customer 59's recorded individual rated gambling activity at SCA was estimated as a buy-in of $56,300 for table games, and for both table games and EGMs, turnover of $156,421 and losses of $7,254.

In 2015, Customer 59's recorded individual rated gambling activity at SCA was estimated as a buy-in of $50,800, turnover of $245,450 and losses of $10,600.

iii. Customer 59 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 17 December 2011 and 8 November 2012, SCA gave the AUSTRAC CEO 11 TTRs detailing chip and cash exchanges made by Customer 59 totalling $173,600, which comprised:

a. three incoming transactions involving the issuance of chips or tokens totalling $31,000; and

b. eight outgoing transactions involving cashing out chips or tokens totalling $142,600.

Customer 59's risk profile during the relevant period

b. Customer 59 received high value gambling services (table 3, s 6 of the Act) at SCA other than through junket programs. Between 7 December 2016 and 27 July 2018, SCA recorded an estimated buy-in of $23,750, turnover for two single days of play estimated at $221,027 for Customer 59, with cumulative losses of $62,250;

Particulars

In 2017, Customer 59's recorded individual rated gambling activity at SCA was estimated as a buy-in of $56,800, turnover of $22,802 and losses of $43,000, which related to a single day of play.

In 2018, Customer 59's recorded individual rated gambling activity at SCA for table games was estimated as a buy-in of $23,750, turnover of $198,225 and losses of $19,250, which related to a single day of play.

c. Customer 59 transacted using large amounts of cash at SCA;

Particulars

See paragraphs 376 to 381 above.

TTRs

Between 22 February 2017 and 27 July 2018, SCA gave the AUSTRAC CEO two TTRs detailing chip and cash exchanges made by Customer 59 totalling $40,000.

d. Customer 59 had access to a private gaming room at SCA;

Particulars

See paragraph 145(e) above.

Customer 59 had access to the Grange Room.

e. SCA was aware that Customer 59 had engaged in unusual transactions, which had no apparent economic or visible lawful purpose;

Particulars

Customer 59 was included in an internal report titled 'AML Unusual Changes in Betting – February' where SCA recorded that for February 2017, Customer 59 had losses of $43,000 for the month.

f. by November 2019, SCA was aware of media articles which reported that Customer 59 was the director of a company suspected of tax evasion;

Particulars

Media articles published in March 2014 named Customer 59 as the director of a company which was alleged to be encouraging its workers not to pay taxes. It was not until November 2019 that SCA became aware of these reports.

Media articles published in July 2021 and August 2021 named Customer 59 as being suspected of suspicious transactions at other Australian casinos involving large amounts of cash.

Media articles published in October 2021 named Customer 59 as being suspected of money laundering at another Australian casino.

g. between 2018 and 2021, publicly available information named Customer 59 as a person who had withdrawn nearly $2,000,000 from ATMs at another Australian casino and who was involved in, among other things, money laundering; and

Particulars

By 2018, publicly available information identified that Customer 59 was:

a. ordered by an Australian regulator to pay a penalty of $43,000 in relation to sham contracting, underpayment of employees and records and payslip contraventions in the course of their role as general manager of a company; and

b. subject to a freezing order from an Australian court related to a government assessment that there had been significant tax shortfalls for Customer 59 through fraud and/or tax evasion.

In 2019, publicly accessible media articles reported that:

a. Customer 59 owed a debt of $121,000,000 in respect of eight companies operated by Customer 59;

b. Customer 59 had consented to pay $42,000,000 in personal taxes and fines to an Australian government agency;

c. Customer 59 engaged in 'phoenixing' behaviour in respect of labour hire companies;

d. Customer 59 was alleged to have gambled significant amounts sums at Australian casinos and had withdrawn nearly $2,000,000 from ATMs there over five years; and

e. Customer 59 sent $43,000,000 overseas.

In 2021, publicly accessible media articles reported that:

a. in 2018, a law enforcement agency executed search warrants in respect of several properties owned by Customer 59 in connection with a recruitment and labour hire syndicate Customer 59 operated;

b. Customer 59 was suspected of several criminal offences including money laundering, tax fraud, secret commissions and breaches of migration law; and

c. Customer 59 unsuccessfully resisted requests by an Australian government agency to establish their wealth on the grounds that the documents would tend to incriminate them.

There are no records of these articles in SCA's due diligence records for Customer 59.

h. SCA did not have adequate reason to believe that Customer 59's source of wealth or source of funds was sufficient to explain the high value gambling services (table 3, s 6 of the Act) provided to Customer 59 by SCA.

Particulars

See paragraph 516 above.

From February 2017, SCA listed Customer 59's occupation as 'Property Developer'. Prior to that date this the field only had a generic descriptor of 'Manager'.

At no time did SCA request source of funds or source of wealth information on Customer 59.

SCA's determination of the ML/TF risks posed by Customer 59

1374. On and from 21 February 2017 Customer 59 was appropriately rated by SCA as a high risk customer for the purpose of the Act and Rules.

Particulars

On 21 February 2017, Customer 59 was rated high risk.

1375. Nevertheless, for the reasons pleaded below, SCA failed to monitor the high ML/TF risks posed by Customer 59 on an ongoing basis because the risk-based procedures, systems and controls in the Part A Program were not aligned to the ML/TF risks reasonably faced by it with respect to Customer 59.

Monitoring of Customer 59's transactions

1376. At no time did SCA apply appropriate transaction monitoring to Customer 59's transactions because SCA's transaction monitoring program did not include appropriate risk-based systems and controls to monitor the transactions of customers, including FMA transactions indicative of ML/TF typologies and vulnerabilities.

Particulars

Sections 36(1)(a) and (b) of the Act and rr 15.4 to 15.8 of the Rules.

See paragraphs 437 to 441 above.

The review, update and verification of Customer 59's KYC information

1377. SCA did not review, update or verify Customer 59's KYC information, having regard to the high ML/TF risks posed, because:

a. the Part A Program did not include appropriate risk-based systems and controls to enable SCA to determine in what circumstances further KYC information should be collected, verified, reviewed or updated for ongoing customer due diligence purposes;

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138 above.

b. SCA did not appropriately review the nature of its business with Customer 59, including the nature, extent and purpose of Customer 59's transactions, having regard to the high ML/TF risks;

c. SCA did not appropriately review, update, or verify Customer 59's source of wealth or source of funds, including the origin of funds, having regard to the high ML/TF risks; and

Particulars

By reason of the matters set out in *Customer 59's risk profile* above, there were higher ML/TF risks associated with Customer 59's source of wealth or source of funds.

d. to the extent that SCA reviewed Customer 59's KYC information on and from 7 December 2016, it failed to appropriately consider the high ML/TF risks posed by the provision of designated services by SCA to Customer 59.

Particulars

Sections 36(1)(a) and (b) of the Act, r 15.2 of the Rules and the definition of KYC information, in relation to a customer who is an individual, in r 1.2.1 of the Rules.

See paragraph 138(h) above.

ECDD triggers in respect of Customer 59

1378. SCA was required to apply the ECDD program to Customer 59 following any ECDD triggers in respect of Customer 59.

Particulars

Sections 36(1)(a) and (b) of the Act.

Rules 15.9(1) and 15.10 of the Rules.

1379. Customer 59 was determined by SCA to be high risk for the purpose of the Act and Rules during the relevant period.

Particulars

See *SCA's determination of the ML/TF risks posed by Customer 59* above.

1380. The matter pleaded at paragraph 1379 was an ECDD trigger.

Particulars

See paragraphs 496 and 504 above.

1381. SCA did not conduct appropriate risk-based ECDD with respect to Customer 59 following an ECDD trigger because:

a. on each occasion prior to 22 October 2021 that SCA conducted ECDD in respect of Customer 59 in response to an ECDD trigger, it failed to appropriately consider the ML/TF risks posed by Customer 59 and failed to appropriately consider whether the ML/TF risks posed by Customer 59 were within SCA's ML/TF risk appetite; and

Particulars

Rules 15.10(2) and (5) of the Rules.

See paragraphs 501 and 511 above.

On 23 July 2018 and 10 April 2019, SCA conducted ECDD in respect of Customer 59.

The ECDD identified media articles published in March 2014 naming Customer 59 as the director of a company which was alleged to be encouraging its workers not to pay taxes.

On 22 October 2021, SCA issued a ban in respect of Customer 59, due to concerns related to the legitimacy of the funds that Customer 59 gambled with.

The ECDD conducted by SCA did not have appropriate regard to Customer 59's higher ML/TF risks: see *Customer 59's risk profile* above.

The ECDD conducted by SCA did not have appropriate regard to the higher ML/TF risks posed by Customer 59's source of funds or source of wealth.

By reason of the matters set out in *Customer 59's risk profile* above, there were higher ML/TF risks associated with Customer 59's source of wealth or source of funds.

b. at no time prior to 22 October 2021 did senior management consider the higher ML/TF risks posed by Customer 59 in response to an ECDD trigger, or appropriately consider whether the ML/TF risks posed by Customer 59 were within SCA's ML/TF risk appetite.

Particulars

Rules 15.10(6) and (7) of the Rules.

On 19 October 2021, a memorandum was sent to the SCA Director and General Counsel by the SCA AML team, as Customer 59 had been rated significant risk. The memorandum referred to the July 2021 media reports naming Customer 59 in connection with tax evasion and 'phoenixing' behaviour. The memorandum concluded that the highly publicised tax proceedings against Customer 59 raised concerns around the legitimacy of the funds that Customer 59 gambled with and recommended that SCA discontinue its business relationship with Customer 59.

On 22 October 2021, SCA issued a ban in respect of Customer 59.

Contravention of s 36 of the Act in respect of Customer 59

1382. By reason of the matters pleaded at paragraphs 1370 to 1381 above, on and from 7 December 2016, SCA:

a. did not monitor Customer 59 in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced; and

b. did not do so in accordance with rr 15.2, 15.5 and 15.9 of the Rules.

Particulars

Sections 36(1)(a) and (b) of the Act are civil penalty provisions: s 36(2) of the Act.

See also rr 9.1.3 and 9.1.4 of the Rules.

1383. By reason of the matters pleaded at paragraph 1382, SCA contravened s 36(1) of the Act on and from 7 December 2016 to 22 October 2021 with respect to Customer 59.

Particulars

Section 36(1) of the Act is a civil penalty provision: s 36(2) of the Act.

Customers transacting through the SCEG Customer Account channel – Confidential Schedule A

1384. On each of the dates listed in column 2 of Confidential Schedule A, money in the currency and amount specified in columns 3 and 4 of Confidential Schedule A was deposited into a SCEG Customer account by or on behalf of the customer specified in column 1 of Confidential Schedule A.

1385. SCA credited each deposit of money specified in column 4 of Confidential Schedule A to an FMA in the name of each corresponding customer specified in column 1 of Confidential Schedule A.

1386. SCA made money available to a customer when it credited the customer's FMA with the money that had been deposited into the SCEG Customer account.

1387. The credit to an FMA, as pleaded at paragraph 1385, was a designated service provided by SCA under:

a. item 32, table 1, s6 of the Act; and

b. item 13, table 3, s6 of the Act.

Particulars

See paragraph 234 above.

1388. Transactions involving the designated services pleaded at paragraph 1386 above were provided or facilitated through the SCEG Customer account channel.

Particulars

See paragraphs 239 to 268 above.

The SCEG Customer account channel involved higher ML/TF risks: see paragraphs 255 and 256 above.

From August 2019, designated services provided via the SCEG Customer account channel also included designated services via the Horizon Tourism channel: see paragraphs 257 and 258 above. Transactions in Confidential Schedule A that involved the provision of designated services through the Horizon Tourism channel are highlighted in blue in Confidential Schedule A.

The Horizon Tourism account channel posed particularly high ML/TF risks: see paragraph 259 above. In particular:

a. three of the customers specified in Confidential Schedule A accessed over $1,300,000 through the Horizon Tourism account channel from 24 June 2020 to 28 March 2022;

b. four of the customers specified in Confidential Schedule A accessed over HKD$34,000,000 through the Horizon Tourism account channel from 28 August 2019 to 5 January 2021; and

c. five of the customers specified in Confidential Schedule A accessed the equivalent of over $1,000,000 in another foreign

currency through the Horizon Tourism account channel from 24 February 2022 to 9 June 2022.

1389. SCA did not appropriately assess the ML/TF risks of providing the designated services pleaded at paragraph 1386 to the customers specified in Confidential Schedule A through the SCEG Customer account channel.

Particulars

See paragraphs 260 and 261 above.

1390. The Standard Part A Program did not include appropriate risk-based systems and controls to understand the source of funds transferred through the SCEG Customer account channel.

Particulars

See paragraphs 262 and 516 above.

1391. SCA did not apply appropriate risk-based transaction monitoring to transactions provided or facilitated through the SCEG Customer account channel at any time.

Particulars

See paragraph 479 above.

1392. SCA did not apply appropriate risk-based systems and controls that were capable by design of identifying, mitigating and managing the ML/TF risks reasonably faced by SCA with respect to the designated services pleaded at paragraph 1386 above that were provided or facilitated through the SCEG Customer account channel.

Particulars

See paragraphs 262 and 268 above.

These transactions involved higher ML/TF risks and less transparency as to the source of funds.

1393. By failing to apply appropriate risk-based transaction monitoring to the transactions involving the designated services pleaded at paragraph 1386 above, SCA failed to monitor each of the 65 customers specified in Confidential Schedule A with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced in relation to the provision of designated services.

1394. By reason of the matters pleaded at paragraphs 1383 to 1392, SCA did not monitor each of the 65 customers specified in Confidential Schedule A in relation to the provision of designated services, with a view to identifying, mitigating and managing the ML/TF risks it reasonably faced, and did not do so in accordance with the Rules.

1395. By reason of the matters pleaded at paragraph 1393, SCA contravened s36(1) of the Act on 65 occasions in relation to the customers specified in column 1 of Confidential Schedule A from the earliest date listed in column 2 until the latest listed date in column 2 of Confidential Schedule A.

Particulars

Section 36(1) of the Act is a civil penalty provision: s36(2) of the Act.

The customers specified in Confidential Schedule A accessed over $16,600,000 through the SCEG customer accounts channel in 72 transactions from 12 December 2016 to 15 July 2022.

The customers specified in Confidential Schedule A accessed over HKD$80,000,000 through the SCEG customer accounts channel in 22 transactions from 16 March 2017 to 5 January 2021.

The customers specified in Confidential Schedule A accessed over NZD$1,400,000 through the SCEG customer accounts channel in seven transactions from 26 January 2017 to 27 May 2019.

The customers specified in Confidential Schedule A accessed the equivalent of over $12,000,000 in other foreign currencies through the SCEG customer accounts channel in 93 transactions from 13 December 2016 to 9 June 2022.

And the Applicant claims the relief specified in the accompanying Application.

Date: 07 December 2022

.....

Sonja Marsic
AGS Lawyer
for and on behalf of the Australian Government Solicitor
Lawyer for the Applicant

This pleading was prepared by Sonja Marsic, Lawyer.

CERTIFICATE OF LAWYER

I, Sonja Marsic, certify to the Court that, in relation to the statement of claim filed on behalf of the Applicant, the factual and legal material available to me at present provides a proper basis for each allegation in the pleading.

Date: 07 December 2022

.....

Sonja Marsic
AGS Lawyer
for and on behalf of the Australian Government Solicitor
Lawyer for the Applicant

Schedule A (confidential)

This schedule is confidential. This page has been intentionally left blank.

Schedule B (confidential)

This schedule is confidential. This page has been intentionally left blank.

Schedule C (confidential)

This schedule is confidential. This page has been intentionally left blank.

Schedule D (confidential)

This schedule is confidential. This page has been intentionally left blank.

Schedule E (confidential)

This schedule is confidential. This page has been intentionally left blank.