NOTICE OF FILING

Details of Filing

Document Lodged:	Statement of Agreed Facts
Court of Filing	FEDERAL COURT OF AUSTRALIA (FCA)
Date of Lodgment:	17/05/2024 2:59:45 PM AEST
Date Accepted for Filing:	17/05/2024 2:59:50 PM AEST
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.

FEDERAL COURT OF AUSTRALIA

DISTRICT REGISTRY: NEW SOUTH WALES

Division: Commercial and Corporations **No NSD1046 of 2022**

CHIEF EXECUTIVE OFFICER OF THE AUSTRALIAN TRANSACTION REPORTS AND ANALYSIS CENTRE

Applicant

SKYCITY ADELAIDE PTY LTD
ABN: 72 082 362 061

Respondent

STATEMENT OF AGREED FACTS AND ADMISSIONS

Table of Contents

Filed on behalf of the Applicant, Chief Executive Officer of AUSTRAC

File ref: 22008262

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

Address for Service:

The Australian Government Solicitor,

4 National Circuit, Barton, ACT 2600

Jane.Healy@ags.gov.au

Telephone: 02 625 37336

Lawyer's Email:

Jane.Healy@ags.gov.au

Facsimile: 02 9581 7732

FEDERAL COURT OF AUSTRALIA

DISTRICT REGISTRY: NEW SOUTH WALES

Division: Commercial and Corporations **No NSD1046 of 2022**

CHIEF EXECUTIVE OFFICER OF THE AUSTRALIAN TRANSACTION REPORTS AND ANALYSIS CENTRE

Applicant

SKYCITY ADELAIDE PTY LTD
ABN: 72 082 362 061

Respondent

A. INTRODUCTION

1 [redacted]
Tender of this paragraph not accepted by the Federal Court.
[redacted]

2 [redacted]
Tender of this paragraph not accepted by the Federal Court.
[redacted]

3 Between 7 December 2016 and 14 December 2022 (the **Relevant Period**), SCA had Anti-Money Laundering and Counter-Terrorism Financing (**AML/CTF**) Programs (**AML/CTF Programs**) in place for the purpose of seeking to comply with section 81(1) of the AML/CTF Act as set out at paragraph 84.

4 SCA admits that it contravened sections 36(1) and 81(1) of the AML/CTF Act in particular respects in the manner set out in this SAFA. While SCA fell short of its obligations to comply with the AML/CTF Act, the contraventions were not a consequence of any deliberate intention to contravene the AML/CTF Act. At all times, SCA's Boards and senior management sought to ensure that SCA would comply with its obligations under the AML/CTF Act.

5 [redacted]
Tender of this paragraph not accepted by the Federal Court.
[redacted]

Filed on behalf of the Applicant, Chief Executive Officer of AUSTRAC
File ref: 22008262
Prepared by: Jane Healy
AGS lawyer within the meaning of s 55I of the *Judiciary Act 1903*
Address for Service:
The Australian Government Solicitor,
4 National Circuit, Barton, ACT 2600
Jane.Healy@ags.gov.au
Telephone: 02 625 37336
Lawyer's Email:
Jane.Healy@ags.gov.au
Facsimile: 02 9581 7732

[redacted]

B. PARTIES AND BACKGROUND

B.1 AUSTRAC

6 The AUSTRAC CEO is appointed pursuant to section 211 of the AML/CTF Act. The AUSTRAC CEO is charged with enforcing compliance with the AML/CTF Act and subordinate legislation, including the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No.1)* (**AML/CTF Rules**), and has brought the Proceeding in that capacity. After this Proceeding was commenced, on 17 June 2023, an Acting AUSTRAC CEO was appointed pursuant to section 221 of the AML/CTF Act. On 15 December 2023, Mr Brendan Thomas was appointed by the Commonwealth Attorney-General, the Hon. Mark Dreyfus KC MP, as the AUSTRAC CEO. Mr Thomas commenced his five-year appointment as the AUSTRAC CEO on 29 January 2024.

B.2 SkyCity Adelaide Pty Ltd

7 SCA is a provider of designated services within the meaning of the AML/CTF Act as outlined below (see paragraph 13).

8 Throughout the Relevant Period, SkyCity Entertainment Group Limited (**SCEG**) was the ultimate parent company of SCA.

9 SCA is, and at all material times during the Relevant Period was:

a. incorporated in Australia;

b. a person within the meaning of section 5 of the AML/CTF Act;

c. a reporting entity within the meaning of section 5 of the AML/CTF Act;

d. a provider of designated services to customers within the meaning of section 6 of the AML/CTF Act; and

e. carrying on activities or business through a permanent establishment in Australia for the purposes of the AML/CTF Act.

10 At all material times during the Relevant Period, SCA operated a casino located at North Terrace, Adelaide, South Australia 5001 (**SCA casino**).

11 At all material times during the Relevant Period, SCA:

a. held a casino licence under section 5 of the *Casino Act 1997* (SA) (**Casino Act**); and

b. operated the SCA casino under the Approved Licensing Agreement between the Minister for Business Services and Consumers (South Australia) and SCA, dated 27 October 1999 (and as amended from time to time) (**ALA**).

12 Throughout the Relevant Period, SCA provided high volume, high value and high frequency designated services within the meaning of table 1 and table 3, section 6 of the AML/CTF Act, in the context of the gambling sector. Some of those designated services included transactions across international borders. From:

a. 7 December 2016 to February 2017, SCA's AML/CTF Programs recorded that the SCA casino attracted an average of over 5,500 visitors per day and provided gaming

[redacted]

services from over 90 tables and 990 gaming machines, and that the SCA casino generated significant interstate and local business; and

b. February 2017 to about 17 November 2022, each version of SCA's AML/CTF Programs recorded that the SCA casino attracted an average of over 5,500 visitors per day and provided gambling services from up to 200 tables and up to 1,500 gaming machines, and that the SCA casino generated international, interstate and local business.

B.3 Designated services

13 The AML/CTF Act applies with respect to the provision of designated services. A person who provides a designated service is a reporting entity. Throughout the Relevant Period, SCA was a reporting entity that provided the following designated services pursuant to section 6 of the AML/CTF Act:

Financial services, table 1, section 6 of the AML/CTF Act

a. item 6, table 1, section 6 of the AML/CTF Act – making a loan as defined under section 5 of the AML/CTF Act, where the loan is made in the course of carrying on a loans business;

b. item 7, table 1, section 6 of the AML/CTF Act – in the capacity of the 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;

c. item 31, table 1, section 6 of the AML/CTF Act – 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; and

d. item 32, table 1, section 6 of the AML/CTF Act – 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 under a designated remittance arrangement;

Gaming services, table 3, section 6 of the AML/CTF Act

e. item 1, table 3, section 6 of the AML/CTF Act – 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;

f. item 4, table 3, section 6 of the AML/CTF Act – paying out winnings in respect of a bet, where the service is provided in the course of carrying on a gambling business;

g. item 6, table 3, section 6 of the AML/CTF Act – accepting the entry of a person into a game, where:

   i. the game is played for money or anything else of value;

   ii. the game is a game of chance or of mixed chance and skill;

   iii. the service is provided in the course of carrying on a gambling business; and

   iv. the game is not played on a gaming machine located at an eligible gaming machine venue;

h. item 7, table 3, section 6 of the AML/CTF Act – exchanging money or digital currency for gaming chips, tokens or betting instruments, where the service is provided in the course of carrying on a business;

i. item 8, table 3, section 6 of the AML/CTF Act – exchanging gaming chips, tokens or betting instruments for money or digital currency, where the service is provided in the course of carrying on a business;

j. item 9, table 3, section 6 of the AML/CTF Act – paying out winnings, or awarding a prize, in respect of a game where:

   i. the game is played for money or anything else of value;

   ii. the game is a game of chance or of mixed chance and skill;

   iii. the service is provided in the course of carrying on a gambling business; and

   iv. the game is not played on a gaming machine located at an eligible gaming machine venue;

k. items 11 to 13, table 3, section 6 of the AML/CTF Act – in the capacity of account provider:

   i. opening an account; or

   ii. allowing a person to be a signatory on an account; or

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

   where the account provider is a person who provides a service covered by item 1, 2, 3, 4, 6, 7, 8 or 9, table 3, section 6 of the AML/CTF Act, and the purpose, or one of the purposes, of the account is to facilitate the provision of a service covered by item 1, 2, 3, 4, 6, 7, 8 or 9, table 3, section 6 of the AML/CTF Act, and the service is provided in the course of carrying on a business; and

l. item 14, table 3, section 6 of the AML/CTF Act – 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 item 1, 2, 3, 4, 6, 7, 8 or 9, table 3, section 6 of the AML/CTF Act, and the service is provided in the course of carrying on a business.

14 Section C and Section F.3 set out details of the designated services provided by SCA during the Relevant Period.

B.4 Overview of the key concepts underlying the AML/CTF Act

15 Section 3 of the AML/CTF Act sets out the objects of the legislation, which relevantly include (from 3 April 2018):

a. to provide for measures to detect, deter and disrupt money laundering (**ML**), the financing of terrorism (**TF**), and other serious financial crimes (section 3(1)(aa) of the AML/CTF Act); and

b. to support cooperation and collaboration among reporting entities, AUSTRAC and other government agencies, particularly law enforcement agencies, to detect, deter and disrupt ML, TF, and other serious crimes (section 3(1)(ac) of the AML/CTF Act).

16 Chapter 1 of the AML/CTF Rules defines ML and TF (**ML/TF**) risk (**ML/TF risk**) as "*the risk that a reporting entity may reasonably face that the provision by the reporting entity of designated services might (whether inadvertently or otherwise) involve or facilitate money laundering or the financing of terrorism.*"

17 The designated services provided by SCA gave rise to ML/TF risk. Relevantly:

a. in addition to gaming services (table 3, section 6 of the AML/CTF Act), casinos can provide loans and remittance services as described in table 1, section 6 of the AML/CTF Act, by enabling customers to move funds into and out of the casino environment (including domestically and internationally). This can involve higher ML/TF risk;

b. casinos are particularly vulnerable to ML, for reasons including because the nature of their business involves a significant amount of cash. It is difficult to trace the source and ownership of cash, and the proceeds of crime are often in cash;

c. customers of a casino can move funds through different designated services, including by:

i. transferring funds through cash and casino value instruments (**CVIs**) (such as chips and tickets) and gaming accounts;

ii. transferring funds to or from their own gaming account; and

iii. drawing on or redeeming credit provided by the casino through a Cheque Cashing Facility (**CCF**);

d. the movement of funds through different designated services at a casino can make it difficult to understand the purpose of transactions, the beneficial owner of the funds or the ultimate beneficiary. The movement of funds through a casino can involve:

i. long and complex transaction chains (such as those identified at subparagraph 17c); and

ii. multiple channels, including non-face-to-face channels;

e. casinos may also provide designated services to customers who involve higher ML/TF risk, including customers transacting through junket programs or individual commission programs (**ICPs**), customers from foreign jurisdictions, and potentially foreign politically exposed persons (**PEPs**); and

f. ML/TF typologies are the various methods that criminals use to conceal, launder or move illicit funds. Set out at **Schedule 1** below are ML vulnerabilities and ML/TF typologies that were relevant to casinos during the Relevant Period.

18 As set out in Section D, to manage ML/TF risk, the AML/CTF Act provides that each reporting entity is required to:

a. identify, mitigate and manage the ML/TF risk it reasonably faces;

b. adopt and maintain[1] an AML/CTF program within the meaning of section 83 of the AML/CTF Act; and

[1] AML/CTF Act, section 81.

c. conduct ongoing due diligence of its customers in relation to the provision by the reporting entity of designated services (see section 36(1) of the AML/CTF Act).

19 The AML/CTF Act does not require ML/TF risk to be eliminated. Nor does the AML/CTF Act prescribe exactly how a reporting entity is to manage its ML/TF risk. The AML/CTF Act reposes trust in a reporting entity to design and implement risk management procedures, systems and controls to detect and deter ML/TF risk that are appropriate for its business and that it will adopt and maintain through its AML/CTF program.

20 As further set out at paragraphs 80a and 80b, some of the requirements specified in the AML/CTF Rules may be complied with by a reporting entity putting in place appropriate risk-based systems and controls.[2] In determining the appropriate risk-based systems and controls to put in place, the AML/CTF Act[3] and AML/CTF Rules require the reporting entity to take into account certain matters, including:

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

b. the ML/TF risk it reasonably faces, having regard to:

i. the type of designated services it provides;

ii. the type of customers it provides designated services to;

iii. the methods through which it delivers designated services (known as channels); and

iv. the foreign jurisdictions with which it deals.

21 An AML/CTF program will not include **appropriate risk-based systems and controls** that meet the requirements of the AML/CTF Act, having regard to the AML/CTF Rules, if:

a. it has not taken the matters set out at paragraph 20 into account when designing and adopting the procedures, systems and controls; and

b. the procedures, systems and controls are not aligned and proportionate to the ML/TF risk reasonably faced by the reporting entity having regard to the matters set out at paragraph 20b.

22 The AML/CTF Act and AML/CTF Rules require reporting entities to have regard to the matters set out at paragraph 20 when determining what ongoing customer due diligence (**OCDD**) is appropriate for its customers (see paragraph 80j).

B.5 Overview of SCA's contraventions of the AML/CTF Act

23 SCA admits that during the Relevant Period:

a. its AML/CTF Programs did not meet all of the requirements of the AML/CTF Act and AML/CTF Rules (see Section D); and

b. it did not carry out adequate OCDD with respect to 56 Higher Risk Customers and 65 SCEG Channel Customers, resulting in 121 contraventions of section 36(1) of the AML/CTF Act (see Section G).

---

[2] AML/CTF Rules, paragraph 8.1.3.

[3] AML/CTF Act, sections 82(a) and (c).

24 SCA admits that the contraventions set out at paragraph 23 made SCA vulnerable to criminal exploitation and exposed the Australian community and financial systems to ML/TF risk (see Section H).

C. GAMING SERVICES AND FINANCIAL SERVICES

25 Throughout the Relevant Period, SCA offered a number of financial and gaming services to customers within the scope of tables 1 and 3, section 6 of the AML/CTF Act, including members of SCA's loyalty program and non-members.

C.1 Membership

26 During the Relevant Period, customers of SCA could apply to become 'members' of SCA's loyalty program. In order to become a member, a customer was required to complete an application process, in the course of which SCA obtained identification information about the customer. Once relevant identification information had been provided, members were then issued with a SCA loyalty card, which allowed them to earn points from gaming and other expenditure at the SCA casino. These points could be redeemed for gaming or other rewards (for example, food and beverages) at the SCA casino. Depending on their level of gaming activity and place of residence, members could attain different 'tiers' of membership, which offered them access to increasing levels of rewards at the SCA casino and certain SCA facilities.

C.2 Gaming locations

27 SCA primarily provided gaming services on the main gaming floor of the SCA casino, which was accessible to all customers. In addition, SCA provided access to VIP gaming areas within the SCA casino which were only accessible to select VIP members who qualified for such access. These VIP gaming areas included individual VIP gaming suites which were allocated to specific higher value VIP customers, based on availability and customer preference. At no time did VIP customers have exclusive access to a permanently allocated VIP gaming area. VIP customers in VIP gaming areas were serviced and monitored at all times by SCA employees.

28 Access to the VIP gaming areas was regulated by the Casino Act and ALA. The ALA required that, subject to exceptions set out in clauses 8.7.2 to 8.7.5, SCA must not permit a person to game in a VIP gaming area unless that person meets the definition of a premium customer, as set out in the ALA. The exceptions allowed VIP customers to request that other persons (who were not premium customers) gamble in VIP gaming areas while they were present on casino premises.

29 VIP customers were members of SCA's loyalty program, which included the following membership levels over the Relevant Period: 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 had a minimum theoretical spend of $6,000 within a six-month period, with a minimum average daily theoretical spend of $200.

30 From July 2016 onwards (that is, for the entirety of the Relevant Period), SCA required that all patrons join SCA's loyalty program prior to being granted entry into the VIP gaming areas, with a limited exception of persons who had no intention of gaming (such as the spouse of a VIP customer, or a person known to be part of a junket operator's staff). In those circumstances, SCA did not require any form of valid identification. However, from mid-2018 onwards, all persons entering the VIP gaming areas were required to join SCA's loyalty program before being granted access to the VIP gaming areas.

C.3 Gaming types

31 Throughout the Relevant Period, SCA offered a range of games that involved the provision of designated services under table 3, section 6 of the AML/CTF Act, including:

a. table games – games offered at tables on the main gaming floor and in VIP gaming areas, including baccarat, roulette, blackjack, poker and others;

b. electronic table games (**ETGs**) – which included semi and fully automated versions of traditional table games, where customers played at terminals; and

c. electronic gaming machines (**EGMs**) – themed games played on electronic machines.

32 SCA provided designated services under items 6 and 9, table 3, section 6 of the AML/CTF Act with respect to these games.

C.4 SCA's ICT Framework

33 Throughout the Relevant Period, SCA used multiple information systems to record information relevant to its customers and the provision of designated services, which comprised of:

a. **Bally CMP System**: a casino management software system used to record relevant personal information about customers. The Bally CMP System was used to create loyalty accounts and record customer detail, including a customer's rated gambling activity on EGMs and table games, transaction history when using their loyalty card or front money account (**FMA**), and loyalty program status and history. It was also used to maintain specific identification and Know Your Customer (**KYC**) information records (against a customer's player profile), including a customer's full name, date of birth, occupation details (if collected), citizenship details (if provided) and VIP sponsorship history. The Bally CMP System also recorded notes entered by frontline staff, information relating to their OCDD or enhanced customer due diligence (**ECDD**) (including amongst other things, the customer's ML/TF risk rating against a player's profile), and tags to record if the customer was a match for a PEP, relative or close associate, or a special interest person. Documents used to verify a customer's identity were to be stored in the Bally CMP System and retained for seven years after the end of SCA's relationship with the customer. From February 2017, transaction records relating to table 3, section 6 of the AML/CTF Act designated services (other than items 1, 2 and 4 (relating to the exchange of chips or tokens only) and item 6, table 3, section 6 of the AML/CTF Act) provided by SCA to its customers were also to be recorded in the Bally CMP System. A copy of the customer's photographic identification was also to be scanned and stored within the Bally CMP System and could be relied on by SCA for verification purposes on subsequent occasions;

b. **Bally Cage System**: an inventory management system used by SCA (primarily by the Cage Manager and cash handling staff members) to perform cage and cash handling functions. Transactions in relation to an FMA were recorded on the Bally Cage System, which sent customer details to the Bally CMP System and assisted in recording transactions for particular customers.[4] The Bally Cage System was also used to record transactions performed at the Cage when linked to a customer's account, including FMA deposits and withdrawals (for example electronic bank transfers and inter-company transfers), chip purchases and redemptions, ticket-in ticket-out (**TITO**) ticket issues and redemptions, hand-pay slip redemptions, chip purchase voucher (**CPV**) purchases and redemptions, transactions that could be

[4] In relation to transactions under $10,000, Bally only contained limited records of these transactions unless the customer elected to play carded (that is, with their loyalty card) (see further at Section F.6 below).

identified as threshold transactions, and manage inventory, including cash, chips and cheques;

c. **Slot Data System** (**SDS**): an integrated information system that monitored EGMs, ETGs and customer activities. SDS captured customer gaming activity by the transfer of data from the relevant EGM or ETG to SDS. Each EGM and ETG was fitted with a gaming machine unit (**GMU**) device, which was configured to transmit data to SDS either every 15 minutes or when a certain event had taken place. An event included (i) the insertion of a customer's loyalty membership card into an EGM or ETG, or (ii) the removal of a customer's loyalty membership card from an EGM or ETG. When a customer was playing on an EGM or 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 the Bally CMP System. The primary function of SDS was slot accounting and player tracking;

d. from March 2015, the **Jade System** (previously named Wynyard): an information system which generated transaction alerts of customer transactions triggered by transaction rules as part of SCA's transaction monitoring program (**TMP**). The Jade System also recorded information relating to a customer's risk rating, customer identification and KYC information, PEP screening records, transaction history, threshold transaction report (**TTR**) submission history against a customer's profile, international funds transfer instruction (**IFTI**) history against a customer's profile (after January 2021), certain customer due diligence information, loyalty program and status history and rule alert history, including the results of reviews of transaction alerts. SCA also used the Jade System to generate reports and alerts through a combination of automated and manual processes, including possible PEP matches and adverse media in relation to SCA customers, and template reports in relation to TTRs and IFTIs for uploading to AUSTRAC. From November 2020, SCA moved to an automated IFTI reporting process;

e. **iTrak**: SCA used iTrak to record incident files and records relating to potentially suspicious matters, customer identification and KYC information records (for subject profiles), information relating to customer PEP screening, incidents recorded by the surveillance department and the security department in the form of incident files, audits and daily logs, source of funds and source of wealth information (where provided), information relating to OCDD or ECDD carried out with respect to a customer (for subject profiles), and transactions monitored or logged by the surveillance department. SCA also used iTrak to store records of suspicious matter reports (**SMRs**) submitted to AUSTRAC;

f. from 4 June 2014, SCA used its **network drives** to record information relating to a customer's risk rating, including records relating to OCDD or ECDD carried out with respect to a customer, customer identification and KYC information records, information relating to customer PEP screening, including the results of a manual check of the Dow Jones database for junket operators, junket representatives and junket players, source of funds and source of wealth information (when provided), and results of system-generated reviews of transactions (other than reviews generated by the Jade System). SCA also used its network drives to store records of SMRs submitted to AUSTRAC. Where a decision to bar particular customers was communicated by way of email between SCA departments, these emails were, in certain circumstances, stored in SCA network drives; and

g. from June 2016, frontline employees used **Microsoft SharePoint** to submit observation report forms to the anti-money laundering (**AML**) team, which would generate an email to the AML team. From 7 December 2016 until about November 2021, the AML team included the AML/CTF Compliance Officer (**AMLCO**), the AML Analyst, the Compliance Manager (up until 1 July 2017) and the AML Compliance Manager (from 5 April 2021).

C.5 Funding of gaming activity

34 Throughout the Relevant Period, SCA provided financial services within the meaning of items 6, 7, 31 and 32, table 1, section 6 of the AML/CTF Act (as described at paragraphs 13a to 13d), that facilitated the movement of funds into and out of the SCA casino environment, including across international borders. SCA also provided gaming accounts to customers, within the meaning of table 3, section 6 of the AML/CTF Act, to facilitate the funding of gaming activity.[5] Gaming activity could also be funded through chips, tokens or betting instruments, within the meaning of table 3, section 6 of the AML/CTF Act, also known as CVIs.[6]

C.5.1 The Cage

35 Depending on the game played, customers were able to fund their gaming activities during the Relevant Period in a variety of ways, including by cash, cheque, telegraphic transfer, credit and CCFs, chips and other CVIs (as outlined below). Central to facilitating the funding of gaming activity was the Cage, which operated as the 'bank' of the casino and managed the monetary transactions between customers and the SCA casino in relation to gaming. SCA had multiple Cage cashier windows in various locations in the SCA casino, at which customers could conduct transactions. The Cage also processed some monetary transactions that SCA customers could conduct non-face-to-face. The Cage had a role in preparing TTRs, transaction monitoring and carrying out KYC procedures, where required.

C.5.2 Front Money Accounts

36 During the Relevant Period, customers were able to establish an FMA at the SCA casino, Customers could use FMAs for the purpose of gaming or hospitality. Customers could credit their FMA by depositing funds in cash, cheque or by telegraphic transfer into bank accounts maintained by SCA (the SCA Customer accounts, as described at paragraphs 41 to 42 and 168 to 172) or a SCEG subsidiary (the SCEG Customer accounts, as described at paragraphs 44 to 45 and 176 to 177). Customers could also credit their FMAs by making a deposit at the Cage in cash, chips, TITO tickets or other CVIs. Funds could also be deposited into a customer's FMA by way of transfer from the customer's FMA established at another SCEG casino (as described at paragraph 47, including via the SkyCity New Zealand channel as described at Section F.3.4 below) to their FMA at the SCA casino, or by a third party (as described at paragraphs 164 to 165). Transfers to and from FMAs, via the SCA Customer accounts, SCEG Customer accounts and the SkyCity New Zealand channel, involved the facilitation of the transfer of funds in and out of the SCA casino environment, by SCA, at the request of its customers, which involved the provision of designated services under items 31 and 32, table 1, section 6 of the AML/CTF Act (as described at paragraphs 13c to 13d) and item 13, table 3, section 6 of the AML/CTF Act.

37 FMAs are described further at Section F.3.1.

C.5.3 Casino Value Instruments

38 SCA provided table 3, section 6 of the AML/CTF Act designated services to customers through the use of CVIs. These included chips, CPVs, TITOs, and hand-pay slips.

39 Customers who did not have an FMA could buy-in at a table game using cash, or were able to purchase a CPV at the Cage, which could be exchanged for chips at a gaming table. During the Relevant Period, SCA offered non-Cage buy-in facilities, which enabled customers to purchase chips or vouchers for use at gaming tables. By way of example, a

[5] Items 11 and 13, table 3, section 6 of the AML/CTF Act.

[6] Items 7 and 8, table 3, section 6 of the AML/CTF Act.

TITO ticket could be generated by an EGM or ETG at the completion of play, which could be used to obtain an item 6, table 3, section 6 of the AML/CTF Act designated service.

40 CVIs are described further at paragraphs Section F.3.7.

C.5.4 SCA Customer account channel

41 During the Relevant Period, SCA maintained two Australian bank accounts in Australian dollars (**SCA Customer accounts**) which were used to facilitate the transfer of funds into and out of an FMA for both international and domestic customers (the **SCA Customer account channel**). SCA customers could deposit funds into these accounts, including by non-face-to-face direct transfer both from within Australia and internationally, to fund gaming activity at the SCA casino or to repay a debt owed to SCA under a CCF. Funds could be deposited into the SCA Customer accounts by cash, cheque or telegraphic transfer. Until 12 January 2022, SCA permitted third party deposits to be made on behalf of SCA customers into the SCA Customer accounts, including from money remitters or other casinos (including non-SCEG casinos and casinos located outside Australia). After 12 January 2022, and up until December 2022, customers could still transfer funds between SCEG casinos.

42 Transfers to and from FMAs, via the SCA Customer accounts, involved the facilitation of the transfer of funds in and out of the SCA casino environment, by SCA, at the request of its customers, which involved the provision of designated services under items 31 and 32, table 1, section 6 of the AML/CTF Act (as described at paragraphs 13c to 13d) and item 13, table 3, section 6 of the AML/CTF Act.

43 The SCA Customer account channel is described further at Section F.3.2.

C.5.5 SCEG Customer account channel

44 During the Relevant Period, SCEG subsidiaries maintained international bank accounts in both Australian dollars and foreign currency (**SCEG Customer accounts**), which were used to facilitate the transfer of funds into and out of an FMA (**SCEG Customer account channel**). SCA customers could deposit funds into these accounts, including by non-face-to-face direct transfer both from within Australia and internationally, to fund gaming activity at the SCA casino or to repay a debt owed to SCA under a CCF. Funds could be deposited into the SCEG Customer accounts by cash, cheque or telegraphic transfer, either in Australian dollars or a foreign currency depending on the account (although some SCEG Customer accounts did not accept cash deposits). Until June 2021, a customer could transfer funds from their FMA to a third party via the SCEG Customer account channel (as described further at paragraphs 166b and 225e). SCA also introduced a standard operating procedure (**SOP**) which provided that after June 2021 third party deposits (via telegraphic transfer) into the SCEG Customer accounts to be transferred to another customer's FMA were no longer accepted (other than in limited circumstances). In September 2022, SCA introduced guidance for staff about the process for third party payment rejection where third party deposits (via telegraphic transfer) were made into the SCEG Customer account channel.

45 Transfers to and from FMAs, via the SCEG Customer accounts, involved the facilitation of the transfer of funds in and out of the SCA casino environment, by SCA, at the request of its customers, which involved the provision of designated services under items 31 and 32, table 1, section 6 of the AML/CTF Act (as described at paragraphs 13c to 13d) and item 13, table 3, section 6 of the AML/CTF Act.

46 The SCEG Customer account channel is described further at Section F.3.3.

C.5.6 SkyCity New Zealand channel

47 Throughout the Relevant Period, a customer with funds in an FMA established at a SCEG casino could request for the transfer of all or some of those funds to the customer's FMA at

the SCA casino (the **SkyCity New Zealand channel**). A customer could use the SkyCity New Zealand channel to make funds available to their FMA at the SCA casino, or to repay a debt owed by the customer to SCA under a CCF from their gaming at the SCA casino.

48 Transfers to FMAs, via the SkyCity New Zealand channel, involved the facilitation of the transfer of funds in the SCA casino environment, by SCA, at the request of its customers, which involved the provision of designated services under item 32, table 1, section 6 of the AML/CTF Act (as described at paragraph 13d) and item 13, table 3, section 6 of the AML/CTF Act.

49 The SkyCity New Zealand channel is described further at Section F.3.4.

C.5.7 Cheque Cashing Facility

50 Throughout the Relevant Period, [7] customers could apply to SCA for a CCF. A CCF was a facility through which approved customers could access funds for gaming. Only customers who were members of the SCA loyalty program (providing access to an FMA) and approved by SCA were eligible for a CCF. The CCF Standard Application Form or, from March 2020, the Group Operator Credit Form or Individual Credit Application Form, 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**). The CCF Agreement with SCA provided for an agreed credit limit. Funds were made available (up to the approved limit) through the customer's FMA, including junket operators. The advance of funds, was a 'loan' within the meaning of section 5 of the AML/CTF Act. From December 2022, SCA ceased the practice of providing CCFs to customers.

51 If a CCF was approved, funds were credited to a customer's FMA (the **drawdown of funds under a CCF**). Before the customer was permitted to drawdown the funds, the customer was required to either present a signed blank personal cheque or was issued with a counter cheque (credit marker) by SCA that could be drawn against the approved CCF limit. A credit marker refers to the practice of creating counter cheques to debit FMAs. A drawdown of funds under a CCF was a transaction in relation to a 'loan'.

52 SCA provided designated services under items 6, and 7, table 1, section 6 of the AML/CTF Act when it executed or approved a CCF Agreement or where a drawdown of funds under a CCF occurred.

53 CCFs are described further at Section F.3.5.

C.5.8 EZYPlay Guest Cards

54 EZYPlay Guest Cards were physical cards used by SCA customers to undertake cashless gaming at the SCA casino, and could be used to add or withdraw funds. EZYPlay Guest Cards were a channel through which SCA provided items 6, 7, 8 and 9, table 3, section 6 of the AML/CTF Act designated services, including non-face-to-face transactions.

55 EZYPlay Guest Cards are described further at Section F.3.6.

C.5.9 Foreign currency exchange

56 SCA accepted physical currency, foreign drafts (except for some limited exceptions), and travellers' cheques for the purposes of currency exchange (SCA ceased accepting travellers' cheques in July 2022). Customers could also deposit or transfer funds into foreign currency accounts maintained by SCEG (the SCEG Customer accounts). SCA would convert the funds to Australian dollars and make them available to the customer in their FMA. Currency

[7] SCA temporarily suspended issuing CCFs and Credit Markers in December 2022. The temporary suspension became a permanent policy in April 2023 at both the SCA casino and other SCEG casinos.

exchange was also facilitated for customers who were repaying debts owed to SCA, including when SCA accepted repayment through the SCEG Customer accounts (following the end of the customer's visit to the SCA casino or when settlement of outstanding debts occurred) or by foreign draft. SCA provided foreign currency exchange services to customers within the meaning of item 14, table 3, section 6 of the AML/CTF Act.

57 Foreign currency exchange services are described further at Section F.3.9.

C.5.10 Foreign currency services

58 SCA provided, or had the capacity to provide, a number of designated services in Hong Kong dollars (**HKD**), including gaming services to international players and the provision of chips and credit in HKD.

C.6 Turnover, revenue and profit

59 Certain transactions engaged in by customers at the SCA casino during the Relevant Period were recorded as 'turnover'. Total turnover reflected the total amount wagered by customers. It included the re-betting of winnings and, accordingly, could be many multiples of the buy-in[8] and/or cash out[9] of the customer. On each occasion that a customer wagered money on a game, a table 3, section 6 of the AML/CTF Act designated service was provided. However, because of re-betting of winnings, 'turnover' does not represent the total value of money presented by the customer and moved through a casino.

60 However, turnover is relevant to quantifying the nature and scale of the ML/TF risks posed by junkets and high risk customers. High turnover, including through complex transaction chains and within junkets, provides criminals with the opportunity to mix illicit funds with legitimate funds and to obscure the source of funds.[10] High turnover increases the risk of ML/TF. Appropriate risk-based procedures, systems and controls are required to be included in AML/CTF programs to address the ML/TF risk of high turnover through junket and high risk customers.[11]

61 Revenue from designated services provided through gaming channels (including junket channels) was a fraction of total turnover. Revenue was the aggregate of customer losses, after the aggregate of customer wins had been paid out.

62 Revenue figures during the Relevant Period did not take into account SCA's costs and as such, revenue in relation to certain customers or groups of customers is not instructive of the profit, if any, to SCA resulting from its dealings with those customers. Profits to SCA, if any, from particular customers or customer groups are difficult to calculate, and due to the nature of gaming usually only represent a small proportion of the revenue earned by SCA in relation to those customers.

63 The revenue and turnover figures referenced in this SAFA measure revenue and turnover generated by recorded customer gaming activities across the Relevant Period. It does not represent revenue and turnover which would not have necessarily arisen but for the contraventions admitted in this SAFA (the extent of which is not known).

C.7 Junkets

64 A junket is an arrangement between a casino and a junket operator that facilitates gambling by one or more high wealth players (referred to as junket players) at the casino, on terms

---

8 Buy-in refers to the purchase by a customer of chips or other CVIs.

9 Cash out refers to the exchange of chips or other CVIs for money.

10 See paragraph 17c for examples of complex transaction chains.

11 See paragraphs 20-21 for an explanation of appropriate risk-based procedures, systems and controls.

agreed between the junket operator and the casino. Junket operators can be represented by one or more junket representatives.

65 Between 7 December 2016 and 12 April 2021, SCA offered and facilitated junket programs, also referred to by SCA as Group Commission Programs (**GCPs**).

66 SCA was required to comply with the Casino (Commission Operations) Directions Notice 2015 (**Directions Notice**) issued by the former Independent Gambling Authority, South Australia, which came into operation on 25 February 2015. The Directions Notice required SCA to collect information relevant to a junket program about the identity and residence of the junket participants. Compliance with this Directions Notice was not directed at SCA's ML/TF risk or compliance with the AML/CTF Act.

67 From 7 December 2016 to 2 January 2021, SCA generated approximately $26 million in revenue from designated services provided through junket channels, and recorded significant turnover associated with the provision of table 3, section 6 of the AML/CTF Act designated services through junket channels at the SCA casino, as described in Section F.4.

68 The last recorded junket program took place at the SCA casino on 2 January 2021. On 12 April 2021, the SCEG Board decided to permanently ban dealing with junket operators. The SCEG Group and SCA ceased doing business with junkets at that time.

C.8 Individual commission programs

69 An ICP is an arrangement between SCA and an individual to provide benefits to the ICP player, 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 beverages, gambling chips and bonus points.

70 From 7 December 2016, SCA offered and facilitated ICPs to interstate and international players only.

71 For each ICP, SCA entered into an ICP agreement (**ICPA**) with the customer which set out the terms and conditions of each program, including any rebates, commissions and/or amounts payable to the customer. The ICPA also set out the terms and conditions on which any other benefits would be made available to the customer, including complimentary airfares, transport, accommodation and food and beverages allowances.

72 SCA offered several types of ICPs, including:

a. non-negotiable commission programs, which utilised non-negotiable chips (**NNEG Programs**);

b. turnover programs, which were only available on baccarat and roulette (**TURN Programs**); and

c. EGM commission programs.

73 In facilitating ICPs, SCA provided table 1 and table 3, section 6 of the AML/CTF Act designated services to ICP program players.

D. RELEVANT OBLIGATIONS UNDER THE AML/CTF ACT AND AML/CTF RULES

74 Throughout the Relevant Period, section 36(1) of the AML/CTF Act required a reporting entity to monitor the reporting entity's customers in relation to the provision of designated services, with a view to identifying, mitigating and managing ML/TF risk. This monitoring had to be conducted in accordance with the AML/CTF Rules, including the requirements set out in Chapter 15 (described at paragraphs 80j to 80o).

75 Throughout the Relevant Period, section 81 of the AML/CTF Act stated that a reporting entity must not commence to provide a designated service to a customer if the reporting entity has not adopted, and does not maintain, an AML/CTF program within the meaning of section 83 of the AML/CTF Act that applies to the reporting entity (being either a standard, joint or special AML/CTF program).

76 The AML/CTF program is the principal document for setting out the risk-based systems and controls a reporting entity will rely upon to ensure compliance with its obligations established under the AML/CTF Act and AML/CTF Rules. It is the means through which a reporting entity is required to take responsibility for managing the ML/TF risk of its own business.

77 Throughout the Relevant Period, section 84(1) of the AML/CTF Act defined a standard AML/CTF program as a written program that applies to a particular reporting entity and is divided into the following parts: Part A (general) and Part B (customer identification).

D.1.1 Part A of an AML/CTF program

78 Throughout the Relevant Period, section 84(2) of the AML/CTF Act defined Part A of a standard AML/CTF program (**Part A Program**) as a part which:

a. had the primary purpose of identifying, mitigating and managing the risk that a reporting entity may reasonably face that the provision of designated services at or through a permanent establishment of the reporting entity in Australia might (whether inadvertently or otherwise) involve or facilitate ML/TF (section 84(2)(a) of the AML/CTF Act); and

b. complied with such requirements as were specified in the AML/CTF Rules (section 84(2)(c) of the AML/CTF Act).

D.1.2 The Part A Program's primary purpose of identifying, mitigating and managing ML/TF risk

79 SCA accepts that the Part A Program of a reporting entity the nature, size and complexity of SCA will not have the primary purpose of identifying, mitigating and managing the ML/TF risk that the reporting entity may reasonably face, within the meaning of section 84(2)(a) of the AML/CTF Act, if the Part A Program:

a. does not expressly refer to or incorporate a written ML/TF risk assessment methodology that is capable of appropriately identifying and assessing the ML/TF risk of all designated services provided by the reporting entity;

b. is not aligned to the ML/TF risk reasonably faced by the reporting entity;

c. does not include or establish an appropriate framework for approval and oversight by Board and senior management; and

d. does not include appropriate risk-based systems and controls that are capable (as a matter of system or control design) of identifying, mitigating and managing ML/TF risk, consistent with risk appetite.[12]

D.1.3 The requirements of the AML/CTF Rules relating to Part A Programs

80 With respect to paragraph 78b, the relevant AML/CTF Rules included, but were not limited to (as summarised):

[12] See paragraphs 20-21 for an explanation of appropriate risk-based procedures, systems and controls.

a. paragraph 8.1.3, which provided that, some of the requirements specified in the AML/CTF Rules may be complied with by a reporting entity putting in place appropriate risk-based systems or controls. When determining and putting in place appropriate risk-based systems or controls, a Part A Program must have regard to the following factors in relation to the reporting entity:

    i. the nature, size and complexity of business; and

    ii. the type of ML/TF risk that might reasonably be faced;

b. paragraph 8.1.4, which provided that, for the purposes of the relevant AML/CTF Rules, in identifying the ML/TF risk, a Part A Program must take account of the risk posed by the following factors in relation to the reporting entity:

    i. the customer types, including any PEPs;

    ii. the types of designated services provided;

    iii. the methods by which designated services are delivered; and

    iv. the foreign jurisdictions dealt with;

    (collectively, the **Four Risk Factors**)

c. paragraph 8.1.5, which provided that a Part A Program must be designed to enable the reporting entity to:

    i. understand the nature and purpose of the business relationship with its customer types, including, as appropriate, the collection of information relevant to that understanding;

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

    iii. identify significant changes in ML/TF risk for the purposes of its AML/CTF program (Part A and Part B), including:

        A. risks identified by consideration of the factors in paragraph 8.1.4 (see sub-paragraph b); and

        B. risks arising from changes in the nature of the business relationship, control structure or beneficial ownership of its customers; and

    iv. recognise such changes in ML/TF risk for the purposes of the requirements of its AML/CTF program (Part A and Part B); 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. part 8.2, which provided that a Part A Program must include an AML/CTF risk awareness training program that satisfies the requirements in part 8.2;

e. part 8.4, which provided that a Part A Program must be approved by and subject to the ongoing oversight of the reporting entity's governing board and senior management;

f. paragraph 8.5.1, which provided that a Part A Program must provide for the reporting entity to designate a person as the 'AML/CTF Compliance Officer' (AMLCO) at management level;

g. part 8.6, which provided that a Part A Program must be subject to regular independent review;

h. part 8.7, which provided that a reporting entity must take into account any applicable guidance material disseminated or published by AUSTRAC and any feedback provided by AUSTRAC in respect of the relevant reporting entity or the industry it operates in that is relevant to the identification, mitigation and management of ML/TF risk;

i. paragraph 8.9.1(2), which provided that a Part A Program must include appropriate systems and controls designed to ensure compliance with the reporting entity's reporting obligations under section 41 (relating to SMRs), section 43 (relating to TTRs) and section 45 (relating to IFTIs) of the AML/CTF Act;

j. paragraph 15.2, which provided that a Part A Program must include appropriate risk-based systems and controls to enable the reporting entity to determine in what circumstances further KYC information or beneficial owner information should be collected or verified, to enable the review and update of KYC information and beneficial owner information for OCDD purposes;

k. paragraph 15.3, which required a reporting entity to undertake reasonable measures to keep, update and review the documents, data or information collected under the applicable customer identification procedure (**ACIP**) (particularly in relation to high risk customers) and the beneficial owner identification requirements specified in Chapter 4 of the AML/CTF Rules;

l. paragraphs 15.4 to 15.7, which provided that a Part A Program must include a TMP that:

    i. included appropriate risk-based systems and controls to monitor the transactions of customers;

    ii. had the purpose of identifying, having regard to ML/TF risk, any transaction that appeared to be suspicious within the terms of section 41 of the AML/CTF Act; and

    iii. had regard to complex, unusual large transactions and unusual patterns of transactions which had no apparent economic or visible lawful purpose;

m. paragraphs 15.8 and 15.9, which provided that a Part A Program must include an enhanced customer due diligence program (**ECDD Program**), which was to be applied by the reporting entity (subject to paragraph 4.4.18 of the AML/CTF Rules) when:

    i. it determined under its risk-based systems and controls that the ML/TF risk was high;

ii. a designated service was being provided to a customer who was or who had a beneficial owner who was a foreign PEP;

iii. a suspicion had arisen for the purposes of section 41 of the AML/CTF Act; or

iv. the reporting entity was entering into or proposing to enter into a transaction and a party to the transaction was physically present in, or was a corporation incorporated in, a prescribed foreign country;

n. paragraph 15.10, which provided that the ECDD Program must include appropriate risk-based systems and controls so that, in cases where one or more of the circumstances in paragraph 15.9 arose, the reporting entity would undertake measures appropriate to those circumstances, including, but not limited to:

i. undertaking more detailed analysis of the customer's KYC information and beneficial owner information, including, where appropriate, taking reasonable measures to identify the customer and each beneficial owner's source of wealth and source of funds; and

ii. seeking senior management approval for continuing a business relationship with the customer and for whether a designated service should continue to be provided to the customer; and

o. paragraph 15.11, which provided that where the customer was a foreign PEP, or had a beneficial owner who was a foreign PEP, the measures at sub-paragraph n must be undertaken, at a minimum.

D.1.4 The requirements of the AML/CTF Rules relating to Part B Programs

81 Throughout the Relevant Period, section 84(3) of the AML/CTF Act defined Part B of a standard AML/CTF program (**Part B Program**) as a part which:

a. had the sole or primary purpose of setting out the customer identification procedures applicable to customers of the reporting entity; and

b. complied with any such requirements as specified in the AML/CTF Rules.

82 With respect to paragraph 81b, the relevant AML/CTF Rules included, but were not limited to (as summarised):

a. paragraph 4.1.3, which provided that, in identifying its ML/TF risk, a reporting entity must consider the risk posed by its customer types, its customers' sources of funds and wealth, the nature and purpose of the business relationship with its customers, including as appropriate the collection of information relevant to that consideration, the control structure of non-individual customers, the types of designated services it provides, the methods by which it delivers designated services and the foreign jurisdictions with which it deals;

b. paragraph 4.2.2, which provided that an AML/CTF program must include appropriate risk-based systems and controls that were designed to enable the reporting entity to be reasonably satisfied, where a customer was an individual, that the customer was the individual that he or she claimed to be;

c. paragraph 4.2.3, which provided that an AML/CTF program must include a procedure for the reporting entity to collect, at a minimum, the name, date of birth and residential address of a customer that was an individual (**minimum KYC information**);

d. paragraph 4.2.5, which provided that an AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine whether, in addition to the KYC information referred to in paragraphs 4.2.3 or 4.2.4, any other KYC information would be collected about a customer;

e. paragraph 4.2.6, which provided that an AML/CTF program must include a procedure for the reporting entity to verify, at a minimum, a customer's full name, and either the customer's date of birth or residential address;

f. paragraph 4.2.8, which provided that an AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine whether, in addition to the KYC information referred to in paragraph 4.2.6, any other KYC information collected about a customer should be verified from reliable and independent documentation, reliable and independent electronic data or a combination of the two;

g. paragraphs 4.11.1 to 4.11.4, which provided requirements relating to the collection and verification of documents and information in circumstances where an agent is acting on behalf of a customer that is an individual; and

h. paragraphs 4.13.1 to 4.13.4, which provided requirements related to PEPs.

D.1.5 Exemption under Chapter 10 of the AML/CTF Rules

83 Throughout the Relevant Period, Chapter 10 of the AML/CTF Rules provided certain exemptions to casinos in relation to obtaining and verifying KYC information about a customer. This included, at paragraphs 10.1.3 to 10.1.7, exemptions for SCA as a casino, in certain circumstances, from the collection, verification and recording of particular customer identification information in relation to the provision of certain table 3, section 6 of the AML/CTF Act designated services.

E. SCA'S AML/CTF PROGRAMS

84 Between 7 December 2016 and 17 November 2022, SCA had in place a standard AML/CTF Program, which comprised a document titled 'SkyCity Adelaide AML/CTF Program'. Each AML/CTF Program included a Part A and a Part B. The AML/CTF Program was updated over time and relevantly comprised the following versions:

a. Version 15, effective from 9 February 2015 to 6 February 2017, comprising the **2015 Standard Part A Program** (sections 1 to 19) and the **2015 Standard Part B Program** (sections 20 to 25);

b. a version identified as 'February 2017', comprising the **2017 Standard Part A Program** (sections 1 to 15) effective from 7 February 2017 to 6 February 2018, and the **2017 Standard Part B Program** (sections 16 to 20) effective from 7 February 2017 to 18 June 2017;

c. an amended version of the 2017 Standard Part B Program with a revised section 19 being the 'Amended February 2017' version, effective from 19 June 2017 to 6 February 2018 (**Amended 2017 Standard Part B Program**);

d. a version identified as 'February 2018', effective from 7 February 2018 to 16 April 2019, comprising the **2018 Standard Part A Program** (sections 1 to 15) and the **2018 Standard Part B Program** (sections 16 to 20);

e. a version identified as 'April 2019', effective from 17 April 2019 to 15 February 2021, comprising the **2019 Standard Part A Program** (sections 1 to 15) and the **2019 Standard Part B Program** (sections 16 to 20);

f. a version identified as 'February 2021', effective from 16 February 2021 to 8 June 2021, comprising the **February 2021 Standard Part A Program** (sections 1 to 15) and the **February 2021 Standard Part B Program** (sections 16 to 20);

g. a version identified as 'June 2021', effective from 9 June 2021 to 27 October 2021, comprising the **June 2021 Standard Part A Program** (sections 1 to 15) and the **June 2021 Standard Part B Program** (sections 16 to 20); and

h. a version identified as 'October 2021', effective from 28 October 2021 to 17 November 2022, comprising the **October 2021 Standard Part A Program** (sections 1 to 15) and the **October 2021 Standard Part B Program** (sections 16 to 20).

85 For the purpose of this SAFA, the following defined terms are adopted:

a. the **Standard Part A Programs** comprise the 2015 Standard Part A Program, 2017 Standard Part A Program, 2018 Standard Part A Program, 2019 Standard Part A Program, February 2021 Standard Part A Program, June 2021 Standard Part A Program, and October 2021 Standard Part A Program;

b. the **Standard Part B Programs** comprise the 2015 Standard Part B Program, 2017 Standard Part B Program, Amended 2017 Standard Part B Program, 2018 Standard Part B Program, 2019 Standard Part B Program, February 2021 Standard Part B Program, June 2021 Standard Part B Program, and October 2021 Standard Part B Program; and

c. SCA's **Standard AML/CTF Program** was comprised of the Standard Part A Programs and Standard Part B Programs.

F. SCA'S CONTRAVENTIONS OF SECTION 81 OF THE AML/CTF ACT

F.1 Risk Assessments

F.1.1 SCA's obligations in relation to identifying ML/TF risk

86 Risk assessments are the foundation of compliance with the obligation for reporting entities to identify, mitigate and manage the ML/TF risk relating to the provision of designated services. Risk assessments must be reviewed and updated as ML/TF risk emerges, evolves and changes.

87 A standard Part A program will not satisfy the requirements of the AML/CTF Act, having regard to the AML/CTF Rules, described in Section D.1.2, if it:

a. does not expressly refer to or incorporate a written ML/TF risk assessment methodology that is capable of appropriately identifying and assessing the ML/TF risk of all designated services provided by the reporting entity;

b. is not based on, and is not aligned to the assessment of ML/TF risk reasonably faced by the reporting entity; and

c. does not include all appropriate risk-based systems and controls necessary to ensure that the Part A program is capable of identifying, mitigating and managing all ML/TF risk reasonably faced by the reporting entity.

88 The Four Risk Factors a reporting entity must consider for the purposes of considering ML/TF risk in the AML/CTF Rules are set out at paragraph 80b.

89 SCA accepts that:

a. although SCA made assessments of ML/TF risk during the Relevant Period, its Standard Part A Programs did not expressly refer to or incorporate a written ML/TF risk methodology;

b. for the reasons outlined below at paragraphs 97, 106 to 109, 111 to 112, 115 to 116, 118 to 119, 131 and 134 to 135, SCA's Standard Part A Programs were not sufficiently aligned with all ML/TF risk reasonably faced by SCA; and

c. for the reasons outlined below at paragraphs 228 to 234, SCA's Standard Part A Programs did not include all appropriate risk-based systems and controls necessary to ensure that the Part A Program was capable of identifying, mitigating and managing all ML/TF risk reasonably faced by the reporting entity.

90 As a result, the Standard Part A Programs during the Relevant Period were not sufficiently aligned to the ML/TF risk reasonably faced by SCA and were not capable (as a matter of control or systems design) of identifying, mitigating and managing these risks contrary to the primary purpose obligation in section 84(2)(a) of the AML/CTF Act. The reasons are set out at Sections F.1 and F.3.

91 SCA also accepts that the matters at paragraphs 89a to 89c were factors that contributed to contraventions of paragraphs 8.1.3, 8.1.4, 8.1.5(1), 8.1.5(3), 8.1.5(4) and 8.1.5(5) of the AML/CTF Rules and section 84(2)(c) of the AML/CTF Act.

F.1.1.1 Risk Assessments

92 Prior to the Relevant Period, when the AML/CTF legislative regime commenced in 2007, SCA engaged and instructed a third party consultant to conduct its initial ML/TF risk assessment, dated October 2007 (**2007 Risk Assessment**). Amongst other things, the 2007 Risk Assessment included an assessment of the Four Risk Factors.

93 Thereafter, between 2007 to 8 February 2015, each updated version of SCA's AML/CTF Program annexed the updated risk assessment or the previous risk assessment if SCA did not consider any update to its risk assessment was required.

94 From 7 December 2016 to November 2022, SCA's ML/TF risk assessments were included or incorporated into the Standard Part A Programs. They were contained in:

a. 9 February 2015 to 6 February 2017 – Appendix B to the 2015 Standard Part A Program (the **2014 Risk Assessment**);

b. 7 February 2017 to 16 November 2022 – Section 3, Schedule 1 (Table of Risks) and Schedule 1A (Issues that may be relevant to ML/TF risk posed by changes to services deliver/technology and new designated services*)* of the 2017-2021 Standard Part A Programs (the **2017-2021 Risk Assessments**);

c. June 2017 – *AML Risk Assessment – Pitcam.* This was a separate ML/TF risk assessment conducted prior to the introduction of the Pitcam technology at the SCA casino to identify any associated ML/TF risk with the provision of designated services, in circumstances where the Pitcam technology was implemented (**Pitcam Risk Assessment**);

d. November 2017 – *2017 AML/CTF Risk Assessment Review – Changes to Delivery Methods, Technology and Services*. This was a separate ML/TF risk assessment conducted to identify changes to ML/TF risk in the previous 12 months to service delivery, technology and designated services that could have AML/CTF implications. It included an assessment of the inherent and residual risk of human resources,

surveillance, ICT frameworks, gaming operations, cash handling, VIP services, food and beverage, international business, and the Premier Rewards customer loyalty program (**2017 Risk Assessment Review**);

e. January 2020 – *Schedule 1 Template.* This was a separate document that was marked as a draft and that set out SCA's identified 'Risk Characteristics' and 'Risk Question', and then recorded whether the risk was present (Yes, No or N/A). This analysis then generated a qualitative risk rating, represented as a percentage, which was then used to conduct an 'overall analysis' of the inherent risk; and

f. October 2020 – *SkyCity Adelaide Money Laundering and Terrorism Financing Risk Assessment – Introduction of Ticket In Ticket Out (TITO) (Main Gaming Floor) and Bank Note Acceptors (**BNAs**)* – version 1.0 (**TITO/BNA Risk Assessment**). This was a separate risk assessment conducted prior to the introduction of TITO and BNA designated services on the main gaming floor at the SCA casino to identify the potential ML/TF risk that the new features posed to SCA,

(together, the **Risk Assessments**).

95 As set out further below at paragraph 122, in around May 2022 SCA introduced risk assessments for each relevant SCA business unit and an enterprise-wide risk assessment, which were conducted in accordance with a written ML/TF risk assessment methodology.

96 At all times, SCA's Standard Part A Programs recorded that SCA offered gaming and related services at multiple locations throughout the SCA complex, identified the average number of visitors per day to the casino, and the total number of table games and EGMs offered. The 2014 and 2017-2021 Risk Assessments stated that: "The volume, size and diversity of transactions at [SCA], its customer types and the fact that it delivers its products and services from multiple locations albeit from within a single venue, suggests that the overall inherent ML risk rating at SCA is medium." [13]

97 The completion of the Risk Assessments was not conducted in accordance with a written ML/TF risk methodology (as set out at paragraph 79a) that covered all inherent risks, adequately considered the Four Risk Factors or adequately assessed the residual risk of the ML/TF risk of designated services once risk-based controls had been applied. As a result, the Risk Assessments did not identify all ML/TF risk reasonably faced by the business, and the Standard Part A Programs were not sufficiently aligned to the ML/TF risk reasonably faced by SCA in contravention of section 84(2)(a) of the AML/CTF Act.

98 This contributed to SCA's contravention of paragraphs 8.1.3, 8.1.4, 8.1.5(1), 8.1.5(3), 8.1.5(4) and 8.1.5(5) of the AML/CTF Rules and the implementation of a Standard Part A Program which was contrary to section 84(2)(c) of the AML/CTF Act.

F.1.1.2 The Four Risk Factors and paragraph 8.1.5 of the Rules

Paragraph 8.1.4(1) – Assessment of customer risk, including PEPs

99 At all times throughout the Relevant Period, SCA's Risk Assessments (as applicable) assessed the ML/TF risk posed by certain customer types, including PEPs.

100 SCA's assessment of its customer risk in the 2014 Risk Assessment identified that individuals (separated into local and international customers) were predominantly "low value recreational gamers who present no ML/TF risk". It concluded that "[i]t would not be practical or reasonable to collect information in respect of every customer who visits the casino as a

[13] The language in the 2015 Standard Part A Program was framed slightly differently, being: "The volume size and diversity of transactions at SKYCITY Adelaide, its customer base and the fact that it delivers its products and services from multiple locations and channels (albeit from a single venue) means that the inherent ML risk at Adelaide is rated as medium".

means of evaluating the risk they may present from an ML/TF perspective". At all times, and unless required otherwise, during the Relevant Period SCA's Standard Part A Programs provided that its customers were to be given a default rating of 'low' risk.

101 SCA's Standard Part A Programs identified a number of factors, which, where present, indicated that there may be a potentially higher ML/TF risk in providing designated services to that customer. The factors identified by SCA as presenting higher ML/TF risk were set out in section 13 of the 2015 AML/CTF Program, and section 3 and Schedules 1 and 1A of the 2017-2021 AML/CTF Programs (**Risk Allocation Criteria**).

102 Under each Standard AML/CTF Program, a customer's risk profile was to be elevated to 'moderate', 'high', or 'significant', if, having regard to the Risk Allocation Criteria, the manner in which the customer used the designated services and any associated behaviour patterns through its transaction monitoring processes presented a higher ML/TF risk. For example, any customer whose primary residence was in a high risk jurisdiction or whose gaming patterns were not supported by their occupation (with no other reasonable explanation to support their level of turnover) was required to be accorded a high risk rating and was to be subject to ECDD.

103 In the 2014 Risk Assessment, the process described above at paragraph 102 was also to inform whether KYC information (or additional KYC information that was not required by default because of the customer type) should be obtained to facilitate a further review of the customer's ML/TF risk rating.

104 At all times, the AMLCO (or their delegate) or the AML/CTF Senior Management Group (under the 2015 Standard Part A Program only) was responsible for considering and allocating a risk rating of 'moderate', 'high' or 'significant' to customers under the Standard Part A Programs.

105 To further assist with identifying customers who posed a higher ML/TF risk, in around September 2019, SCA introduced the:

a. **'*High & Standard Risk Elevations*' SOP**: this SOP set out 11 'triggers' that would warrant an elevation of a customer's risk rating to high and three 'triggers' that would warrant an elevation of a customer's risk rating to 'significant'. These replicate the Risk Allocation Criteria that were included in SCA's 2017-2021 Standard Part A Programs.[14] The SOP also set out the procedure for recording the customer's elevated risk rating in Bally against the specific trigger (including tagging the rating to a specific narrative that noted the relevant trigger for the elevated risk-rating).

b. **'*High Risk Jurisdictions*' SOP**: this SOP set out the process for elevating the risk rating of customers from jurisdictions recognised as 'high' or 'monitored'. This was based on a 'High Risk Countries Report', which was generated monthly. For example, SCA required that any customers identified as being from a 'high' or 'monitored' jurisdiction who had attended SCA casino in the previous month were to be investigated, but did not provide appropriate guidance on how to carry out this process.

106 The Standard Part A Programs:

a. that included the Risk Allocation Criteria for categorising customers, did not appropriately describe all ML/TF risk that SCA might reasonably face with respect to all customer types;

[14] With the only difference being that the February 2021 Standard Part A Program included an additional trigger for elevating a customer's rating to 'high', where the customer was a junket operator.

b. did not include documented guidance on the searches or checks to be performed by the AMLCO in considering a customer's risk rating, in particular, whether the customer may not have been low risk; and

c. did not include appropriate guidance or criteria on assessing the ML/TF risk of customers with respect to loans and remittance services for the purposes of considering whether a customer may not have been low risk.

107 The Standard Part A Programs also did not:

a. include appropriate procedures or guidance to identify and escalate customers who may not have been low risk because of the matters outlined at paragraphs 343b (with respect to credit risk assessments) and 319a (with respect to its TMP);

b. include adequate screening procedures to identify PEPs, as the procedures in place were not capable of consistently identifying and escalating PEPs to the AML team for an assessment of their risk rating (as described further below at paragraphs 383 to 384 and 393);

c. include or incorporate appropriate risk-based procedures to collect and assess information about source of wealth or source of funds information (as set out further below at paragraph 343i). In the absence of such a requirement, SCA was unable to understand the risk posed by certain customers;

d. prior to 12 May 2022, 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; and

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

108 In 2018 an external review identified that the process to record and elevate a customer's risk rating was manual, prone to error and that it was difficult to establish a reliable audit trail in the risk rating recording process. SCA's own documents noted that the limitations with the system included a lack of auditability of when and by whom a customer's risk rating was changed and an ability to record a risk rating comment.

109 As a result, during the Relevant Period, SCA's Standard Part A Programs were not sufficiently aligned to all the ML/TF risk posed by its customers, and as a result SCA's systems and controls were insufficient due to the lack of risk identification.

Assessment of designated services

110 SCA's assessments of its ML/TF risk associated with the provision of designated services were set out as follows:

a. The 2014 and 2017-2021 Risk Assessments identified a list of table 3, section 6 of the AML/CTF Act designated services provided by SCA. The Risk Assessments did not identify table 1, section 6 of the AML/CTF Act designated services provided by SCA. The 2014 Risk Assessment stated that these designated services "are standard across casinos and are primarily designed to facilitate the use of the casino's gaming products, namely table gaming and gaming machines". The 2017-2021 Risk Assessments stated the "major distinguishing characteristics associated with the different games include the mathematical advantage to the house; maximum wagering

limits; the wagering options available to players (in particular balanced betting wagering options) and the level of action the game is likely to attract".

b. The 2014 Risk Assessment identified some ML/TF risk associated with the provision of the following categories of designated services:

i. **account related** – "Casino account activity which has no linkage to gambling or otherwise shows an unusual pattern may suggest a customer is using an account for layering or refinement purposes to cloud the origin of illegal funds";

ii. **currency exchange** – "Currency exchange services may potentially be used to refine illegal funds to disguise their origin";

iii. **use of CVIs** – "[CVIs] such as chips, gaming machine cancelled credits, gaming machine tickets and credits for cashless cards may be purchased and cashed out with little or no gaming in an effort to refine funds and disguise their true origin. Casino chips or other instruments may potentially be used as currency in illegal transactions"; and

iv. **use of gambling products** – "Some gambling products have the potential to be used to generate 'winnings' which are not genuine, and which ultimately may disguise the origin of the funds use[d] to generate those winnings".

c. Attachment 1 to the 2014 Risk Assessment identified some possible methods through which customers could potentially exploit the designated services provided to them by SCA. The attachment set out some indicators of these ML/TF risks, as well as corresponding controls.

d. The 2017-2021 Risk Assessments identified six categories of ML/TF risk associated with the provision of these designated services, which reflected the categories identified above at subparagraph-b as well as "sudden spikes or unusual patterns in the use of gambling products".

111 Notwithstanding the matters set out at paragraph 110, the assessments SCA conducted of its ML/TF risk from 7 December 2016 to 17 November 2022 did not assess all the ML/TF risk reasonably faced by SCA with respect to each designated service it provided. For instance:

a. SCA did not undertake any ML/TF risk assessments in respect of the provision of designated services described at items 6, 7, 31, and 32, table 1, section 6 of the AML/CTF Act; and

b. SCA did not sufficiently assess the ML/TF risk of the provision of items 6 and 9, table 3, section 6 of the AML/CTF Act designated services.

112 By not conducting an ML/TF risk assessment of each designated service it provided, SCA also did not appropriately identify and assess each specific ML/TF typology or vulnerability associated with every designated service it provided to its customers (as set out in Schedule 1). This contributed to a contravention of paragraph 8.1.4(2) of the AML/CTF Rules (and therefore section 84(2)(c) of the AML/CTF Act) and to SCA's Standard Part A Programs not being sufficiently aligned with the ML/TF risk reasonably faced by SCA (as required by section 84(2)(a) of the AML/CTF Act).

Assessment of methods and channels by which SCA provided designated services

113 The 2014 Risk Assessment identified that SCA provided the majority of its designated services face-to-face to its customers, and that its designated services were provided by licensed casino employees. SCA also provided certain designated services to customers that were not face-to-face. The provision of non-face-to-face designated services was not

recognised in SCA's Standard Part A Programs, except for the reference in the 2015 Standard Part A Program with respect to the SCA Customer account channel, as described below at paragraph 115b.

114 The 2017-2021 Risk Assessments also identified that customers structuring transactions at different locations within the casino to avoid identification and reporting requirements was particularly relevant to the ML/TF risk posed by the delivery of SCA's designated services. If a customer was suspected of this, they were to be accorded a high risk.

115 SCA accepts that it did not assess all of the ML/TF risk it reasonably faced with respect to each method or channel. In particular:

a. the Risk Assessments did not assess the specific ML/TF risk associated with providing designated services through the channel of junkets, through the SCA Customer and SCEG Customer account channels, through the SkyCity New Zealand channel, through VIP gaming rooms or through EZYPlay Guest Cards; and

b. aside from the 2015 Standard Part A Program which recognised that designated services provided through the SCA Customer account channel could be facilitated when the customer was not physically present at the SCA casino, the Standard Part A Programs did not, up until November 2022, otherwise recognise that certain designated services provided by SCA were not provided face-to-face, including transactions through the SCEG Customer account channel, some CCF transactions and designated services provided through EGMs, automated table games (**ATGs**) and cash redemption terminals (**CRTs**). As such, the Standard Part A Programs did not identify the specific ML/TF risk associated with providing designated services through non-face-to-face channels.

116 By not identifying all ML/TF risk specifically associated with each method and channel through which designated services could be provided, SCA's Standard Part A Programs were not sufficiently aligned to the ML/TF risk reasonably faced by SCA (as required by section 84(2)(a) of the AML/CTF Act).

Assessment of foreign jurisdictional risk

117 The 2014 Risk Assessment identified ways in which dealings with foreign jurisdictions could arise from the designated services provided by SCA, namely:

a. transfers through channels based in a foreign jurisdiction. Although SCA did not provide designated services from a permanent establishment in a foreign country, the SCEG Group entities operated foreign holding accounts in Singapore, Hong Kong and Malaysia, and these foreign holding accounts could be used to facilitate deposits into and withdrawals from a customer's FMA at the SCA casino. Funds could also be deposited into a customer's FMA at the SCA casino from SCEG New Zealand casinos via an inter-company journal entry. Singapore, Hong Kong and Malaysia were not featured on the Financial Action Task Force's (**FATF**) list of uncooperative nations or nations seen as AML deficient, which was used as the primary reference point in determining the suitability of jurisdictions in which it could operate a foreign holding account; and

b. international customers visiting from overseas jurisdictions, where a customer's country of origin may be a relevant consideration to the ML/TF risk that they posed.

118 The 2017-2021 Risk Assessments (at section 3 of each of the relevant AML/CTF Programs) did not set out a comprehensive analysis of foreign jurisdictional risk. However, there were certain parts of the 2017-2021 Standard Part A Programs that reflected some consideration of jurisdiction risk had been considered. For example, the Risk Allocation Criteria provided that a customer was to be rated 'high risk by default where they resided in a high risk

jurisdiction or 'significant' risk where they resided in a high risk jurisdiction and spent over $100,000. However, it was not until SCA introduced the 'High Risk Jurisdictions' SOP in September 2019 (as described at paragraph 105b above) that SCA provided operational guidance with respect to which countries SCA considered posed a higher ML/TF risk to SCA.

119 SCA did not appropriately identify all of the ways in which jurisdictional risk could arise with respect to customer risk, designated services risk and channel risk. In particular:

a. the 2015 and 2017-2021 Standard Part A Programs did not incorporate an overall assessment of SCA's jurisdictional risk, despite the number of international customers and the volume of funds received from overseas;

b. the 2015 and 2017-2021 Standard Part A Programs did not identify all foreign jurisdictions with which SCA dealt, indicating that SCA did not sufficiently identify the associated ML/TF risk, including those that may have arisen from foreign jurisdictions from which it accepted transfers of money;

c. in around September 2019, SCA introduced the 'High Risk Jurisdictions' SOP, providing for jurisdiction to be considered (once known) by utilising recognised lists published by relevant government authorities. The SOP did not include an appropriate methodology to identify, mitigate or manage the risks of a customer who was identified as being from a high risk jurisdiction;

d. the 2015 and 2017-2021 Standard Part A Programs did not identify how jurisdictional risks were factored into the assessment of the ML/TF risk of designated services or channels. For example, the jurisdictional risks of international payment channels were not appropriately considered; and

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

Controls

120 As set out in Section F.3 of this SAFA, SCA put in place certain systems and controls which sought to identify, mitigate and manage the identified ML/TF risk. However, given SCA's assessment of its ML/TF risk was not based on a written ML/TF risk assessment methodology until May 2022, and given the absence of an appropriate risk assessment, SCA's controls were not sufficiently aligned to the ML/TF risk faced by SCA (see paragraphs 97, 106 to 109, 111 to 112, 115 to 116, 118 to 119, 131 and 134 to 135 in relation to the deficiencies). Further, the Risk Assessments did not sufficiently consider all of the ML/TF risk posed, having regard to the nature, size and complexity of the SCA casino business, by the designated services it provided to its customers, the types of designated services it provided and the channels or the foreign jurisdictions with which it was dealing through the provision of designated services.

October 2021 and November 2022 AML/CTF Program

121 In or around December 2021, following the work completed by an external AML consultancy, who produced an independent report that assessed SCA's AML/CTF Program and compliance, SCA engaged this external consultancy further, to support SCA to develop a revised ML/TF risk assessment methodology and to conduct an updated ML/TF risk assessment as part of the AML Enhancement Programme. In 2022, SCA introduced the *SkyCity Adelaide Business Unit and Enterprise ML/TF Risk Assessment Methodology V1.0* (**2022 ML/TF Risk Assessment Methodology**).

122 In or around May 2022, SCA introduced risk assessments for each relevant SCA business unit, namely, the Cage, EGMs, Loyalty Rewards, the Player Programs and Table Games

(the **2022 BURAs**) and an enterprise-wide risk assessment (**2022 EWRA**), together the **2022 Risk Assessments**.

123 The 2022 ML/TF Risk Assessment Methodology:

a. described its purpose as to set the standards against which SCA assessed the vulnerability to ML/TF risk of relevant sections of its business, including establishing a consistent approach to, and basis for, the identification, assessment and rating of the ML/TF risk reasonably faced by SCA's business units;

b. states that it considers the impact of SCA's operating model as a casino on its ML/TF risk, noting that the nature of casinos is distinct from other reporting entities;

c. states that the identification, mitigation and management of ML/TF risk is to be undertaken by:

i. identifying the inherent ML/TF risk reasonably faced by SCA, having regard to the Four Risk Factors;

ii. mitigating the inherent ML/TF risk that is identified by relevant AML/CTF systems and controls; and

iii. managing the residual ML/TF risk identified after relevant AML/CTF systems and controls have been applied to the inherent ML/TF risk and to ensure the residual ML/TF risk is within SCA's risk appetite; and

d. outlines that the business unit risk assessments required an assessment of the inherent ML/TF risk in each relevant business unit, the effectiveness of the AML/CTF controls that were designed and implemented to mitigate and manage the inherent ML/TF risk, an assessment of the level of remaining residual ML/TF risk and ongoing management of changes to ML/TF risk.

124 From November 2022, following the introduction of the 2022 ML/TF Risk Assessment Methodology in May 2022, SCA expressly referred to a documented ML/TF risk methodology in its Standard AML/CTF Programs.

125 In December 2022, Standards and SOPs were also designed and introduced to support SCA's ML/TF risk assessment process (see Section F.10 for more detail).

126 SCA accepts that it did not have a sufficient basis to conclude that the controls under the October 2021 or November 2022 Standard Part A Programs were aligned to the 2022 Risk Assessments until 14 December 2022, at which time all supporting Standards were approved by SCA's AML/CTF Senior Management Group.

F.1.1.3 Identification and assessment of significant changes in ML/TF risk and changing ML/TF risk

127 Throughout the Relevant Period, the Standard Part A Programs included some systems and controls intended to identify significant changes in SCA's ML/TF risk and emerging risks in accordance with paragraphs 8.1.5(3) and 8.1.5(4) of the AML/CTF Rules:

a. between February 2015 and February 2017, the 2014 Risk Assessment provided for SCA to review and update its ML/TF risk assessment from "time to time", having regard to material changes to SCA's operating environment, new AUSTRAC typology reports, new FATF reports relevant to casinos in the Asia Pacific area, AUSTRAC guidance, and other matters that SCA considered appropriate;

b. from April 2019 to 17 November 2022, the requirement in the 2017-2021 Standard Part A Programs for (i) the ML/TF risk assessment to be subject to a formal review process every two years; and (ii) SCA to review any typology reports or feedback from AUSTRAC and SCA's own intelligence gathering and audit process to determine whether changes to the ML/TF risk assessment may be necessary from time to time; and

c. the 2022 ML/TF Risk Assessment Methodology which required SCA to "regularly review and reperform the BURA and EWRA risk assessments to identify changes in the ML/TF risk over time".

128 At all times during the Relevant Period, the AMLCO was responsible for reviewing and responding to findings of audits of the Standard Part A Programs and proposing appropriate revisions, ensuring that any new games, services or procedures relating to a designated service had been assessed for risk and reporting any material issues relating to the discharge of SCA's AML obligations to the General Manager Adelaide and the Group General Counsel, AML/CTF Senior Management Group or SCA Board (as applicable under each Program). In the 2015 Standard Part A Program, the AML/CTF Senior Management Group was known as the AML Committee. From the February 2021 Standard Part A Program, the AML/CTF Senior Management Group was known as the AML/CTF Committee. A reference to the AML/CTF Senior Management Group in the SAFA includes the AML Committee and the AML/CTF Committee, as applicable. The AML/CTF Senior Management Group was a group of SCA senior staff from relevant departments.

129 The AML team supported the AMLCO in discharging their obligations. The AML team could escalate any concerns or issues with the AMLCO, as appropriate. Notwithstanding this, the Standard Part A Programs did not include procedures identifying how new ML/TF risk information and intelligence should be escalated and to whom, or when a review of SCA's ML/TF risk assessment should be triggered.

130 The AML/CTF Senior Management Group was required to oversee and manage the ongoing identification and assessment of changing and emerging ML/TF risk. One of the regular agenda items of the AML/CTF Senior Management Group was to consider game changes, new games, and material events.

131 As the Standard Part A Programs did not expressly refer to or incorporate a written ML/TF risk assessment methodology, SCA accepts that emerging or changing ML/TF risk was not capable of being consistently assessed and re-assessed over time. This contributed to SCA's contravention of paragraphs 8.1.5(3) and 8.1.5(4) of the AML/CTF Rules. It also meant that the Standard Part A Programs were not sufficiently aligned to the risks reasonably faced by SCA, as required by section 84(2)(a) of the AML/CTF Act. Specifically:

a. as the Risk Assessments did not include some of the key ML/TF risk reasonably faced by SCA with respect to all designated services (see paragraphs 111 and 112 above), the reviews were not capable of identifying significant changes in those ML/TF risks or recognising such changes for the purposes of the Standard Part A and Standard Part B Programs; and

b. the Standard Part A Programs did not include risk-based procedures for SCA to consistently identify, assess and report to senior management, ML/TF risk, trends arising from, or disclosed by, the provision of designated services or channels, transaction monitoring, suspicious matter reporting, internal financial crime reporting, information from AUSTRAC and law enforcement or the external ML/TF risk environment.

Risk assessments of new designated services, channels and technologies

132 The Standard Part A Programs required SCA to conduct ML/TF risk assessments of all new designated services, new methods of designated service delivery (channels) and developing technologies prior to their introduction. The Standard Part A Programs provided some guidance on SCA's approach to considering any ML/TF risk arising from new designated services, new channels and new or developing technologies.

133 However, it was not until the introduction of the 2022 ML/TF Risk Assessment Methodology that SCA set out procedural requirements for identifying and assessing ML/TF risk with respect to new designated services, new channels through which designated services may be provided and new technology. This was further uplifted with the implementation of the '*FC – Perform Product and/or Service Risk Assessment'* SOP in May 2023, which set out the procedural steps by which ML/TF risk assessments on gaming produces and services were required to be carried out and which forms part of the November 2022 AML/CTF Program.

134 During the Relevant Period, SCA did not, at all times, appropriately identify all ML/TF risk associated with new designated services, new channels and new technologies (or changes to existing designated services, channels or technologies) prior to the implementation of the change.

135 Until May 2022, in the absence of clear written guidance outlining what might constitute a new designated service, a new channel or a developing technology warranting a risk assessment, or identifying a procedure outlining how any such ML/TF risk assessment should be conducted, not all new designated services, new channels and developing technologies were risk assessed (for example, the provision of designated services through the Horizon Tourism account, see paragraph 184g, was not risk assessed prior to its implementation) and those which were (for example, the Pitcam Risk Assessment and the TITO/BNA Risk Assessment) were inconsistently risk assessed. This contributed to SCA's contravention of paragraph 8.1.5(5) of the AML/CTF Rules, and resulted in the Standard Part A Programs not being sufficiently aligned with the ML/TF risk reasonably faced by SCA, as required by section 84(2)(a) of the AML/CTF Act.

2022 Risk Assessment Methodology, BURAs and EWRA

136 SCA accepts that, between May 2022 and 14 December 2022, the October 2021 and November 2022 AML/CTF Programs were not appropriately aligned to the 2022 Risk Assessments, as the systems and controls that had been designed to mitigate and manage the ML/TF risk identified had not been completed or approved at this time.

F.2 Board and senior management oversight

F.2.1 Relevant legal obligations in relation to board and senior management oversight

137 At all times during the Relevant Period, paragraph 8.4.1 of the AML/CTF Rules required that a reporting entity's standard Part A program be:

a. approved by a reporting entity's governing board and senior management (or, in circumstances where the reporting entity does not have a board, approved by its chief executive officer or equivalent); and

b. subject to the ongoing oversight of the reporting entity's board and senior management (or, in circumstances where the reporting entity does not have a board, overseen by its chief executive officer or equivalent).

138 A reporting entity of the nature, size and complexity of SCA, having regard to the ML/TF risk it faces, cannot adopt and maintain a Part A Program that has the primary purpose within the meaning of section 84(2)(a) of the AML/CTF Act of identifying, mitigating and managing

ML/TF risk reasonably faced with respect to the provision of designated services if its Part A Program does not establish an appropriate framework for approval and oversight by the board and senior management.

F.2.2 Board and senior management approval of the Standard Part A Programs

139 As described at Section E, SCA adopted and implemented Part A Programs during the Relevant Period, being the Standard Part A Programs identified at paragraph 84.

140 Between 7 December 2016 and 27 October 2021:

a. each version of SCA's Standard AML/CTF Program was authored and approved by the Group General Manager Regulatory Affairs and AML and/or the SCA General Manager Legal Compliance and Regulatory Affairs (who was also SCA's AMLCO); and

b. each of the Standard Part A Programs was approved by the Audit and Financial Risk Committee (**AFRC**) and/or the SCEG Board.

141 All Standard Part A Programs identified the responsible entity for approving any new iteration to the Standard Part A Programs.[15]

142 During the Relevant Period, SCEG and SCA were signatories to a Management Services Agreement dated 2013 and a Master Services Agreement for Services, dated 1 July 2018 (together, the **MSAs**). Pursuant to the MSAs, and until at least 28 October 2021 (when SCA amended its AML/CTF Program as set out at paragraph 84h), SCEG provided SCA with management services that included assisting SCA with its regulatory compliance and corporate governance requirements. The MSAs stated that SCEG had the expertise to provide the relevant services.

F.2.3 Board and senior management oversight of the Standard Part A Programs

143 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. The October 2021 Standard Part A Program provided that the AML/CTF Senior Management Group, the SCA Board and, (on an advisory basis) the Audit and Risk Committee were to have oversight of the Standard Part A Programs. However, for the reasons set out at paragraphs 148 and 149, in the absence of an adequate oversight framework, the Board and senior management did not consistently have oversight of the Standard Part A Programs (see paragraphs 150 and 151).

144 Each of the 2015-October 2021 Standard Part A Programs set out how the Part A Program was to be overseen. The 2015-June 2021 Standard Part A Programs established reporting lines through the roles of the AMLCO, the General Manager and the Company Secretary, which included reporting on any matters concerning implementation of and any performance issues relating to the Standard Part A Programs at scheduled AML/CTF Senior Management Group meetings and to the AFRC for consideration. The roles and reporting responsibilities of each of those roles were set out in sections 3, 8 and 9 and Appendix B of the 2015 Standard Part A Program and in sections 3, 6, 7, 9, 11 and 14 of the 2017-June 2021 Standard Part A Programs.

145 The October 2021 Standard Part A Program provided for the same process, except the SCA Board and the AML/CTF Senior Management Group were to be assisted by the AMLCO.

[15] Between 7 December 2016 to February 2017, SCA's 2015 Standard Part A Program provided that the Audit and Financial Risk Committee (AFRC), later known as the Audit and Risk Committee (ARC) – a sub-committee of the Board of Directors of SCEG - shall approve any amendments to SCA's Part A Program. At various times, the February 2017- June 2021 Standard Part A Programs provided that the SCEG Board or the AFRC and the AML/CTF Senior Management Group (later known as the AML/CTF Committee or AML Committee) shall approve any amendments to the Standard Part A Program.

Sections 3, 4, 6, 7, 9, 11, 13, 14 and 18 of the October 2021 Standard Part A and Part B Program set out the responsibilities of the AMLCO.

146 Other senior management roles in SCA also had responsibility for reporting to the Board, AFRC and AML/CTF Senior Management Group on AML/CTF compliance and to assist SCA in the discharge of its AML obligations. For example, the Standard Part A Programs required any risk assessments associated with new games, services or procedures relating to a "designated service" be reported to the AML/CTF Senior Management Group (prior to implementation, until October 2021).

147 In addition to the above, oversight of the Standard Part A Programs was supported by the following processes documented in the Standard Part A Programs:

a. receipt and review of reports by the AML/CTF Senior Management Group (typically reporting every three months) and the AFRC (typically four reports per year) or SCA Board (quarterly reports), related to the implementation of the program;

b. receipt of reports of the results of transaction monitoring by the AML/CTF Senior Management Group including SMRs, TTRs and IFTIs (typically every three months); and

c. receipt and review of reports from the independent reviews of the Standard Part A Programs (and, from February 2017, the management actions and timelines to address any remedial issues or enhancements raised in the report) to the relevant Boards and committees, including the SCA Board, AFRC and the AML/CTF Senior Management Group.

F.2.4 Appropriate approval and oversight framework

148 Notwithstanding the matters set out at paragraphs 143 to 147 that were directed at Board and senior management oversight, the 2015-June 2021 Standard Part A Programs did not establish an appropriate framework for adequate approval and oversight by the Board and senior management because they did not:

a. determine and set SCA's ML/TF risk appetite for the purposes of the Standard Part A Program;

b. include a formal structure to ensure the Board received and reviewed sufficiently detailed management reports about all new and emerging sources of ML/TF risk and about the measures management were taking to deal with those risks;

c. establish appropriate ML/TF risk management capability frameworks, including with respect to specific roles and accountabilities, operational procedures, reporting lines, escalation procedures, assurance and review, and information management;

d. provide a clear mandate for the AML/CTF Senior Management Group to make or recommend decisions with respect to identifying, mitigating and managing the ML/TF risk reasonably faced by SCA;

e. provide for sufficient resources for an AML team commensurate with the nature, size and complexity of SCA and the ML/TF risk it reasonably faced; and

f. establish a clear common understanding within SCA as to:

i. reporting lines to and from senior management; and

ii. the roles and accountabilities with respect to ML/TF risk management and compliance.

149 In relation to the October 2021 Standard Part A Program, SCA acknowledges that it did not establish an appropriate framework for sufficient approval and oversight by the Board and senior management because:

a. it did not determine or set SCA's ML/TF risk appetite;

b. it did not ensure sufficient resources for an AML team commensurate with the nature, size and complexity of SCA's business and the ML/TF risk it reasonably faced, including an appropriate framework for end-to-end accountabilities or processes for ML/TF risk management or compliance; and

c. there was a lack of clear processes to escalate, mitigate and manage material ML/TF risk.

150 For a reporting entity of the nature, size and complexity of SCA, the failure to establish an appropriate framework for approval and oversight by the Board and senior management, for the reasons set out at paragraphs 148 to 149, meant that SCA did not satisfy the primary purpose requirement within the meaning of section 84(2)(a) of the AML/CTF Act.

151 Not establishing an appropriate approval and oversight framework for the reasons set out at paragraphs 148 and 149 was also a factor which contributed to SCA's failure to comply with section 84(2)(c) of the AML/CTF Act and paragraphs 8.1.3, 8.1.4, 8.1.5(4), and 8.4.1 of the AML/CTF Rules.

152 The steps SCA has taken to uplift and enhance its AML/CTF function and compliance with respect to Board and senior management governance and oversight are discussed at paragraph 513below.

F.3 Risk-based systems and controls

153 A reporting entity's standard Part A Program must include appropriate risk-based systems and controls to identify, mitigate and manage the ML/TF risk it may reasonably face in providing designated services. The systems and controls designed and implemented by the reporting entity should be aligned to the reporting entity's current ML/TF risk. Those risks are to be identified through the risk assessments undertaken by the reporting entity, which have regard to the matters described at paragraph 8.1.3 and 8.1.4 of the AML/CTF Rules. A reporting entity's standard Part A Program will not satisfy the primary purpose requirement within the meaning of section 84(2)(a) of the AML/CTF Act if it does not include appropriate risk-based systems and controls necessary to ensure that the standard Part A Program is capable of identifying, mitigating and managing all the ML/TF risk the reporting entity may reasonably face.[16]

154 At all times throughout the Relevant Period, SCA provided its customers with designated services through the channels described at Section C.5. The designated services could be facilitated through Australian dollars, foreign currencies, cash and third party transactions.

155 Over the Relevant Period, SCA undertook risk assessments to identify and assess the ML/TF risk it might reasonably face in relation to the provision of designated services it provided. For the reasons described in Section F.1.1.2, from 7 December 2016 to about 17 November 2022, the Standard Part A Programs were not based on an adequate assessment of all of the ML/TF risk associated with the provision of designated services to SCA's customers.

156 As a result, and as described in paragraphs 228 to 234, the systems and controls described in the Standard Part A Programs were not sufficiently aligned to the ML/TF risk that SCA might reasonably face across all designated services provided by SCA. As a consequence,

[16] See paragraphs 20-21 for an explanation of appropriate risk-based procedures, systems and controls.

between 7 December 2016 and about 17 November 2022, the systems and controls in the Standard Part A Programs did not fully satisfy the requirements of paragraphs 8.1.3 and 8.1.4 of the AML/CTF Rules and sections 84(2)(a) and 84(2)(c) of the AML/CTF Act.

157 The following channels and designated services are set out in this section:

a. FMAs;

b. SCA Customer account channel;

c. SCEG Customer account channel;

d. SkyCity New Zealand channel;

e. CCFs;

f. EZYPlay Guest Cards;

g. exchange of money for CVIs, including chips and tokens;

h. table games, ETGs and EGMs; and

i. foreign currency exchange services.

F.3.1 Front Money Accounts

Overview

158 A brief overview of FMAs is at Section C.5.2 above. What follows is additional information relevant to the operation of FMAs.

159 Before funds could be transferred to a customer's FMA, the customer was required to be a member of SCA's loyalty program. FMAs were opened in the name of a customer. Upon establishing an FMA, a customer was required to provide SCA with the relevant KYC information which was required by SCA's Standard Part B Programs (as described at paragraph 374). An FMA established by a customer with SCA could not be used at other SCEG casinos. Transactions on FMAs involved the provision of items 31 and 32, table 1, section 6 of the AML/CTF Act and items 7, 8, 11 and 13, table 3, section 6 of the AML/CTF Act designated services. An FMA was a general ledger account which was created and managed by SCA. FMAs were not accessible externally and there were no individual BSB and account numbers attributed to FMAs.

160 Customers could credit their FMA as described above at paragraph 36 including by depositing funds into bank accounts maintained by SCA (the SCA Customer accounts, as described at paragraphs 41 to 43) or a SCEG subsidiary (the SCEG Customer accounts, as described at paragraphs 44 to 46 and 176 to 177). Deposits received from customers into an SCA bank account were recorded as transactions into the SCA accounting ledger. Once the deposit was received by SCA from the customer, SCA's Bally CMP System and Bally Cage System were updated to reflect the receipt of funds. Once a customer presented onsite at the SCA casino, signed the customer deposit receipt and provided photo identification (to confirm they were the intended recipient of the funds), their FMA was credited with the amount which had been deposited, and the funds on the FMA would be released to them. The circumstances in which third parties could deposit funds into FMAs are described at paragraphs 41, 44 and 164 to 165.

161 Once the funds were credited to a customer's FMA, the customer could access those funds at the SCA casino by:

a. obtaining chips or other CVIs, including TITO tickets and casino cheques[17] at the SCA Cage;

b. withdrawing cash in Australian dollars[18] at the SCA Cage;

c. withdrawing cash in a foreign currency at the SCA Cage (in the same currency that had been previously exchanged for Australian dollars at the commencement of the customer's trip and subject to availability of that particular foreign currency);

d. inserting their membership card at an EGM/ETG for the purpose of cashless gaming by transferring funds from their FMA onto an EGM/ETG as credits;[19] and

e. 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 certain limits.[20]

162 A customer could also withdraw funds from their FMA by instructing SCA to transfer funds out of their FMA into:

a. their personal bank account;

b. a SCEG New Zealand casino (in circumstances where the customer held an FMA at another SCEG casino);

c. a third party bank account (until June 2021 via the SCEG Customer account channel);

d. the bank account of another casino (either foreign or Australian dollars, until February 2022 for transactions via the SCEG Customer account, see paragraph 225e); or

e. another customer's FMA. However, this was typically permitted for authorised transfers where a Funds Authorisation Form was completed and approved (described further at paragraphs 164 to 165).

163 Customers could transfer funds from their FMAs at the SCA casino through non-face-to-face channels, without being present at the Cage, by completing a Telegraphic Transfer Request Form for an electronic transfer or by requesting a casino cheque (payable to the customer only and mailed to the customer's personal home address).

Deposits to and transfers between customer FMAs

164 SCA permitted deposits to, and transfers between, two different customer's FMAs, including:

a. transfers between ICP customers' FMAs; or

b. from 14 February 2017 to 12 April 2021, requests from a junket operator for a junket representative to conduct transactions on the junket operator's FMA on their behalf, and other transfers related to junket programs. For example, a junket operator to a junket player's FMA.

---

17 Items 7 and 13, table 3, section 6 of the AML/CTF Act.

18 Item 13, table 3, section 6 of the AML/CTF Act.

19 Item 13, table 3, section 6 of the AML/CTF Act.

20 Item 13, table 3, section 6 of the AML/CTF Act.

165 Where a deposit to or transfer request between FMAs was made in the above circumstances, that request was to be accompanied by a Funds Authorisation Form (as described at paragraph 225d).

ML/TF risk of Front Money Accounts

166 Transfers through FMAs involved higher ML/TF risk. The higher ML/TF risk associated with FMAs are set out as follows:

a. FMAs could be used to facilitate the movement of funds into and out of the SCA casino environment through complex transaction chains, which could provide opportunities for layering laundered funds;

b. customers and third parties could deposit or withdraw funds from FMAs through non-face-to-face channels, without being present at the Cage, creating opportunities for layering of funds. With respect to third party deposits (via telegraphic transfers) into the SCEG Customer account channel, SCA introduced a SOP which provided that after June 2021, third party deposits were no longer accepted (see paragraph 44). In September 2022, SCA introduced guidance for staff about the process for third party payment rejection where third party deposits (via telegraphic transfer) were made into the SCEG Customer accounts. Until June 2021 SCA permitted transfers from a customer's FMA to a third party (see paragraph 225e below);

c. funds in FMAs could also be transferred to, or received from other casinos, including non-SCEG casinos and casinos located outside of Australia (until February 2022 for transactions via one of the SCEG Customer accounts, as described at paragraph 225e);

d. funds could be transferred between FMAs of different customers (as described above at paragraph 164) These attributes created risks relating to some of the ML/TF typologies set out in Schedule 1;

e. cash could be withdrawn from a customer's FMA at the SCA casino in circumstances where the customer had applied the funds to minimal or no gaming; and

f. by nature of their design, FMAs held by VIP customers of SCA could be used as a method to 'park' funds, putting distance between an act or acts that generated illicit funds and the ultimate recipient of those funds, which could make it more difficult to understand or trace the flow of the funds.

167 For the reasons described in paragraphs 153 to 156, from 7 December 2016 to about 17 November 2022, the Standard Part A Programs were not based on an adequate assessment of the ML/TF risk associated with the provision of designated services to SCA's customers through FMAs. As a result, SCA did not ensure during the Relevant Period that its Standard Part A Programs included appropriate risk-based systems and controls that were capable of identifying, mitigating and managing all ML/TF risk associated with the provision of designated services by SCA through FMAs. See paragraphs 230 with respect to deficiencies with risk-based systems and controls relating to cash, 231 with respect to third party transactions and 233 with respect to remittance services.

F.3.2 SCA Customer account channel

Overview

168 A brief overview of the SCA Customer account channel is at Section C.5.4 above. What follows is additional information relevant to the SCA Customer account channel.

169 Once funds had been deposited into the SCA Customer accounts, the customer would notify SCA staff of the deposit and provide evidence of the deposit, including bank transfer receipts. Once SCA had confirmed the amount had been received, it would credit the funds to the customer's FMA in the relevant Bally system. When a customer wanted to access funds from their FMA for gaming, they would be required to present themselves at a Cage cashier window, where they were required to sign a customer deposit receipt and have their identity verified by Cage staff (to confirm they were the intended recipient of the funds), before they were able to draw on funds credited to their FMA. Once the funds were credited to the customer's FMA, the customer could also access and withdraw the funds as described in paragraphs 161 to 162.

170 SCA Customer accounts also facilitated the payment of winnings to customers, or the return of funds which were ultimately not used for gaming. These payments were facilitated by the transfer of customer funds from an FMA to a bank account nominated by a customer (which could be the customer's personal bank account, a third party bank account or a bank account of another casino).

171 The withdrawal details were recorded in the FMA records in SCA's systems. In some circumstances, customers could also withdraw funds from FMAs through non-face-to-face channels, without being present at the Cage by requesting and completing a 'Threshold Transaction Request Form' for an electronic transfer, or by requesting a casino cheque payable to the customer only and mailed to the customer's home address.

172 Transfers to and from FMAs, via the SCA Customer accounts, involved the facilitation of the transfer of funds in and out of the SCA casino environment, by SCA, at the request of its customers, which involved the provision of designated services under items 31 and 32, table 1, section 6 of the AML/CTF Act and item 13, table 3, section 6 of the AML/CTF Act.

ML/TF risk of the SCA Customer accounts

173 Transfers through FMAs, via the SCA Customer accounts, involved higher ML/TF risk, including:

a. the ML/TF risk related to FMAs (as described at paragraph 166);

b. funds could be deposited into a SCA Customer account through non-face-to-face channels, which created risks as to the source of funds;

c. cash could also be deposited into a SCA Customer account, which created risks as to source of funds;

d. deposits from overseas remitters could be accepted for SCA customers and could be used to facilitate the movement of funds into the SCA Customer accounts from international jurisdictions;

e. SCA accepted deposits into the SCA Customer accounts from third parties, including some corporate third parties, which could create risks as to the source of funds; and

f. customers could deposit funds into the SCA Customer accounts from overseas.

174 SCA did not conduct assessments of the ML/TF risk associated with the provision of items 31 and 32, table 1, section 6 of the AML/CTF Act designated services by facilitating the transfer of funds to and from FMAs via the SCA Customer account channels (as described at paragraphs 41 to 42).

175 By not undertaking a ML/TF risk assessment for items 31 and 32, table 1, section 6 of the AML/CTF Act designated services with respect to the SCA Customer account channel, SCA did not ensure during the Relevant Period that its Standard Part A Programs included

adequate risk-based systems and controls that were capable of identifying, mitigating and managing all ML/TF risk associated with the provision of these designated services, which contributed to SCA's contravention of paragraph 8.1.4 of the AML/CTF Rules. See paragraphs 231 and 233 for the deficiencies with the systems and controls relating to the SCA Customer account channel.

F.3.3 SCEG Customer account channel

Overview

176 As described above in further detail at Section C.5.5, SCA customers could deposit funds into the SCEG Customer accounts during the Relevant Period. What follows is additional factual background relevant to the operation of the SCEG Customer account channel.

177 A customer could deposit funds, or arrange for funds to be deposited, into:

a. a SCEG Customer account, to be credited to the customer's FMA at SCA;

b. a SCEG Customer account, to repay an amount owed to SCA under a CCF; and

c. until at least February 2022, a SCEG Customer account, by a transfer of funds from another casino, including non-SCEG casinos, to one specific SCEG Customer account. The funds would then be credited to a customer's FMA (in the circumstances described in paragraph 160).

178 A customer could request SCA to transfer funds from their FMA via the SCEG Customer accounts to:

a. the customer's personal bank account for the purpose of returning funds in their FMA or remitting winnings;

b. a personal bank account, which was not in the customer's name (until at least June 2021, see paragraph 225e); or

c. another casino, including non-SCEG casinos and casinos located outside of Australia (provided the customer was a SCA loyalty member). From around February 2022, SCA ceased allowing customers to transfer funds from their FMA to another casino (that was not a SCEG casino).

179 Deposits from a customer through a SCEG Customer account for gaming were recorded as transactions in the SCA accounting ledger. Each ledger record included the transaction date, the value of the transaction and the customer's name. Once funds had been transferred into a SCEG Customer account, the customer provided a copy of the transaction receipt to the SCEG International Business Sales team, which was forwarded to either the SCEG International Business Patron Accounts team or the SCEG New Zealand casino Cage to reconcile against the bank statements for the SCEG Customer account. Details of the deposit were then communicated to SCA, including the transaction receipt.

180 Once the customer was onsite at the SCA casino, had signed the customer deposit receipt and provided photo identification (to confirm they were the intended recipient of the funds), SCA would credit the funds to the customer's FMA. Once the funds were credited to the customer's FMA the customer could access and withdraw the funds as described in paragraphs 161 to 162.

181 The funds were not physically transferred from the SCEG Customer account to a SCA Customer account until the end of the customer's visit and when settlement of outstanding debts occurred.

182 SCEG Customer accounts also facilitated the payment of winnings and the return of funds not used for gaming. Winnings from gaming could not be directly deposited into a SCEG Customer account by customers. These payments were facilitated by the transfer of customer funds from an FMA to a bank account nominated by a customer (which could be the customer's personal bank account, a third party bank account (until at least June 2021), or a bank account of another casino (until February 2022), via the SCEG Customer accounts.

183 Transfers to and from FMAs, via the SCEG Customer accounts, involved the facilitation of the transfer of funds in and out of the SCA casino environment, by SCA, at the request of its customers, which involved the provision of designated services under items 31 and 32, table 1, section 6 of the AML/CTF Act and item 13, table 3, section 6 of the AML/CTF Act.

ML/TF risk of the SCEG Customer account channel

184 Transfers through FMAs, via the SCEG Customer accounts, involved higher ML/TF risks, including:

a. designated services provided by SCA through the SCEG Customer accounts involved FMAs and accordingly also involved the ML/TF risk set out in paragraph 166;

b. funds could be deposited into a SCEG Customer account through non-face-to-face channels, which created risks as to the source of funds;

c. cash could also be deposited into a SCEG Customer account, which created risks as to the source of funds;

d. most of the SCEG Customer accounts were located in foreign jurisdictions. SCA customers and third parties, including other casinos, overseas remitters and junket operators (including corporate junket operators), could deposit funds into the SCEG Customer accounts, including in foreign currencies. This created risks as to source of third party deposits;

e. money could be made available to a SCA customer in Australia through the SCEG Customer account channel without the need for a cross-border transfer of funds, which reduced the transparency of transactions;

f. junket operators (including corporate junket operators), overseas remitters, other casinos (including casinos located outside of Australia until at least February 2022), and other third parties used the accounts, including to remit money across international borders without the physical movement of funds into Australia, which created risks as to the source of funds and reduced transparency; and

g. the Horizon Tourism account channel involved additional ML/TF risk, including because SCA's connection with the Horizon Tourism accounts was not apparent on their face, as the accounts operated in the name Horizon Tourism (New Zealand) Limited.

185 SCA did not conduct assessments of the ML/TF risk associated with the provision of items 31 and 32, table 1, section 6 of the AML/CTF Act designated services by facilitating the transfer of funds to and from FMAs, via the SCEG Customer accounts (as described at paragraphs 44 to 45).

186 By not undertaking a ML/TF risk assessment for items 31 and 32, table 1, section 6 of the AML/CTF Act designated services with respect to the SCEG Customer account channel, SCA did not ensure during the Relevant Period that its Standard Part A Programs included adequate risk-based systems and controls that were capable of identifying, mitigating and managing all ML/TF risk associated with the provision of these designated services, which

contributed to SCA's contravention of paragraph 8.1.4 of the AML/CTF Rules. See paragraphs 231, 232c and 233 for the deficiencies with SCA's systems and controls relating to the SCEG Customer account channel.

F.3.4 SkyCity New Zealand channel

Overview

187 As described above at paragraph 47, from 7 December 2016 to about 17 November 2022, a customer with funds in an FMA established 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). A customer could use the SkyCity New Zealand channel to make funds available to their FMA at SCA or to repay a debt owed by the customer to SCA under a CCF from their gaming at the SCA casino.

188 To initiate a transfer, a customer completed a template letter which identified their FMA at a SCEG New Zealand casino, the amount to be transferred, and the location the amount was to be transferred to (being the SCA casino). 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. The transfer of funds from the customer's FMA at a SCEG casino to a customer's FMA at the SCA casino was done by way of inter-company journal entry. The customer's funds at the SCEG casino were not transferred by way of cross-border banking transaction from New Zealand to Australia. The funds were instead offset between SCEG and SCA.

189 Once the customer presented on site at the SCA Cage and the standard KYC checks were completed, SCA credited the funds to the customer's FMA at SCA (in the circumstances described in paragraph 160). Once the funds were credited to the customer's FMA they could access and withdraw the funds as described in paragraphs 161 to 162.

190 Transfers to and from FMAs, via the SkyCity New Zealand channel, involved the facilitation of the transfer of funds in and out of the SCA casino environment, by SCA, at the request of its customers, which involved the provision of designated services under item 32, table 1, section 6 of the AML/CTF Act and item 13, table 3, section 6 of the AML/CTF Act.

ML/TF risk of the SkyCity New Zealand channel

191 The SkyCity New Zealand channel involved higher ML/TF risks because customers could request that funds that had been deposited into their SCEG FMA (including deposits by third parties by cash or telegraphic transfer) be transferred to their FMA at the SCA casino, which resulted in an offsetting process (by-passing the traditional banking system).

192 SCA did not conduct assessments of the ML/TF risk associated with the provision of item 32, table 1, section 6 of the AML/CTF Act designated services, by facilitating the transfer of funds to and from FMAs through the SkyCity New Zealand channel.

193 By not undertaking a ML/TF risk assessment for the provision of designated services by SCA through the SkyCity New Zealand channel, SCA did not ensure during the Relevant Period that its Standard Part A Programs included appropriate risk-based systems and controls that were capable of identifying, mitigating and managing all ML/TF risk associated with the provision of designated services by SCA through the SkyCity New Zealand channel, and as a result, this contributed to SCA's contravention of paragraph 8.1.4 of the AML/CTF Rules. See paragraph 233 for the deficiencies with the systems and controls relating to the SkyCity New Zealand channel.

F.3.5 Cheque Cashing Facilities

Overview

194 As described above in further detail at Section C.5.7, customers could apply for a CCF from the SCA casino. What follows is additional information relevant to CCFs.

195 All CCF applicants were subject to approval by senior management pursuant to the Delegated Financials Authority (**DFA**) and Delegated Gaming Authorities (**DGA**). CCF applications were referred to the International Business Accounts Team, which was part of SCEG, who were responsible for assessing and approving/refusing CCF applications for international customers.[21] The International Business Accounts Team conducted a credit assessment pursuant to the 'Patron Accounts Risk Matrix' (as amended from time to time).

196 SCA provided designated services under item 6, table 1, section 6 of the AML/CTF Act when it executed or approved a CCF Agreement. The advance of funds was a 'loan' within the meaning of section 5 of the AML/CTF Act.

197 Once the customer had provided a signed blank personal cheque or had been issued a counter cheque/credit marker, the customer could then draw down 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 otherwise approved by SCA management);

b. a customer could be issued with chips or a CPV; and

c. customers (other than ICP players, junket operators and junket representatives) could use their SCA loyalty card at any EGM, CRT or ATG.

198 Customers using CCF facilities were typically issued 'commission chips'. Players on GCPs may have been issued with 'non-negotiable chips' or commission branded gaming chips. Non-negotiable chips allowed customers to play on the tables specified in the junket agreement and could not be exchanged for other chips at the Cage, unless authorised by International Business personnel.

199 A drawdown of funds under a CCF was a transaction in relation to a 'loan'. Where a drawdown of funds under a CCF occurred, SCA provided an item 7, table 1, section 6 of the AML/CTF Act designated service.

200 A customer could repay a CCF by cash or chip deposit into the customer's FMA at the Cage, or through a domestic or international telegraphic transfer through a:

a. SCA Customer account (including by a third party); or

b. SCEG Customer account (including by a third party up to December 2021 for cash deposits, see paragraph 44 with respect to deposits via telegraphic transfer).

201 A customer could also repay a CCF by providing a cheque issued by another casino, requesting SCA to transfer funds from an FMA held at a SCEG New Zealand casino to the customer's SCA FMA by way of inter-company transfer, applying funds from the customer's FMA at the conclusion of gaming or by setting-off the amount owing against the customer's winnings at SCA.

202 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

[21] For example, *Order of the Liquor and Gambling Commissioner* pursuant to the Casino Act, signed March 2020, clause 3.1.

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 debt.

203 The repayment of a CCF involved a transaction in relation to a loan (including by banking or redeeming a personal cheque, counter cheque or credit marker) where SCA provided an item 7, table 1, section 6 of the AML/CTF Act designated service.

ML/TF risk of Cheque Cashing Facilities

204 The provision of CCFs by SCA involved higher ML/TF risk because:

a. CCFs could be drawn down and repaid as part of a complex chain of designated services;

b. CCFs may have enabled funds held by customers in foreign jurisdictions to be used in Australia without the need for cross-border transfers;

c. repayments of CCFs could be made by way of international and domestic transfers into a customer's FMA, which was a non-face-to-face channel. CCFs could also be repaid by third parties through non-face-to-face channels.

d. CCFs could be drawn down by way of an 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);

e. CCFs were subject to credit limits and could be drawn down on multiple occasions within the approved limit; and

f. junket operators and junket representatives were provided with significant lines of credit through CCFs.

205 SCA did not conduct assessments of the ML/TF risk associated with the provision of items 6 and 7, table 1, section 6 of the AML/CTF Act designated services through CCFs. By not undertaking a risk assessment for CCFs, SCA did not ensure during the Relevant Period that its Standard Part A Programs included adequate risk-based systems and controls that were capable of identifying, mitigating and managing all ML/TF risk associated with CCFs, which contributed to SCA's contravention of paragraph 8.1.4 of the AML/CTF Rules. See paragraph 232 for the specific deficiencies with the systems and controls relating to CCFs.

F.3.6 EZYPlay Guest Cards

206 As described above at Section C.5.8, EZYPlay Guest Cards were physical cards used by SCA customers to undertake cashless gaming at the SCA casino. These cards were not issued in the name of the customer, and SCA did not take any steps to identify or verify the identity of the customer when they were issued with an EZYPlay Guest Card. EZYPlay Guest Cards were a channel through which SCA provided items 6, 7, 8 and 9, table 3, section 6 of the AML/CTF Act designated services, including non-face-to-face transactions.

207 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 at the SCA Cage;[22]

[22] Item 7, table 3, section 6 of the AML/CTF Act.

b. a customer could transfer credits from an EGM or ETG to an EZYPlay Guest Card;[23]

c. a customer could transfer funds from an EZYPlay Guest Card to an EGM;[24] 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.[25]

208 Throughout the Relevant Period, EZYPlay Guest Cards were subject to an ongoing balance limit in the main gaming area of $1,000 (from the start of the Relevant Period until around August 2019) and $5,000 (from around August 2019 until the end of the Relevant Period). These limits did not apply in VIP gaming areas, however all customers (including those in VIP gaming areas) were prohibited from making cash deposits and withdrawals from EZYPlay Guest Cards which exceeded $2,000 (prior to August 2019) or $2,500 (after August 2019) in a single transaction.

ML/TF risk of EZYPlay Guest Cards

209 The provision of designated services through EZYPlay Guest Cards involved higher ML/TF risk as:

a. EZYPlay Guest Cards were not issued in a customer's name, the card was transferable and facilitated transactions where the source of funds could be concealed;

b. EZYPlay Guest Cards could be used to conduct non-face-to-face transactions, including at CRTs, EGMs and ETGs;

c. cash could, subject to the limitations described above at paragraph 208, be deposited and withdrawn using EZYPlay Guest Cards through the Cage and CRTs;

d. EGM and ETG credits could be deposited and withdrawn from an EZYPlay Guest Card, including credits that had been uploaded to an EGM or ETG from a TITO; and

e. EZYPlay Guest Cards could have been used to facilitate multiple transactions in complex chains of designated services in circumstances where the identity of the customer was not known.

210 For the reasons described in paragraphs 153 to 156, from 7 December 2016 to about 17 November 2022, the Standard Part A Programs were not based on an adequate assessment of SCA's ML/TF risk associated with the provision of designated services to its customers. As a result, SCA did not ensure during the Relevant Period that its Standard Part A Programs included appropriate risk-based systems and controls that were capable of identifying, mitigating and managing all ML/TF risk associated with the provision of designated services by SCA through EZYPlay Guest Cards. See paragraph 234d for the specific deficiencies with the systems and controls relating to EZYPlay Guest Cards.

F.3.7 Exchange of money for CVIs, including chips and tokens

Overview

211 As described at Section C.5.3, at all times during the Relevant Period, SCA provided designated services pursuant to items 6, 7, 8, 9 and 13, table 3, section 6 of the AML/CTF Act to customers through the use of CVIs (including chips and tokens).

---

[23] Item 9, table 3, section 6, of the AML/CTF Act.

[24] Item 6, table 3, section 6 of the AML/CTF Act.

[25] Item 8, table 3, section 6 of the AML/CTF Act.

ML/TF risk of exchanging of money for CVIs, including chips and tokens

212 The provision of designated services through CVIs involved higher ML/TF risk, as:

a. chips could be purchased with cash (in some circumstances, cash generated through criminal activity), then redeemed by a casino cheque or money transfer to integrate funds into the formal financial system;

b. CVIs were highly transferrable, could not always be traced to an account holder or identified customer and could be issued in large values;

c. 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;

d. the redemption of CVIs could not always be attributable to winnings and could be cashed out with minimal or no play; and

e. the issue or redemption of tickets was not always face-to face.

213 For the reasons described in paragraphs 153 to 156, from 7 December 2016 to about 17 November 2022, the Standard Part A Programs were not based on an adequate assessment of the ML/TF risk associated with the provision of designated services to SCA's customers. As a result, SCA did not ensure during the Relevant Period that its Standard Part A Programs included appropriate risk-based systems and controls that were capable of identifying, mitigating and managing all ML/TF risk associated with the exchange of money for CVIs. See paragraph 234 for the deficiencies with the systems and controls relating to the exchange of money for CVIs.

F.3.8 Table games, ETGs and EGMs

Overview

214 As described at paragraphs 31 to 32, at all times during the Relevant Period, SCA provided designated services pursuant to items 6 and 9, table 3, section 6 of the AML/CTF Act to customers.

ML/TF risk of table games, ETGs and EGMs

215 The provision of designated services through table games, ETGs and EGMs involved higher ML/TF risk because:

a. in table games that permitted 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;

b. baccarat also involved a low 'house edge' and each hand could be high in value and played within seconds. Funds could therefore be turned over quickly, with minimal net loss and in collusion with other players;

c. poker permitted peer-to-peer gaming, which created risks of collusion;

d. the risks of even-money wagering were higher with certain semi-automated and fully-automated games, as there was inappropriate oversight and a player could play several terminals at the same time;

e. money including cash could be inserted into ETGs and EGMs, and tickets could be collected with minimal or no play;

f. EGMs and ETGs were vulnerable to refining because they were capable of processing large volumes of smaller amounts of funds quickly. Funds could also be moved through ETGs and EGMs through buying-in and cashing-out using cash, chips, TITO tickets and other CVIs; and

g. play on table games, EGMs and ETGs could be used to layer funds, as part of a more complex transaction chain of designated services, making it difficult to understand the purposes of transactions, the beneficial owner of funds or the ultimate beneficiary of the value moved.

216 For the reasons described in paragraphs 153 to 156, from 7 December 2016 to about 17 November 2022, the Standard Part A Programs were not based on an adequate assessment of the ML/TF risk associated with the provision of designated services to SCA's customers. As a result, SCA did not ensure during the Relevant Period that its Standard Part A Programs included appropriate risk-based systems and controls that were capable of identifying, mitigating and managing all ML/TF risk associated with the provision of table games, ETGs and EGMs. See paragraph 234 for the specific deficiencies with the systems and controls relating to table games, ETGs and EGMs.

F.3.9 Foreign currency exchange services

Overview

217 As described at Section C.5.9, at all times during the Relevant Period, SCA provided foreign currency exchange services to customers within the meaning of item 14, table 3, section 6 of the AML/CTF Act.

ML/TF risk of foreign currency exchange services

218 Chapter 2 of the FATF / Asia/Pacific Group on Money Laundering Casino Typologies Report identifies the following as indicators of ML/TF risk associated with foreign currency exchange:

a. bank drafts/cheques cashed in for foreign currency;

b. multiple currency exchanges;

c. dramatic or rapid increases in size and frequency of currency exchange transactions for regular account holders;

d. currency exchange for no reasonable purpose;

e. currency exchanges with low denomination bills for high denomination bills;

f. currency exchanges carried out by third parties;

g. large, one-off or frequent currency exchanges for customers not known to the casino;

h. requests for casino cheques from foreign currency;

i. currency exchanges with little or no gambling activity; and

j. structured currency exchanges.

219 For the reasons described in paragraphs 153 to 156, from 7 December 2016 to about 17 November 2022, the Standard Part A Programs were not based on an adequate assessment of the ML/TF risk associated with the provision of designated services to SCA's customers. As a result, SCA did not ensure during the Relevant Period that its Standard Part A

Programs included appropriate risk-based systems and controls that were capable of identifying, mitigating and managing all ML/TF risk associated with the provision of foreign currency exchange services.

F.3.10 Risk-based systems and controls

220 ML/TF risk-based systems and controls may be either 'preventative' or 'detective'.

221 Preventative controls are those that limit the ability to use a product or channel in a way that would increase ML/TF risk. Examples of preventative controls include setting transaction limits, having a management approval process for high risk customers, products or countries, applying different identification processes for customers not dealt with in person, and not accepting customers who are deemed too high risk.

222 Detective controls seek to detect and 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 assist in identifying suspicious activity and may trigger further action like reporting suspicious transactions to AUSTRAC and conducting ECDD. Detective controls do not, of themselves, reduce inherent ML/TF risk.

223 The AML/CTF Act and the AML/CTF Rules require a reporting entity to have regard to a number of factors in determining the appropriate risk-based systems and controls that it will include in Part A of its AML/CTF program. These factors are set out at paragraph 20.

224 The Standard Part A Programs included some risk-based systems and controls intended to mitigate and manage the ML/TF risk of providing the designated services referred to in Section F.3. Certain systems and controls were supported by SOPs and other documents and internal procedures.

225 A summary of the controls with certain examples is set out below and at paragraphs 226 to 227, 273, 275 and 287 to 288:

a. **FMAs**: See the processes described above at paragraphs 159 with respect to opening an account, 162 with respect to withdrawing funds from an FMA and 160 with respect to releasing funds from a customer's FMA. The matters described below at paragraph 226a (with respect to AML/CTF staff training), 226b (with respect to KYC), 226c (with respect to PEP screening), 226e (with respect to transaction monitoring) and 227 (with respect to reporting obligations) were also applicable to transactions on FMAs.

b. **Customer risk ratings**: At all times during the Relevant Period, the Standard Part A Programs required customers to be risk rated (as described above at paragraph 102). See also the description of the processes at paragraphs 332 to 333, 341, 383 to 384 and 389 when customers' risk ratings were elevated (with respect to PEP screening, ECDD and the escalation to the General Manager).

c. **Transaction limits**: Throughout the Relevant Period, SCA implemented certain transaction limits in respect of the provision of designated services involving EGMs and ETGs, cash redemptions at the Cage or a CRT, deposits and withdrawals using a CRT, TITOs, and EZYPlay Guest Cards (as described above at paragraph 208). For example, if a customer sought to withdraw more than $5,000 from an EGM on the main gaming floor, the EGM would lock up and prohibit the withdrawal until it was verified by the Gaming Machine Supervisor or Surveillance Team, as the circumstances required.

d. **Transfers between different customers' FMAs**: Throughout the Relevant Period, SCA required the completion of Funds Authorisation Forms before facilitating any transfer of funds from one customer's FMA to another customer's FMA (described

above at paragraphs 164 to 165), including via the SkyCity New Zealand channel. The Funds Authorisation Form was a form used by SCA to facilitate the movement of funds between FMAs. The process of accepting Funds Authorisation Forms in respect of the above transactions ceased on 12 January 2022.

e. **Limitations on third party transactions**: SCA's policies in relation to third party telegraphic transfers were not supported by documented procedures and, as such, were not capable of being consistently and reliably applied. However:

   i. from June 2021, transfers from a customer's FMA to a third party via the SCEG Customer accounts were prohibited but for specific exceptions, which was documented in December 2021. Further restrictions on transfers from a customer's FMA to third parties via the SCEG Customer accounts were imposed in around February 2022 (in relation to casinos);

   ii. an International Business Patron SOP, which was updated in May 2022, set out certain limitations on third party transactions on SCEG Customer accounts; and

   iii. further, in September 2022, SCEG introduced a documented policy setting out the process for rejecting third party deposits into SCEG Customer accounts.

f. **CCFs**: At all times throughout the Relevant Period, all transactions relating to credit markers and CCFs were subject to the following:

   i. all transactions relating to credit markers and cheque securities were required to be conducted in full view of the surveillance camera;

   ii. any transfer into an FMA via the SCEG Customer accounts or SCA Customer accounts, including for the repayment of a CCF, was required to be accompanied by a transaction receipt (as described above at paragraphs 169 and 179);

   iii. in May 2021, SCA introduced a flowchart titled 'SkyCity Credit Application Process for IB Patrons'. This flowchart listed matters relating to the 'credit application', 'patron information', 'credit history at SkyCity', 'watchlist check' and 'risk assessment'; and

   iv. from June 2021, the International Business 'credit application training guide' provided that if, in the course of assessing the CCF application, a CCF applicant was found to be a PEP, a relative or a close associate of a PEP, or involved in any criminal charges, the CCF application could not proceed until the Compliance Team provided approval. Alternatively, where this approval was not provided, the CCF application and CCF would be refused.

226 During the Relevant Period, SCA's Standard Part A and Part B Programs required it to address its ML/TF risk in the following ways:

a. SCA's AML/CTF staff training program, which incorporated training for SCA employees with a low-moderate risk rating or above with a refresher course every two years;

b. SCA's KYC processes (as further described at paragraphs 374 to 376 and 381);

c. PEP screening (as described below at paragraphs 334 and 383 to 384);

d. collection of source of funds information in certain circumstances (as described at paragraphs 378 to 379); and

e. transaction monitoring (as described at Section F.6).

227 SCA was also required to report to AUSTRAC SMRs, TTRs and IFTIs within specified timeframes and, to facilitate this, had internal transaction recording and reporting processes in place (as described at paragraphs 353 to 361). At all times during the Relevant Period, staff who observed suspicious customer behaviour were also required to report the matter to the SCA AML team by way of observation reports as part of SCA's systems and controls to comply with its requirement to report suspicious matters (as described further at paragraphs 351 to 352).

F.3.11 Deficient risk-based systems and controls

228 SCA's Standard Part A Programs did not satisfy the primary purpose requirement within the meaning of section 84(2)(a) of the AML/CTF Act because they did not include appropriate risk-based systems and controls necessary to ensure that the Standard Part A Programs were capable of identifying, mitigating and managing all the ML/TF risk reasonably faced by SCA.

229 Further, for the reasons set out at paragraphs 97, 106 to 109, 111 to 112, 115 to 116, 119 to 120, 126, 131 and 135 to 136, the systems and controls in the Standard Part A Programs were not sufficiently aligned to the ML/TF risk reasonably faced by SCA with respect to the provision of designated services it provided. These deficiencies contributed to SCA's breach of section 84(2)(c) of the AML/CTF Act and paragraphs 8.1.3. and 8.1.4 of the AML/CTF Rules.

Cash

230 From 7 December 2016 to about 17 November 2022, the Standard Part A Programs did not include appropriate risk-based systems and controls with respect to cash. For example:

a. prior to 23 December 2019, it was not a requirement for a customer to provide source of funds information in order to make a large cash deposit at the Cage;

b. on 23 December 2019, SCA commenced requiring a Source of Funds Declaration Form to be completed by International Business customers presenting $100,000 or more in cash. However, it was not a requirement for customers to provide supporting documentation with this form. There was no requirement for domestic customers to complete a Source of Funds Declaration Form for cash deposits;

c. a requirement to provide supporting documentation in relation to large cash deposits was introduced on 17 December 2020, which related to:

   i. International Business customers presenting $250,000 or more in cash; and

   ii. domestic customers presenting $150,000 or more in cash;

d. the requirement in (c) was updated on 19 July 2021 as follows:

   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. there were deficiencies in the written guidance for SCA staff members conducting source of funds and source of wealth checks as described in sub-paragraphs (b) to (d), and in information management and record keeping, as set out in paragraph 343i;

f. there were no daily or transaction limits relating to cash deposits and payments at the Cage;

g. there were no 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 (see paragraph 409j with respect to the acceptance of cash that appeared to be suspicious); and

h. SCA did not place any caps on cash transactions in VIP gaming rooms, including as used by junkets.

Third party transactions

231 The Standard Part A Programs did not include appropriate risk-based controls with respect to third party transactions. For example:

a. SCA did not prohibit or restrict third party payments from SCEG Customer accounts until June 2021, exposing SCA to risks concerning the source and destination of funds for particular transactions. SCA introduced a SOP that provided after June 2021 third party deposits via telegraphic transfer into the SCEG Customer account were no longer permitted. In September 2022, SCA introduced guidance for staff about the process for the rejection of third party payments, to outline the steps to be taken to reject third party deposits that were made into the SCEG Customer accounts (as described further at paragraph 44) or SCA Customer accounts;

b. third parties could deposit funds via the SCA Customer accounts or SCEG Customer accounts to repay a customer's CCF, where SCA did not have adequate processes to identify or limit such third party payments; and

c. while a Funds Authorisation Form was typically used to facilitate transactions between FMAs (as described at paragraphs 164 and 165 above), the form was not used to understand the source of funds relating to third party transactions or to understand the nature of the relationship between the customer and the third party.

Cheque Cashing Facilities

232 The Standard Part A Programs did not include appropriate risk-based systems and controls with respect to CCFs. For example:

a. the approval of credit limits under CCFs was subject to credit risk assessments which were largely focused on credit risk not ML/TF risk (including the documents described above at paragraph 225f);

b. from 7 December 2016, the Standard Part A Programs did not include appropriate risk-based systems and controls to understand the ML/TF risk posed by a customer's source of wealth when approving a CCF for a customer;

c. the Standard Part A Programs did not include appropriate controls to mitigate and manage the ML/TF risk of CCFs and repayments (including in relation to junkets), such as controls to:

i. impose limits on credit (rather, credit limits were required to be set by other SCA documents and internal procedures which were focused on a customer's credit worthiness, rather than ML/TF risk);

ii. identify customers to whom the provision of credit was outside of ML/TF risk appetite; and

iii. restrict the ability of third parties to repay loans on behalf of customers until September 2022 (see further at paragraph 225e on restrictions on third party payments in June 2021 in relation to SCEG Customer accounts);

d. the Standard Part A Programs did not include systems and controls to monitor drawdowns under CCFs; and

e. 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.

Remittance Services

233 The Standard Part A Programs did not include appropriate risk-based controls with respect to remittance services (related to transactions on FMAs, via the SCEG Customer account channel, SCA Customer account channel and the SkyCity New Zealand channel). For example:

a. the Standard Part A Programs did not include appropriate controls, such as daily or transactional limits on remittance transactions;

b. the Standard Part A Programs did not include appropriate risk-based controls to mitigate and manage the ML/TF risk associated with the provision of remittance services as part of a complex chain of different designated services;

c. 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;

d. the Standard Part A Programs did not include appropriate systems or controls for SCA to reliably ascertain and verify whether transfers between FMAs (as described at paragraphs 164 to 166) gave rise to any red flags that might indicate a ML/TF risk;

e. prior to December 2021, when SCA introduced the International Business SOP, SCA had no controls or procedures to identify or limit cash deposits into SCEG Customer accounts. The SOP stated that cash deposits were no longer accepted after September 2021; and

f. SCA did not have in place adequate risk-based processes related to its Standard Part A Programs to satisfy itself as to the source of funds being transferred via the SCEG Customer account, SCA Customer account and SkyCity New Zealand channels.

Gaming Services

234 The Standard Part A Programs did not include appropriate risk-based controls with respect to table 3, section 6 of the AML/CTF Act gaming services. For example:

a. with respect to table games and EGMs:

i. the Standard Part A Programs did not include appropriate transactional limits and thresholds (including those set by SCA with respect to EGMs as noted above at paragraph 225c) with respect to buy-ins and cash-outs that were appropriate to consistently identify transactions that may have given rise to higher ML/TF risk in all circumstances; and

ii. the controls in relation to EGMs and ETGs were largely reliant on staff observation and surveillance. By their nature, manual and observational controls were not capable of consistently detecting the use of table games,

ETGs and EGMs to layer funds, as part of a more complex transaction chain of designated services. The Standard Part A Program controls did not allow the Cage adequate 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. Cage staff applying controls to item 8, table 3, section 6 of the AML/CTF Act designated services did not have adequate visibility over complex transaction chains involving CVIs;

b. 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, section 6 of the AML/CTF Act designated services (especially with respect to uncarded play);

c. the Standard Part A Programs did not include appropriate risk-based controls to mitigate and manage the ML/TF risk associated with the provision of table 3, section 6 of the AML/CTF Act gaming services as part of a complex chain of different designated services;

d. with respect to EZYPlay Guest Cards:

i. there were no limits on the number of EZYPlay Guest Cards that could be obtained by a customer;

ii. EZYPlay Guest Cards were not issued in the name of a customer;

iii. whilst there were specified limits on a per transaction basis with respect to the use of EZYPlay Guest Cards (as described above at paragraph 208), there were no overall daily limits on total transfers from an EGM or ETG to an EZYPlay Guest Card and no overall daily limits on cash deposits into, or cash withdrawals from, an EZYPlay Guest Card at the Cage; and

iv. limited transaction monitoring was applied and, with the exception of surveillance from security staff, there were no other controls to identify whether funds were being withdrawn from these accounts with little or no play; and

e. in general, manual processes were not supported by adequate ML/TF risk awareness training for SCA staff.

F.4 Junket Programs

F.4.1 Introduction and Background

235 As set out above at Section C.7, a junket is an arrangement between a casino and a junket operator that facilitates gambling by one or more high wealth players (referred to as 'junket players') at the casino, on terms agreed between the junket operator and the casino. Junket operators could be represented by one or more junket representatives. In return for bringing the junket player(s) to the SCA casino, SCA provided the junket operator with benefits in accordance with the terms of the agreement between the casino and the junket operator. This included rebates, which were calculated based on the junket's gross win/loss recorded by SCA at the time of settlement, or commissions, which were calculated based on the total turnover of the junket program. SCA may have also provided other benefits to the junket operator (depending on the specific terms of the agreement between the casino and the junket operator).

236 From 7 December 2016 to 12 April 2021, SCA offered and facilitated junket programs, also referred to by SCA as GCPs. SCA offered junket programs to interstate and international players only. The last date of junket play recorded at the SCA casino was 2 January 2021 and the SCEG Board decided to permanently cease dealing with junket operators on 12 April 2021.

237 Relevant key terms used throughout this section of the SAFA are defined as follows:

a. ***Group Commission Operator (junket operator)*** referred to a person representing an individual or a group of interstate or international players while they were gaming at the SCA casino as Group Commission Players pursuant to a Group Commission Program Agreement.

b. ***Group Commission Player (junket player)*** referred to an interstate or international player participating in gaming at the SCA casino while being represented by a Group Commission Operator or authorised Group Commission Representative under a Group Commission Program.

c. ***Group Commission Program Agreement (GCPA)*** referred to a contract between SCA and a Group Commission Operator that related to the conduct of a Group Commission Program at the SCA casino, including any conditions which may have applied. Sometimes these agreements were referred to as revenue share programs.

d. ***Group Commission Program (junket program)*** referred to an offering to a Group Commission Operator to bring a Group Commission Player or Group Commission Players to game at the SCA casino under conditions superior to SCA's normal customer loyalty program. These conditions, which typically involved either a commission rate based on gaming turnover, or a revenue share payment based on win/loss results and complimentaries, were set out and agreed to under a Group Commission Program Agreement.

e. ***Group Commission Representative (junket representative)*** referred to a person who was, or persons who were, nominated by a Group Commission Operator to represent the Group Commission Operator in relation to an individual or a group of interstate or international players while they are gaming at the SCA casino as Group Commission Players under the Group Commission Program Agreement relating to that Group Commission Operator and who may act on behalf of that Group Commission Operator as a signatory on that Group Commission Operator's account.

238 For each junket program, SCA and the junket operator entered into a GCPA. The GCPA set out the terms and conditions of each junket program, including the junket operator and their representative(s) (if any), rebates, commissions and/or amounts payable to the junket operator or SCA (as applicable). The GCPA could be executed by either the junket operator or one of their representatives. The GCPA also set out the terms and conditions upon which any other benefits would be made available to the junket operator, junket representative(s) and junket player(s) such as complimentary airfares, airport transfers, accommodation, and food and beverage allowances. Junket operators would typically arrange for the transfer of funds from the junket to SCA and were responsible for providing junket players with access to their individual funds throughout the junket program, as well as returning any funds or winnings to the junket players at the conclusion of the junket program.

239 The International Business department, which included the International Business Patron Accounts Team, was a division of SCEG that was responsible for facilitating trips for international and interstate VIP customers visiting SCEG casinos in New Zealand and the SCA casino in Adelaide for gambling and entertainment purposes.

240 The International Business department was headed by senior SCEG personnel and had personnel located in multiple jurisdictions, including Adelaide.

241 SCA relied on the International Business department for the following functions:

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 customer's FMAs; and

c. facilitating applications from junket operators to determine their suitability to operate junket programs.

242 In facilitating junket programs, SCA provided table 3 and table 1, section 6 designated services to customers through junket channels in both Australian dollars and, on limited occasions, HKD.

ML/TF risk of Junkets

243 The provision of designated services by SCA to customers through junket channels at the SCA casino involved higher ML/TF risk because:

a. higher value gaming services were provided by the SCA casino through the junket programs;

b. junket programs often involved the movement of large amounts of funds across foreign borders, and, depending on the specific junket program, may have involved the use of multiple bank accounts, including by third parties, which could obscure to the SCA casino the identities of persons conducting the transactions through junket programs and the source and ownership of funds used in the junket;

c. on a per-transaction and per-customer basis, the junket tour operations sector was exposed to the risks associated with high-value cash activity;

d. junket operators used formal (for example, corporate junkets or remittance companies) or informal systems to remit money (for example, third parties);

e. inherent in the junket tour operators' sector was exposure to some higher ML/TF risk jurisdictions. In particular, there were vulnerabilities associated with jurisdictions with currency flight and gambling restrictions in place as these measures could create demand for covert money remittances which could be exploited by criminal groups. As the junket customer base was comprised of predominantly foreign residents, this could increase the junket sector's attractiveness and exposure to transnational serious and organised crime, and could mean that the source of funds, designation of funds and information about customers' criminal and financial activity were difficult to identify as the junket participants were located in foreign jurisdictions;

f. the contractual arrangements (including financial arrangements) between a junket operator and their junket player(s) were not disclosed to SCA;

g. junket players generally relied on the junket operators to make their funds available at the SCA casino, including through CCFs;

h. there could be a lack of transparency and level of anonymity occasioned by the long and complex value chains associated with the flow of junket-related funds, the pooling of junket players' funds by the junket operator and conduct of all players' funds and transactions under the name of the junket operator, and the provision of cash to players in circumstances where the source of funds and purpose for which the cash was used may be unknown. Each junket player's gaming activity was not individually tracked and recorded against that particular individual while playing on the junket, which could obscure the activity of the individual junket players from SCA under such programs. As a result, SCA was not able to identify the level of gaming activity by individual junket players when they were gaming as part of a junket program;

i. junket programs could be vulnerable to cuckoo smurfing and structuring; and

j. funds deposited into a junket operator's FMA at the SCA casino and withdrawn with minimal gaming activity could give the appearance of legitimacy. In addition, any 'parking' of illicit funds could put distance between the act or acts that generated the illicit funds and the ultimate recipients of those funds, making it difficult to trace the flow of funds or the transaction chain.

244 Gaming activity at the SCA casino was reduced due to COVID-19 related travel restrictions and lockdowns from around March 2020 to January 2021. Between 22 March 2020 and 4 October 2020, junket play ceased entirely, and no designated services were provided to junket programs. This was due to border restrictions relating to COVID-19. On 12 April 2021, an 'international business strategic review' paper was submitted to the SCEG Board, in which management recommended SkyCity "*no longer work with group operators or junkets in their historical form"*. The reasons in the paper included that "*from a regulatory perspective, it is unlikely to be tenable to continue with junkets or group operators in their historical form*." In response, the SCEG Board determined to permanently cease dealing with junket operators across the SCEG Group and, accordingly, SCA ceased all junket operations business at that time (with the last junket program taking place on 2 January 2021).

F.4.2 Junkets and the Rules

245 Between 7 December 2016 and 12 April 2021, SCA provided items 6, 7, 31 and 32, table 1, section 6 of the AML/CTF Act designated services and table 3, section 6 of the AML/CTF Act designated services to junket operators, junket representatives and junket players.

246 Paragraphs 8.1.3, 8.1.4, 8.1.5(3) to 8.1.5(5) and 15.4 to 15.11 and Chapter 4 of the AML/CTF Rules were relevant to the provision by SCA of table 1 and table 3, section 6 of the AML/CTF Act designated services during the Relevant Period to junket operators, junket representatives and junket players. The obligations relating to these provisions of the AML/CTF Rules are set out in detail at paragraphs 80a to 80c and 80l to 80o.

F.4.3 Risk Assessments with respect to junkets

247 As set out at paragraphs 99 to 119, SCA identified and assessed the ML/TF risk associated with the provision of designated services through junket channels in the same manner as it identified and assessed its ML/TF risk for the general designated services it provided at the SCA casino. SCA accepts that it did not carry out a specific risk assessment of the higher ML/TF risk of providing designated services through the junket channel in the period from 7 December 2016 to 12 April 2021.

248 The Risk Assessments are set out above at Section F.1. Below is a summary of certain matters considered by SCA in its Risk Assessments with respect to junkets. There was no ML/TF risk identified as specific to junkets with respect to designated services and foreign jurisdictions.

249 The 2014 Risk Assessment included Attachment 1, which was referred to under the heading 'Casino ML typologies' and stated that Attachment 1 "*sets out some of the broad ML typologies using a pictorial flow chart and acts as a general reference tool for understanding how ML might occur in a casino context*". Attachment 1 identified the following risks related to junket programs under the heading, 'Rewards & Commission Programs':

> "Refining/Converting Illicit Funds" [type] – "Illicit cash funds are used to wager under individual or group commission programs, and winnings and commission earned are combined and redeemed for high denomination cash" [method];
>
> "Concealing Illicit Funds as Winnings" [type] – "Illicit cash funds are used to wager under individual or group commission programs, and winnings and commission earned are combined and redeemed for an Adelaide casino cheque" [method]; and

"Layering Illicit Funds" [type] – "Illicit funds are transferred to deposit account [sic] via wire transfer, to wager under individual/group commission programs with winnings and commission earned transferred to a domestic or off-shore account through wire transfer" [method].

250 The Risk Allocation Criteria that were included in the 2015 Standard Part A Program stated that SCA was to accord "*any customer who visits [the casino] in their capacity as a junket operator/representative or player*" a moderate risk rating; and accord "*any customer who visits [the casino] in their capacity as a junket operator/representative or player on more than three occasions throughout the year*", a high risk rating.

251 The 2014 Risk Assessment also included under the heading, 'Treating risks (mitigating, managing, control, monitoring and periodic reviews)' the following:

a. "*[…] junket operators require the approval of the regulating authority in Adelaide*"; and

b. as part of its risk evaluation process, SCA was to verify the identity of all participants on a junket program and was to undertake a PEP database check to determine whether the junket operators/representatives and players were PEPs and/or from a high risk jurisdiction.

ML/TF risk factors – customer types

252 Despite the higher ML/TF risks associated with junkets, between 7 December 2016 and February 2021, customers receiving designated services through junket programs were not considered high risk by default.

253 As stated at paragraph 250, the Risk Allocation Criteria included in the 2015 Standard Part A Program provided that junket operators, junket representatives and junket players were to be rated 'moderate' risk, unless they attended SCA in that capacity on more than three occasions throughout the year (then they were rated 'high' risk).

254 Between 2017 and 2021, junket representatives and junket players were to be rated 'moderate' risk according to the Risk Allocation Criteria in the 2017-February 2021 Standard Part A Programs. Further steps could be taken to consider whether the customer risk rating needed to be elevated in accordance with the factors set out in Risk Allocation Criteria, however these escalation procedures were inadequate for the reasons set out at paragraph 256.

255 It was not until February 2021, that junket operators were to be rated high risk by default for the purpose of the AML/CTF Act and the AML/CTF Rules.

256 At no time did the Standard Part A Programs set out specific escalation procedures to determine whether the customers receiving designated services through the junket channel should have been rated higher risk, having regard to the customer's specific ML/TF risk.

ML/TF risk factors – channels

257 While the 2017-February 2021 Standard Part A Programs identified junket operators, junket representatives and junket players as a standalone 'customer type', the 2015-February 2021 Standard Part A programs did not clearly identify junkets as a channel through which SCA provided designated services.

Cheque Cashing Facilities

258 From 7 December 2016 to 12 April 2021, SCA provided some junket operators with CCFs. From 14 February 2017, a junket operator could delegate authority to operate the CCF to a junket representative, either up to the full amount of the approved CCF or some lesser

specified amount. The matters referred to in Section F.3.5 are repeated here in relation to the provision of CCFs to junket operators or representatives.

Remittance

259 From 7 December 2016 to 12 April 2021, SCA provided remittance services (items 31 and 32, table 1, section 6 of the AML/CTF Act designated services) through junket channels. The matters referred to above in Sections C.5.2 and F.3.1 (FMAs), C.5.4 and F.3.2 (SCA Customer account channel), C.5.5 and F.3.3 (SCEG Customer account channel) and C.5.6 and F.3.4 (SkyCity New Zealand channel) and paragraphs 164 to 165 (FMA to FMAs) are repeated here with respect to remittances services through junket channels.

260 As set out above at paragraphs 164 and 165, from 14 February 2017 to 12 April 2021, a junket operator was able to provide 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. SCA also permitted transfers in the following circumstances:

a. a junket operator to a junket player's FMA;

b. a junket player to a junket operator's FMA;

c. a junket representative to another junket representative's FMA;

d. a junket representative to a junket player's FMA; and

e. a junket player to a junket representative's FMA.

The deficiencies with the Funds Authorisation Form are set out at paragraph 231c above.

F.4.4 VIP Gaming Areas/Premium Customers

261 Junket game play was conducted in VIP gaming areas at the SCA casino. The use of premium gaming areas is described at paragraphs 27 to 30. At no time did junkets have exclusive unsupervised access to a permanently allocated VIP gaming area. An FMA was automatically established at the time a junket operator, junket representative or junket player became a member of SCA's loyalty program. As all junket operators, junket representatives and junket players were required to join SCA's loyalty program to enter the premium gaming rooms, they each held respective and individual FMAs and were subject to the KYC requirements applicable to all customers holding an FMA (see Section F.9, which also sets out deficiencies with respect to SCA's Standard Part B Program).

262 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**). As part of SCA's TMP, SCA had a Front Money Balance Report which sought to identify funds left dormant (as described below in Section F.6). However, there was no clear criteria or document with respect to considering this report (see paragraph 321i). Otherwise, there were:

a. no other processes, procedures or controls to manage dormant FMAs; and

b. no transaction or daily limits on the amount of funds 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.

263 At all times during the Relevant Period, the systems and controls outlined at paragraphs 225 and 226, and Sections F.6.3 to F.6.7 (with respect to TMP), F.7.2 to F.7.2.2 (with respect to ECDD), F.8.2 to F.8.3 (with respect to reporting obligations) and F.9.2 (with respect to ACIP) applied to junkets gaming in VIP gaming areas. The deficiencies with respect to those

systems and controls are outlined at paragraphs 228 to 234 and Sections F.6.8 (with respect to TMP), F.7.2.3 (with respect to ECDD), F.8.4 (with respect to reporting obligations) and F.9.3 (with respect to ACIP).

F.4.5 ACIP/KYC processes/PEP screening / other processes for junkets

264 At all times, junket operators, junket representatives and junket players were subject to the same due diligence requirements and PEP screening checks that applied to all customers, as set out in the Standard Part A and Part B Programs (see paragraph 383 in relation to PEP screening).

265 Prior to SCA providing designated services to junket operators, junket representatives and junket players, they were subject to the same ACIP procedures that applied to other customers as set out in the Standard Part B Programs (as described in Section F.9.2). The ACIP for junket operators, junket players and junket representatives was to be carried out by the International Business team (International Business Host or International Business Manager) immediately upon arrival at the SCA casino and before funds were deposited into the junket operator's FMA.

266 Prior to SCA providing designated services to a junket operator, junket representative or junket player, they were each screened against a global PEP database as outlined in paragraph 384.

267 From around October 2019, SCA implemented a SOP which stated that a law enforcement agency and another government agency "must be sent a photo board of the Junket and its participants prior to play". The AML Advisor and International Business Team were responsible for completing the reporting. This process was not directed at SCA's ML/TF risk or compliance with the AML/CTF Act.

268 From 1 August 2019, junket operators proposing to visit the SCA casino were required to have completed and passed a suitability assessment in New Zealand prior to attending the SCA casino. Up until July 2018, the suitability assessment for junket operators was conducted by the New Zealand government agency pursuant to legislation in force in that country. From July 2018 onwards, the suitability assessment was conducted by SkyCity New Zealand and submitted to the New Zealand regulator for approval. From 1 August 2019, junket operators proposing to visit the SCA casino were required to have completed and passed a suitability assessment in New Zealand prior to attending the SCA casino. The suitability assessment included the completion of an application form, which included:

a. submission of identification documents;

b. the name of the applicant's current employer/business, including the start date, city, country and job title;

c. obtaining a police clearance certificate (or a statutory declaration that such a certificate was not obtainable from the applicant's jurisdiction); and

d. answering questions about the applicant's personal history, including:

   i. details of any disqualifications from management of a company, bankruptcy, fraud, and civil proceedings relating to financial matters; and

   ii. whether the applicant had ever been a member of an organisation refused a gambling licence in any country, whether the applicant had ever been refused a gambling licence in any country and details of junkets held at other casinos.

269 Successful applicants were required to apply for renewal every two years.

270 SCA accepts that, from 1 August 2019, there was no framework 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. SCA's reliance on SCEG personnel conducting due diligence on prospective junket operators and considering whether they were suitable to conduct business with did not have specific regard to SCA's ML/TF risk appetite, nor did SCA take steps to satisfy itself that the assessment conducted by NZ would appropriately satisfy SCA's obligations under Australian law.

271 All junket participants were subject to PEP screening (as set out at paragraph 383). Prior to arrival at the SCA casino, or on arrival, all junket participants provided SCA with copies of identity documents. Those identity documents were then used by the AML team to conduct manual checks of the junket participants against the Dow Jones database (via the Jade System) to identify whether they were a PEP, on a terrorism or sanctions list or otherwise subject to adverse media. The *PEP Screening Standard Operating Procedure* dated 17 September 2019 set out operating procedures relating to PEP screening.

F.4.6 Transaction Monitoring and Transaction Limits with respect to junkets

272 At all times throughout the Relevant Period, SCA applied its TMP to junket program participants as a whole, by monitoring transactions recorded against the junket operator (SCA's TMP is described at Section F.6.3 to F.6.7). At no time did SCA monitor the gambling activity of individual junket players, rather, SCA maintained a documented record of transactions and turnover generated by each junket program as a whole for the purposes of paying commissions or rebates to the junket operator. SCA's TMP did not include appropriate risk-based systems and controls to monitor the transactions of customers receiving designated services through junket channels.

273 On and from 7 December 2016, and pursuant to its casino licence, SCA had in place the *Adelaide Casino Control Standards Cash Handling Operating Procedures – CH 09* (**CH 09**). CH 09 applied to all cash handling staff performing duties in relation to the operation of commission-based gaming. CH 09 stated under the heading, 'Commission Programs':

> From the commencement of play, until the player(s) advise that they are ceasing play, all player(s) turnover will be recorded by a Table Games Supervisor or Cash Handling Department representative. The player(s) turnover will be recorded using a Premium Player Rating Sheet or an approved electronic recording device, and subsequently summarised on a Commission Program Summary Sheet or an approved electronic reporting system. The player(s) turnover will be tracked by the Table Game Supervisor using the Casino electronic monitoring system which will include the factors of average bet and length of play.

274 At all relevant times, SCA distributed specific gaming chips, being non-negotiable or commission branded chips, to junket operators and junket representatives so that only junket players were entitled to use those chips. SCA's failure to monitor the gambling activity of each junket player individually meant that SCA did not have visibility of how gaming chips were distributed amongst junket players.

275 Between December 2015 and April 2021, where the junket operator presented cash to buy in on behalf of a junket, SCA required junkets to complete a Group Funds Disclosure Form (**GFDF**). The GFDF stated that the junket operator or representative must provide the information prior to commencing game play. The GFDF set out the funds each junket player contributed to the cash buy-in. However, SCA had no documented process to analyse the GFDFs. Junket players could only conduct cash transactions through junket operators or junket representatives.

276 At the conclusion of a junket program, SCA paid any winnings to the junket operator or junket representative in cash, cheque, by electronic transfer to their FMA, including at another SCEG casino, or by bank transfer. The junket operator or junket representative paid

winnings to players of that junket program pursuant to agreements between them, to which SCA was not privy.

Observation reports

277 As set out at paragraphs 350 to 353, observation reports were prepared by frontline staff to monitor customer behaviour for indicators of illicit activity, including in relation to junkets.

AML/CTF reporting obligations with respect to junkets

278 At all relevant times, SCA's 2015-February 2021 Standard Part A Programs included certain systems and controls in place to identify and report SMRs, TTRs and IFTIs, including those concerning the provision of designated services to junkets (as described at Section F.8.2 and F.8.3). However, those systems and controls were not appropriate to ensure compliance with SCA's obligations as set out at Section F.8.4.

F.4.7 Non-compliance with paragraphs 8.1.3, 8.1.4, 15.5, 15.9 and 15.10 of the AML/CTF Rules

279 Between 7 December 2016 and 12 April 2021, SCA did not independently assess all ML/TF risk associated with providing designated services to junket operators, junket representatives and junket players. In particular, SCA accepts that failing to independently assess the ML/TF risk of junket programs contributed to SCA's contravention of paragraphs 8.1.3, 8.1.4, 15.5, 15.9 and 15.10 of the AML/CTF Rules because:

a. although SCA identified some ML/TF risk arising with respect to play through junkets generally and had in place certain systems or controls more generally (as described above at paragraphs 225 and 226), SCA did not identify, mitigate or manage all of the specific ML/TF risks that arose with respect to the complex operational structure of junket programs and the provision of designated services to junket operators, junket representatives and junket players;

b. notwithstanding the higher ML/TF risk associated with junkets, the systems and controls that applied to the provision of designated services to junkets were generally no different to the risk-based systems and controls that applied to other customers and did not sufficiently have regard to the ML/TF risks that were unique to the provision of designated services to junket programs;

c. the relationship and contractual arrangements between the junket operator, junket representative and junket players were not clear to SCA as SCA entered into GCPAs with junket operators and not the junket players. As such, SCA's systems and controls to mitigate and manage ML/TF risk with respect to the junket player were not appropriate. For example, SCA's Standard Part A Programs did not:

    i. set out adequate escalation procedures for junket programs to determine whether the junket operator, junket representative or junket player should have been assigned an elevated risk rating, having regard to junket-specific ML/TF risk;

    ii. provide for the assessment of jurisdictional risks associated with customers receiving designated services through the junket channel;

    iii. include appropriate risk-based systems and controls to obtain and analyse source of wealth and source of funds information with respect to junket operators, junket representatives and junket players. In particular, SCA did not have oversight of the payment of winnings from the junket operator or junket representative to junket players. The payment of winnings from the junket operator or junket representative was based on agreements between the junket

operators or junket representative and the junket players, to which SCA was not privy; and

iv. include appropriate risk-based systems and controls to collect and verify information with respect to junket operators and other customers receiving designated services through junket channels, in particular, with respect to the beneficial ownership of funds or the beneficiaries of transactions being facilitated by SCA on behalf of junket operators, including the distribution and destination of funds within the junket program;

d. the default ML/TF risk rating of 'moderate' for junket operators (from February 2017 until February 2021), junket representatives and junket players (from 7 December 2016 until April 2021) was not appropriate having regard to the ML/TF risks associated with junket programs;

e. at no time did SCA monitor the gaming activity of individual junket players. The gambling activity of junket players was recorded by SCA collectively under the junket program, and not on an individual player basis. Failure to monitor the gambling activity of each junket player individually meant that SCA had no visibility over how gambling chips were distributed amongst junket players;

f. as gaming records of junket players were not recorded, SCA was unable to form a complete overview of the customer's gaming activity which formed a part of their ML/TF risk profile, meaning that SCA may not have identified transactions that appeared to be suspicious within the terms of section 41 of the AML/CTF Act for the purposes of paragraph 15.5 of the AML/CTF Rules; and

g. as a result of the structure between the junket operator, junket representative and junket player, in some circumstances, SCA did not apply its ECDD Program when required pursuant to paragraph 15.9 of the AML/CTF Rules. Where ECDD was applied, the ECDD that was undertaken was, at times, deficient as it was not appropriate to the circumstances as required by paragraph 15.10 of the AML/CTF Rules.

280 The Standard Part A Programs did not 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, section 6 designated services) because:

a. there was no framework in place in the Standard Part A Program for SCA to determine whether decisions with respect to the approval of CCFs or lines of credit, including credit limits, for junket operators were within SCA's risk appetite. The absence of such a framework meant that when a customer applied for credit, SCA's risk assessment was largely focused on credit risk not ML/TF risk;

b. SCA did not have any processes in place to identify how CPVs, gambling 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;

c. SCA had no visibility as to how the junket operators funded junket players' FMAs or how junket operators distributed winnings to junket players;

d. a CCF or line of credit was opened in the name of the junket operator. Once approved, the funds were credited to the junket operator's FMA. From 14 February 2017, a junket representative could conduct transactions on a junket operator's FMA, where a written authorisation form was in place. A junket operator could delegate authority to operate the CCF to a junket representative, either up to the full amount of the facility or some lesser specified amount. Following each drawdown of a line of

credit by the junket operator, the CVIs issued by SCA for use in the relevant junket program would be provided at the junket operator's or representative's discretion to the junket players. There was a lack of transparency and level of anonymity created by the pooling of all players' funds and transactions, including any CCFs or lines of credit provided to the junket operator, under the name of the junket operator;

e. the Standard Part A Programs did not include appropriate controls to identify, mitigate and manage the ML/TF risk associated with providing remittance services through junket channels for the following reasons:

    i. at no time did SCA appropriately identify and assess the ML/TF risk of transactions on FMAs held by junket operators or representatives; and

    ii. records of winnings by junket players were unreliable because there was a lack of transparency and level of anonymity because of the long and complex value chains associated with the flows of junket-related funds, and the pooling of players' funds, credit and transactions under the name of the junket operator;

f. transactions through junket channels involved higher ML/TF risk because:

    i. the funds could be remitted out of SCA following play on a junket program, in circumstances where the source of funds was not clear;

    ii. the funds could be remitted across international borders using one of the SCEG Customer accounts, obfuscating that the funds originated in Australia; and

    iii. the junket operators could disburse the funds to third parties, including junket players, with no oversight from SCA,

    however, for the reasons set out at paragraphs 113 to 116, SCA did not identify, mitigate or manage ML/TF risks associated with providing these services involving complex transaction chains;

g. the Standard Part A Programs did not have any specific processes in place to identify or maintain oversight in relation to how junket operators or representatives were distributing CVIs to junket players where a CCF was opened in the name of a junket operator;

h. the Standard Part A Programs did not include appropriate controls to identify, mitigate and manage the ML/TF risk associated with large cash transactions through junkets, including ML/TF risks associated with source of wealth and source of funds, for the following reasons:

    i. SCA did not carry out an appropriate ML/TF risk assessment with respect to the risks associated with the provision of designated services within the VIP gaming rooms used to facilitate junket programs;

    ii. the GFDF required to be completed for cash buy-ins made on behalf of a junket, which identified the junket player(s) who contributed to the cash buy-in and the amount that each contributed, was not an adequate control on its own to manage the ML/TF risk associated with large cash transactions through junkets. SCA had no documented process to analyse the GFDF; and

    iii. the processes to collect source of funds information were not appropriate (as described above at paragraph 279c.iii);

i. aside from collecting ACIP information and conducting PEP screens, SCA conducted no independent due diligence on prospective junket operators and was reliant on due

diligence conducted by SCEG personnel, and therefore did not consider whether junkets were suitable to conduct business with, having regard to SCA's ML/TF risk appetite; and

j. the Standard Part A Programs did not include or incorporate a framework to determine whether decisions relating to SCA customers or designated services provided by SCA through junket channels were within the ML/TF risk appetite of SCA (see paragraphs 239 to 241), including in relation to 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.

F.5 Individual Commission Programs

F.5.1 Overview

281 As described above at Section C.8, an ICP is an arrangement between an interstate or international customer who had agreed to participate in an ICP when gaming at the SCA casino.

282 The provision of table 1 and table 3, section 6 of the AML/CTF Act designated services by SCA to customers through ICPs involved higher ML/TF risk because:

a. ICPs could involve high volume and high value gambling;

b. ICPs exclusively used CVIs;

c. ICP customers were eligible to apply for CCFs and lines of credit for gaming purposes;

d. SCA facilitated third party deposits for ICP customers when an ICP player had provided written authorisation via a Funds Authorisation Form, to transfer funds from their FMA to another ICP player's FMA (as described above at paragraph 164);

e. SCA facilitated ICP customers using foreign cheques; and

f. ICPs could be vulnerable to refining, converting or layering of illicit funds.

283 SCA continued to provide designated services to international VIPs via ICPs after ceasing its junket business in April 2021.

F.5.2 ICPs and the Rules

284 The following AML/CTF Rules were relevant to the provision by SCA of table 1 and table 3, section 6 of the AML/CTF Act designated services during the Relevant Period to individual commission players.

Transaction Monitoring

285 Paragraphs 15.5 to 15.7 of the AML/CTF Rules, which outline SCA's obligations for its TMPs, are set out at paragraph 80l.

F.5.3 SCA's Transaction Monitoring Program in relation to ICPs

286 At all times during the Relevant Period, SCA applied its TMP to ICP customers.

287 Under a TURN Program, each wager placed by a customer that had a win/loss result was recorded as turnover and then all relevant wagers were calculated in order to provide the total cash turnover. All wagers were manually recorded and tallied on an approved

document by a table games staff member who had direct supervision of each bet that was placed by the ICP player at the relevant table game. This document was then provided to Cage staff for the purposes of entering the turnover into the player's account in the Bally CMP System as 'cash turnover'.

288 Under a NNEG Program, each player placed their wagers using NNEG chips. Any winning wagers were paid out to the customer in commission chips with the player also retaining the NNEG chips used for their initial wager. If the customer lost, then the dealer would retain the NNEG chips. In the event of a tie, no chips were issued but the player retained their NNEG chips used to wager. Prior to July 2018, each chip exchange was recorded manually on an approved document by the Table Games staff at the relevant gaming table. This document was then provided to Cage staff for entry in the Bally CMP System as 'NNEG turnover'. Since July 2018, chip exchange transactions have been entered directly into the Bally CMP System by Table Games staff.

F.5.4 ICP related contraventions

289 SCA did not maintain accurate records of the designated services SCA provided through ICPs (as set out above at paragraphs 287 and 288), including records of the gambling activity of ICP players playing on NNEG programs, including amounts wagered, winning bets and losing bets. In those circumstances, SCA was unable to adopt and maintain appropriate risk-based systems and controls to monitor the provision of designated services to its ICP players. 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 table 3, section 6 of the AML/CTF Act designated services to ICP customers.

F.6 Transaction Monitoring Program

F.6.1 SCA's obligations in relation to Transaction Monitoring Programs

290 At all times during the Relevant Period, SCA was required to have a TMP in place that complied with the requirements described at paragraph 80l.

F.6.2 Standard Part A Programs - TMPs

291 At all times during the Relevant Period, SCA's Standard Part A Programs included a TMP (**SCA's TMPs**).

292 SCA's TMPs were set out in:

a. section 12, including table 2, of the 2015 Standard Part A Program; and

b. subsections 5 to 13 of section 13, including schedules 4 and 5, of the 2017-2021 Standard Part A Programs.

293 The Standard Part A Programs also included sections that were supported by SCA's TMPs. Those sections were concerned with reporting suspicious matters to AUSTRAC, setting out certain Risk Allocation Criteria and SCA's ECDD Program.

294 SCA's TMPs were supported by procedural documents that provided guidance on the operation of SCA's TMPs (although these procedures were not expressly referred to in the Standard Part A Programs).[26] These documents identified when and how certain transaction

[26] 'AML Unusual Changes in Betting Habits SOP' dated 28 March 2017; 'AML Analyst Role' document dated 6 November 2017; and the 'AML Advisor Role' document dated 12 May 2020.

monitoring rule alerts should be run in SCA's information management systems and provided for the recording and reviewing of several transaction monitoring reports.

295 SCA relied on the data collected through its TMP to determine if transactions of customers were suspicious for the purposes of section 41 of the AML/CTF Act. SCA also relied on reports generated from Bally to determine if customer risk ratings should be elevated, based on what was revealed in the reports (as described at paragraphs 300 to 307) with respect to customer transactions and whether any of the elevation triggers in the Risk Allocation Criteria were met.

296 SCA accepts that, between 7 December 2016 and 17 November 2022, SCA's TMP did not at all times fully comply with all of the requirements of the AML/CTF Rules, for the reasons described in paragraphs 319 to 322. As a result of the deficiencies in SCA's TMPs between 7 December 2016 and 17 November 2022, SCA contravened section 84(2)(c) of the AML/CTF Act.

F.6.3 SCA's TMPs

297 SCA's TMPs included both manual and automated processes, which were supported by the following information management systems: the Bally CMP System and the Jade System (see paragraphs 33a and 33d above). The systems assisted SCA in monitoring the transactions of SCA's customers. Within the Jade System was the Jade IT system which included an automated transaction monitoring tool. That tool assisted SCA to facilitate PEP screening, transaction monitoring and reporting functions.

298 As part of its manual processes, SCA's TMPs also comprised of:

a. manual review of system-generated reports;

b. observation reports submitted by frontline staff to the AML team;

c. from February 2017, manual review of the Jade System transaction monitoring rule alerts; and

d. the reporting of certain results of these processes to the AML/CTF Senior Management Group.

299 Other systems or controls included or incorporated in SCA's TMPs to monitor the transactions of customers are also described at paragraph 315.

F.6.4 The Bally CMP System

300 Bally consisted of the Bally CMP System and the Bally Cage System. These systems are described at paragraphs 33a and 33b above.

301 The types of transactions and information recorded in the Bally CMP System included, but were not limited to, transactions in and out of customers' FMAs, IFTIs recorded by the Cage staff, cheques issued to customers at the Cage, EGM and ETG gaming activity such as 'cash inserted or collected' and 'machine turnover' (where the customer had used their loyalty membership card), currency exchanges of $1,000 or more (unless the customer presented their membership card to get a better exchange rate, in which case all currency exchange would be recorded in the Bally CMP System), and certain exchanges of money for chips where the customer presented their loyalty membership card at the time of the transaction.

302 As set out at paragraph 83 above, pursuant to Chapter 10 of the AML/CTF Rules, SCA was, at all times, exempt from certain KYC, verification and record keeping obligations under the

AML/CTF Act with respect to the provision of certain types of designated services that were less than $10,000.

303 When a customer played 'uncarded', SCA would not monitor transactions of less than $10,000 except in the following circumstances:

a. until 23 February 2017, table games staff had a discretion to monitor the play of uncarded patrons by creating an 'uncarded' account for a customer in a particular session in the Bally CMP System. The 'uncarded' account would record the gaming activity of non-loyalty members or members who had not disclosed their loyalty card and could, include transactions less than $10,000; and

b. if a loyalty member did not present their membership card at a table game but the customer was identifiable by SCA staff, then the staff member would, in certain instances, track and record their play against their membership number in the Bally CMP System. This could include transactions less than $10,000.

304 SCA accepts that the approach to monitoring transactions of less than $10,000 for uncarded play was ad hoc and resulted in limited and inaccurate records of transactions that were less than $10,000.

F.6.5 The Bally CMP System generated transaction monitoring report

305 Data from the Bally CMP System was used by SCA to manually generate transaction monitoring reports, which were to be manually reviewed against certain indicators of ML/TF risk.

306 Deficiencies in SCA's Standard Part A Programs (and other operational documents relating to SCA's TMPs) in relation to review criteria and the process for the persons responsible for reviewing the reports meant that SCA did not consistently monitor its customers with respect to the ML/TF risk it reasonably faced.

307 The reports generated by the Bally CMP System as described in Table 2 of the 2015 Standard Part A Program and Schedule 4 of the 2017-2021 Standard Part A Programs (the **Transaction Monitoring Table**) included, for example: [27]

a. **Transaction Listing Report**: A report that sought to identify transactions of $10,000 or more to assess significant cash deposits or chip purchases and changes in transaction patterns that might warrant further analysis; foreign exchange transactions of $1,000 or more to assess significant and/or frequent exchanges which might be inconsistent with a customer's known gaming activity and background; and significant expenditure and/or changes in customer spend inconsistent with the customer's profile which might suggest access to illicit funds and/or risk that transactions were unrelated to gaming activity.

b. **Front Money Balances Report**: Between February 2017 and 2019, SCA commenced generating a 'Front Money Balances' Report, which was to be reviewed monthly. The report sought to identify accounts containing $10,000 or more that had unusual activity or funds left dormant for extended periods.

c. **IFTI Transaction Report**: The indicators described in the Transaction Monitoring Table were "transfers to and from high-risk countries with weak AML controls" and "frequent transfers". The report sought to cover all international transfers to review

[27] The full list of reports was the Transaction Listing Report, Foreign Exchange Transactions Report, Cheque Transactions Report, Inventory Movement Report; Major EGM Jackpots Report; a report identifying changes in betting habits; Reports identifying cash buy-ins greater than $100,000 and customers who made more than five threshold transactions; Reports identifying cash buy-ins greater than $100,000 and customers who made more than five threshold transactions; IFTI Transaction Report; Front Money Balances Report..

jurisdiction source, destination of funds, the frequency and context of transfers, and their relationship to gaming activity. The report was to be reviewed manually daily and monthly.

F.6.6 Jade System

308 The Jade System as described at paragraph 33d above, generated transaction alerts triggered by transaction rules, which were used by SCA as part of its TMPs. An example of one of the Jade rules was that all transactions between $6,000 and $9,000 were to be captured and recorded in a report for consideration (however, see paragraph 321i with respect to the adequacy of data recorded for transactions under $10,000).

309 In addition to the transaction alerts that were generated, SCA was also able to manually run other transaction monitoring rules periodically within the Jade System for the purpose of monitoring its customers' transactions.

310 The Jade System relied on data entered from the Bally CMP System, which captured the transactions set out at paragraph 301 above. However, due to limitations with the data maintained and recorded for transactions under $10,000 (and see paragraph 304 with respect to monitoring transactions of less than $10,000 for uncarded play) the Jade System was not operationally effective to monitor SCA's customer transactions with respect to ML/TF risk.

311 The Jade System was also used to identify PEPs and adverse media about a customer. Subsection 6 of section 19 of the 2017-2021 Standard Part B Programs stated that individual customers who were provided a designated service that met certain transactional criteria were to be screened against the Dow Jones database available via the Jade System.

312 Reports identifying customers who returned a possible PEP match and/or adverse media searches and containing transaction alerts which had been triggered by the transaction rules were generated by the Jade System and were to be provided to the AML Analyst, Compliance Manager, AML Compliance Manager, and Legal and Compliance Advisor to determine whether further analysis or an elevation of customer risk rating was required.

313 The results of reviews of transaction alerts generated by the Jade System were to be recorded in the Jade System. As stated at paragraph 33d above, the Jade System was also used to record customer information, such as a customer's risk ratings, customer identification, and PEP screening records. With respect to the elevation of a customer's risk rating, see explanation of the Risk Allocation Criteria at paragraphs 101 and 102. The Risk Allocation Criteria included certain transaction criteria that could result in a customer's risk rating being elevated to high or significant risk, for example, transactions greater than $250,000 over the course of a month.

314 SCA's TMPs did not specifically set out how transaction alerts generated by the Jade System were to be reviewed and considered against a customer's ML/TF risk profile to ensure consistent assessments of the customers' transactions.

F.6.7 Other systems and controls included or incorporated in SCA's TMPs to monitor the transactions of customers

315 In addition to the processes explained in paragraphs 297 to 313, SCA's TMPs also included or incorporated:

a. frontline staff observations of customer transactions and observation reports submitted by frontline staff to the AML team where unusual behaviour was observed. Further information on observation reports is set out at paragraphs 350 to 352;

b. section 12 of the 2015 Standard Part A Program provided that the transactions and reports specified in Table 2 of the 2015 Standard Part A Program were to be monitored and reviewed to assist the AML/CTF Senior Management Group in determining whether a customer should forego their default rating of low risk and be accorded an elevated risk rating, and whether there were grounds for lodging an SMR;

c. subsection 11 of section 13 of the 2017-2021 Standard Part A Programs under the heading 'system generated reports' stated that the results of the TMP were to be used to review the level of risk accorded to customers, and that the AMLCO was to determine whether there were reasonable grounds to lodge an SMR; and

d. reporting of the results of the manual review of system-generated reports or the Jade System transaction monitoring rule alerts to the AML/CTF Senior Management Group. From May 2017, this was by way of a report titled 'Transaction Monitoring Overview', which was provided to the AML/CTF Senior Management Group for discussion at its quarterly meetings. The report contained details of the outcome of the transaction monitoring alerts and reports generated during the period (from the date of the previous meeting up to the current meeting). The meeting agenda was accompanied by a document which contained high level details of specific transactions and customers, and also identified some transactions and customers that potentially presented a higher risk for further consideration by the AML/CTF Senior Management Group.

316 SCA's AML team reviewed three separate daily reports which provided an overview of cashless transactions, namely cashless transactions equal to or above a $5,000 threshold, including those that were conducted via EZYPlay Guest Cards (if any); transactions conducted on each CRT; and jackpots paid to all customers.

F.6.8 Non-compliance of SCA's TMPs

317 Pursuant to paragraph 15.5 of the AML/CTF Rules, SCA was required to include appropriate risk-based systems and controls to monitor the transactions of customers in its TMPs. Pursuant to paragraph 8.1.3 of the AML/CTF Rules, when determining and putting in place appropriate risk-based systems and controls, SCA was to have regard to the nature, size and complexity of its business and the types of ML/TF risk it might reasonably face.[28]

318 As described in Section F.1 above, SCA did not appropriately assess the ML/TF risks associated with its provision of designated services. As a result, as described in paragraphs 319 to 321 below, the systems and controls in the TMPs were not able to appropriately address the ML/TF risk that SCA faced across all designated services.

319 Between 7 December 2016 and 17 November 2022, SCA did not include appropriate risk-based systems and controls in its TMPs to monitor the transactions of all its customers, for the reasons set out below:

a. SCA's processes and procedures, including the manual and observational processes in SCA's TMPs, to identify transactions that met the Risk Allocation Criteria in the Standard Part A Program which would require a customer to be risk-rated above 'low' were not adequate to ensure that a customer's risk rating was commensurately elevated by SCA where required;

b. SCA's TMP did not consistently identify transactions that may be suspicious and were required to be considered further for the purpose of section 41 of the AML/CTF Act;

[28] See paragraphs 20-21 for an explanation of appropriate risk-based procedures, systems and controls.

c. as stated above at paragraph 272, SCA's TMPs did not apply to transactions conducted by individual junket players;

d. in relation to transactions which were conducted through the SCEG Customer account channel, the SCA Customer account channel or the SkyCity New Zealand channel, SCA did not appropriately monitor those transactions having regard to the ML/TF risks identified at paragraphs 173, 184 and 191 above;

e. in relation to the provision of CCFs, having regard to the ML/TF risk associated with providing those designated services, SCA did not appropriately monitor those transactions;

f. in relation to transactions from one customer's FMA to another customer's FMA (as described above at paragraphs 164 and 165 and in certain other circumstances), SCA was unable to consistently identify any transactions that may have been suspicious or unusual;

g. in relation to transactions on EGMs, ATGs or ETGs, as neither Jade nor Bally captured any EGM or ETG transactional activity where customers were playing 'uncarded';

h. other than by way of observation by SCA staff, only limited transaction monitoring was applied to EZYPlay Guest Cards and SCA did not have adequate controls to identify indicators of the various ML/TF risks that EZYPlay Guest Cards were susceptible to, as set out at paragraph 209 above;

i. SCA's TMPs 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; and

j. SCA's TMPs did not include or incorporate sufficient risk-based systems and controls for assurance. As a result, SCA did not have in place adequate risked-based systems and controls to ensure that SCA's TMPs were, in all circumstances, being applied correctly, operating as intended and remained appropriate.

320 As a result of the deficiencies identified in paragraphs 319b to 319i and 321a to 321h, SCA's TMPs did not include adequate risk-based procedures to consistently monitor all transactions of customers indicative of the following ML/TF typologies and vulnerabilities across all channels:

a. structuring on FMAs, including via the SCEG Customer accounts 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. cuckoo 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 were 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.

321 SCA's TMPs relied on manual and observational processes. Those manual and observational processes, whilst forming an important aspect of SCA's TMPs to support its automated processes, were not adequate, having regard to the nature, size and complexity of the business that SCA operated and the types of ML/TF risk that arose from that business. In particular, SCA's manual and observational processes were not capable of consistently monitoring all customer transactions to identify, manage and mitigate the potential ML/TF risk of complex, unusually large transactions and unusual patterns of transactions as these transactions may not have been observable or consistently detected using the manual and observational processes in the TMPs. This is because:

a. most of the Jade System reports or alerts were required to be manually generated, but SCA did not have processes that articulated the criteria to review the Jade System reports or alerts, the frequency or circumstances in which each rule would be run or the frequency with which each report or alert would be reviewed. Instead, these were left to the discretion of the AML Analyst;

b. there were limitations with the data used by the Jade System. For the most part, the Jade System relied on data entered from Bally CMP System, which was subject to limitations. Further, the Jade System did not link to all data from the Bally CMP System, which impacted the application of the transaction monitoring rules that could be implemented in the Jade System. The Jade System also required some information to be manually entered, which was labour-intensive and required data gaps to be filled by the AML team;

c. there were inadequate processes or procedures in place to ensure that the transaction monitoring rules were regularly reviewed and updated to respond to new or emerging ML/TF risk. As a result, the Jade System transaction monitoring rules were not at all times adequate;

d. there was no clear guidance or criteria provided to the AMLCO to monitor the reviews performed by delegates to ensure a complete assessment of the Jade System reports or alerts;

e. the manual and observational processes were focused on individual transaction data sets, and were therefore not capable of consistently detecting suspicious or unusual patterns of transactions or behaviours across complex transaction chains involving multiple designated services;

f. not all staff responsible for reviewing system-generated transaction activity reports and alerts received adequate ML/TF risk awareness training;

g. the AML team was not adequately resourced to support the consistent generation, review and actioning of system-generated reports or transaction monitoring rule alerts;

h. many of the reports were reviewed on a monthly basis only and there was no clear criteria or guidance on how to review those reports, including how to identify unusually large transactions; and

i. the system-generated transaction activity reports were reliant on data accessible from the Bally CMP System, which:

i. was overly reliant on manually entered data (except where the customer was playing on an EGM or ETG and using their membership card) which was incomplete, inaccurate or susceptible to human error. This limitation also impacted SCA's ability to consistently monitor customer transactions through table games. For example, dealers at tables were responsible for manually recording transaction data into Bally whilst facilitating table games. Due to the nature of table game play, table games staff members did not capture all transactions at table games relating to the provision of designated services pursuant to items 6 and 9, table 3, section 6 of the AML/CTF Act; and

ii. did not always contain complete records of customer transactions. In particular, the Bally CMP System had limited records of customer transactions under $10,000 unless a customer elected to play carded (that is, with their loyalty card). Therefore, SCA was unable to sufficiently monitor, among other things, transactions structured to avoid threshold transaction reporting. In addition, currency exchanges up to $1,000 and payment of winnings in relation to EGMs and ATGs under $10,000 were not recorded in the Bally CMP System. Where a customer played uncarded and engaged in a threshold transaction, this was recorded as it was required to be reported.

322 From 7 December 2016 to around 17 November 2022, SCA's TMPs did not at all times fully comply with the requirements of paragraphs 8.1.3, 8.1.4, 15.5, 15.6 and 15.7 of the AML/CTF Rules for the reasons set out at paragraphs 319 to 321. As a result, from 7 December 2016 to around 17 November 2022, the Standard Part A Programs did not comply with section 84(2)(c) of the AML/CTF Act.

323 The steps SCA has taken to uplift and enhance its AML/CTF function and compliance with respect to its TMP are set out at paragraph 505 below.

F.7 Enhanced Customer Due Diligence Programs

F.7.1 SCA's obligations in relation to ECDD Programs

324 At all times during the Relevant Period, SCA was required to have an ECDD Program in place that complied with the requirements described at paragraphs 80m to 80o.

F.7.2 SCA's ECDD Programs

325 At all times during the Relevant Period, SCA included an ECDD Program in its Standard Part A Programs (**ECDD Programs**).

326 The ECDD Programs were set out in:

a. section 17 of the 2015 Standard Part A Program;

b. subsections 5 to 12 of section 14 of the 2017-2019 Standard Part A Programs; and

c. subsections 5 to 14 of section 14 of the February-October 2021 Standard Part A Programs.

327 The Standard Part A and Part B Programs also included sections that supported the ECDD Programs. Those sections were not expressly referred to in the ECDD Programs and did not exclusively apply to the ECDD Programs. Those sections, among other things, included the Risk Allocation Criteria for assigning 'moderate', 'high' and 'significant' ML/TF risk ratings to customers and provided for PEP screening, PEP source of wealth and/or source of funds enquiries and the consideration of the business relationship with the PEP.

328 The ECDD Programs were supported by certain SOPs that provided additional guidance on the operation of the ECDD Programs (although these procedures were not expressly referred to in the Standard Part A Programs). These documents were implemented to assist SCA with complying with its ECDD obligations under the AML/CTF Rules, and included, for example, monitoring procedures for players residing in high risk countries and facilitated the centralisation of ECDD information located in multiple systems.[29]

329 SCA accepts that, between 7 December 2016 and 17 November 2022, its ECDD Programs did not at all times fully comply with the requirements in paragraphs 15.9 to 15.11 of the AML/CTF Rules for the reasons described in paragraphs 343 to 344. As a result of the deficiencies identified below in its ECDD Programs, between 7 December 2016 and 17 November 2022, SCA contravened section 84(2)(c) of the AML/CTF Act.

F.7.2.1 SCA's ECDD Programs and paragraph 15.9 of the AML/CTF Rules

330 At all times throughout the Relevant Period, SCA's ECDD Programs provided that the ECDD Program must be applied when one or more of the circumstances specified in paragraph 15.9 of the AML/CTF Rules arose.

331 Throughout the Relevant Period, SCA had certain risk-based systems, controls and procedures referred to in paragraphs 332 to 335 to identify when one or more of the circumstances in paragraph 15.9 of the AML/CTF Rules arose. However, for the reasons set out at paragraphs 343b and 343c, those risk-based systems, controls and procedures were not sufficient for SCA to ensure that where one or more of the circumstances in sub-paragraphs 15.9(1) to (3) of the AML/CTF Rules arose, customers were escalated for ECDD as and when appropriate.

332 To identify whether the "ML/TF risk [was] high" (paragraph 15.9(1)), which may have meant that the customer was to be referred for ECDD, SCA's processes involved:

a. general guidance, a table (in which all customers were low risk by default) of risk elevation triggers, and from September 2019, a SOP, all of which described the circumstances in which a customer was to be rated 'moderate', 'high', or 'significant' risk. For example, customers categorised as international organisation PEPs and foreign PEPs were automatically accorded a 'significant' risk rating;

b. section 3 of SCA's 2017-2021 Standard Part A Programs stated that SCA's "[c]ustomer screening, transaction monitoring and front line reporting processes all played a role in determining whether particular customers should be assigned an elevated risk rating"; and

c. section 19 of SCA's 2018-2021 Standard Part B Programs stated that SCA was to rescreen all customers rated 'moderate or above', against a global PEP database, the Dow Jones database each year.

[29] The 'ECDD Template Standard Operating Procedure' 4 October 2019; the 'High & Significant Risk Elevations Standard Operating Procedure' dated 16 September 2019; the 'High Risk Jurisdiction Standard Operating Procedure' dated 17 September 2019; the 'PEP Screening Standard Operating Procedure' dated 17 September 2019; and the 'SMR Reporting Standard Operating Procedure' dated 1 October 2019.

333 SCA's TMPs had regard to customer risk ratings (however, see Section F.6.8 as to the adequacy of SCA's TMP). For example, subsection 10 of section 13 of the 2017-2021 Standard Part A Programs required the generation and monitoring of reports of customer transaction activity each month as a means of identifying "*materially abnormal transaction values or activity which might suggest an escalated risk of ML/TF activity requiring further investigation*".[30]

334 To identify whether a designated service was being provided to a customer who was, or who had a beneficial owner who was, a foreign PEP (paragraph 15.9(2)), the 2017-2021 Standard Part B Programs provided that customers who satisfied certain criteria were to be screened against the Dow Jones database available via the Jade System.

335 The Standard Part A Programs contained processes to seek to identify whether a suspicion had arisen for the purposes of section 41 of the AML/CTF Act (paragraph 15.9(3)). Those processes are set out further in Sections F.6.3 to F.6.7, F.7.2 to F.7.2.2, F.8.2 to F.8.3 and F.9.2.

336 The deficiencies with the processes described above at paragraphs 332 to 335 in the Standard Part A Programs are set out below at paragraph 343b.

F.7.2.2 SCA's ECDD Programs and paragraphs 15.10 and 15.11 of the AML/CTF Rules

337 Under the Standard Part A Programs, the AMLCO (or their assigned delegate) was responsible for applying the ECDD Programs in the circumstances described at paragraphs 330 to 332 and for determining the range of measures to be applied in response to those circumstances. In addition, other roles were responsible for the implementation of the ECDD Programs, including:

a. the AML Analyst;

b. until July 2017, the Compliance Manager;

c. from 5 April 2021 to 19 July 2021, the AML Compliance Manager; and

d. from 19 July 2021 onwards, the Cash Handling Shift Manager and the Senior Casino Manager (a role within the Table Games department).

338 While the above roles were responsible for the implementation of SCA's ECDD Program, those roles required greater resourcing for the consistent conduct of ECDD - having regard to the nature, size and complexity of SCA's business and the ML/TF risk it reasonably faced. SCA's investment in increased resourcing is discussed at paragraphs 514 to 517 below.

339 During the Relevant Period, SCA's ECDD Programs set out the ECDD measures that SCA staff were required to undertake, as well as some additional ECDD measures that could be undertaken if the AMLCO (or their assigned delegate) determined any of those measures were appropriate to apply or where one or more of the circumstances in paragraph 15.9 of the AML/CTF Rules arose. However, the ECDD Programs did not include or incorporate adequate procedures or guidance on the suite of risk-based ECDD measures to be applied by the AMLCO (or their assigned delegate).

340 SCA's ECDD Programs did not provide specific written guidance to ensure that source of wealth and source of funds information was obtained, analysed and recorded for the purposes of carrying out ECDD. In the period since 23 December 2019, SCA has updated various processes relevant to obtaining source of funds or source of wealth information (see paragraph 230 above). However, this was not for the sole purpose of carrying out ECDD and

[30] Subsection 12 of the 2015 Standard Part A Program adopted a slightly different language and stated the reports would be "monitored…".

there were deficiencies associated with these processes as outlined at paragraphs 343i and 343j.

341 Whilst SCA's Standard Part A Programs provided for the General Manager of Adelaide to make decisions about whether to continue a business relationship with a 'significant' risk customer, foreign PEPs, international organisation PEPs or domestic PEPs who had been accorded a high or significant risk rating, the Standard Part A Programs did not expressly set out an ML/TF risk appetite for customers and so there was no specific criteria against which senior management could appropriately determine whether to approve continuing the business relationship with a customer, the provision of a designated service to a customer, or a transaction or particular transaction.

342 During the Relevant Period, SCA recorded information obtained as a result of undertaking ECDD in its iTrak system and within its relevant shared information drives.

F.7.2.3 Non-compliance with the AML/CTF Act and AML/CTF Rules

343 Between 7 December 2016 and 17 November 2022, SCA:

a. did not appropriately identify, manage and mitigate the ML/TF risk it reasonably faced in providing designated services to its customers due to deficiencies with its ECDD Programs;

b. SCA's Standard Part A Programs did not include appropriate risk-based systems, controls or procedures (i) to identify customers who were required under the Standard Part A Programs to be categorised as high or significant risk, or who presented high risks, and to escalate them for ECDD as and when appropriate; (ii) to identify customers who were foreign PEPs; and (iii) until September 2019, to appropriately escalate customers for ECDD when a section 41 suspicion arose. This was because:

   i. the processes for identifying and escalating customers who were not low risk (but were assessed as such, by default) were inadequate;

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

   iii. prior to September 2019, there was no written procedure to ensure that the ECDD Programs were applied automatically when a suspicion arose for the purposes of section 41 of the AML/CTF Act;

   iv. the screening procedures to identify and escalate PEPs and to identify whether a customer was on a terrorism or sanctions list or was otherwise subject to adverse media were inadequate;

   v. the transaction monitoring programs were not capable of consistently identifying and escalating customers engaging in unusual or suspicious transactions or otherwise identifying customers who should be categorised as high or significant risk (as stated at paragraph 333 above);

   vi. there was no appropriate process to consistently identify and escalate customers from high risk jurisdictions; and

   vii. 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.

c. SCA's ECDD Programs identified some ECDD measures that could be undertaken when ECDD was triggered, but did not include appropriate systems, controls and procedures to ensure that the appropriate ECDD measures were undertaken when an ECDD trigger arose;

d. SCA's ECDD Programs did not set out ECDD measures that were adequately aligned to the nature, size and complexity of SCA's business, and the ML/TF risk posed by the customers;

e. SCA's ECDD Programs did not contain written processes or guidance as to which ECDD steps or measures were to apply in response to the specific risks posed by a customer;

f. the ECDD Programs did not include appropriate procedures to ensure analysis of the full suite of designated services received by customers across multiple transaction chains and channels, including designated services provided under table 1, section 6 of the AML/CTF Act;

g. the ECDD Programs did not include appropriate procedures to ensure analysis of third party transactions;

h. SCA's application of the ECDD process was unstructured and not replicated to the same standard in each and every instance and in a consistent manner. It was ad hoc and discretionary, with no process or procedure setting out the relevant measures to be undertaken when completing ECDD based on the level of ML/TF risk faced. A report commissioned by SCA dated September 2021 identified that carrying out appropriate extensive ECDD would be challenging given resourcing and capacity constraints;

i. SCA's ECDD Programs did not provide written guidance to ensure that source of wealth and source of funds information were obtained, analysed and recorded for the purposes of carrying out ECDD. For example:

    i. SCA's ECDD Programs required the AMLCO (or their assigned delegate) to take reasonable measures to identify the sources of wealth and funds for PEPs who were rated at least high risk, but the reasonable measures were at the discretion of the AMLCO (or their assigned delegate) and were not subject to specific written guidance;

    ii. SCA's Standard Part A Programs required source of wealth and source of funds information to be obtained in limited circumstances and not necessarily for the purpose of carrying out ECDD. From December 2019, some updates were made in relation to the circumstances in which this information was to be obtained, which are referred to at paragraphs 230b to 230d above;

    iii. SCA's Standard Part A Programs did not have appropriate processes or controls to consistently carry out appropriate risk-based ECDD measures where source of funds or source of wealth checks were required, for the purposes of ECDD. This included 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 purpose of ECDD. For example, SCA was not able to consistently identify customers whose transactions or gaming activity did not align with their stated occupation, or identify circumstances where a customer's source of wealth was unexplained or possibly illegitimate. This gave rise to some instances where SCA was not able to appropriately understand the ML/TF risk posed by a customer's transaction and determine whether that specific transaction(s) should be processed or if an ongoing relationship with the customer should continue;

iv. with respect to the SOPs that related to the requirements introduced in December 2020 and July 2021 for transactions over $100,000, they each stated that in all circumstances the customer must undergo ECDD by: (a) completing the Source of Funds Declaration Form; and (b) providing independent documentation to verify the information provided in the Source of Funds Declaration Form. However, each SOP was focused on whether the transaction should be approved or refused based on the information provided; and

v. there was no appropriate written review criteria to assess the information provided on the Source of Funds Declaration Forms.

j. SCA did not have in place documented systems or processes 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 the Bally CMP System or any other information system accessible by SCA employees responsible for ECDD;

k. the Standard Part A Programs did not set out the criteria against which senior management could appropriately determine whether to approve continuing a business relationship with a customer, or whether the provision of designated services was outside SCA's ML/TF risk appetite; and

l. the ECDD Programs were not supported by appropriate information management and record keeping.[31] In particular:

i. by reason of the deficiencies in information and record keeping, SCA did not always have a full view of customers' transactions for ECDD purposes;

ii. SCA did not in all instances 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:

A. 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 was unable to readily access, monitor and/or review basic information in relation to the extent of ECDD conducted up to May 2018;

B. in or around May 2018, SCA introduced an ECDD template SOP form to centralise ECDD information located in multiple systems, but there was no documented guidance in place about how the ECDD template SOP should be used;

C. 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 the customer's source of funds or source of wealth; and

D. SCA did not have in place documented procedures to ensure that adverse information held by SCEG staff in relation to SCA customers was escalated to SCA or recorded as part of the SCA customer's risk profile; and

E. the nature of SCA's record keeping meant that it did not readily 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.

[31] See paragraphs 20-21 for an explanation of appropriate risk-based procedures, systems and controls.

344 In the circumstances of the matters set out at paragraph 343, SCA's ECDD Programs did not fully comply with paragraphs 15.9 to 15.11 of the AML/CTF Rules at all times during the Relevant Period. As a result of these deficiencies, SCA contravened section 84(2)(c) of the AML/CTF Act.

345 The steps SCA has taken to uplift and enhance its AML/CTF function and compliance with respect to its ECDD program are set out at paragraph 506 below.

F.8 AML/CTF reporting obligations

F.8.1 SCA's AML/CTF reporting obligations

346 At all times during the Relevant Period:

a. pursuant to section 41 of the AML/CTF Act, SCA was required to submit SMRs to AUSTRAC;

b. pursuant to section 43 of the AML/CTF Act, SCA was required to submit TTRs to AUSTRAC;

c. pursuant to section 45 of the AML/CTF Act, SCA was required to submit IFTI reports to AUSTRAC; and

d. pursuant to paragraph 8.9.1 of the AML/CTF Rules, SCA's Standard Part A Programs were required to include:

i. the obligations that applied to SCA under sections 41, 43 and 45 of the AML/CTF Act; and

ii. appropriate systems and controls of SCA designed to ensure compliance with its AML/CTF reporting obligations.

(collectively, **AML/CTF Reporting Obligations**).

F.8.2 Documentation of SCA's systems and controls in respect of AML/CTF Reporting Obligations

347 SCA's systems and controls with respect to its AML/CTF Reporting Obligations were set out in:

a. section 9 of the 2015 Standard Part A Program;

b. section 11 of the 2017-2021 Standard Part A Programs; and

c. section 11 of the 2022 Standard Part A Program.

348 The systems and controls relating to SCA's AML/CTF Reporting Obligations under the Standard Part A Programs were supplemented and supported by certain documents and procedures, which contained internal guidance publications outlining AML/CTF processes and procedures.[32] For example, documents relevant to the roles of AML Analyst and AML Adviser set out, amongst other things, their responsibilities relating to the AML/CTF Reporting Obligations.

[32] AML Analyst Role document dated 6 November 2017; AML Advisor Role document dated 12 May 2020; 'AML Checking Process' document 26 March 2015; IFTI Help Guide dated 18 July 2013; IFTI Advice document dated 16 September 2016; SMR Reporting Standard Operating Procedure dated 1 October 2019.

F.8.3 SCA's systems and controls in respect of compliance with paragraph 8.9.1

349 At all times during the Relevant Period, SCA had in place certain systems and controls in relation to its compliance with its AML/CTF Reporting Obligations. These are summarised below at paragraphs 350 to 361.

SMRs

350 From June 2016, SCA's frontline casino staff were required to submit observation reports to SCA's AML team. SCA's 2017-2021 Standard Part A Programs required staff to submit observation reports when triggered by indicators of illicit activities. For example, the use of third parties for cash/chip exchanges or multiple chip cash-outs on the same day.

351 As part of SCA's AML/CTF risk awareness training program, required under the AML/CTF Act and the AML/CTF Rules, certain training and guidance was provided to SCA staff explaining how to identify potentially suspicious activities and behaviour. Staff were also able to access intranet resources, which included FAQs on suspicious matters. Up until 2020, an 'AML newsletter' was also distributed to employees on a regular basis, which included recent examples of suspicious behaviour detected at the SCA casino to educate SCA casino staff on recent real-life examples of suspicious behaviour.

352 The AMLCO delegated the day-to-day investigation of suspicious matters to the AML Analyst / AML Advisor / AML Compliance Manager (as applicable at the relevant time). The AML team was to review observation reports made by SCA staff to determine whether further analysis and/or investigation was warranted, and whether an SMR should be submitted to AUSTRAC. The AML team was also to investigate transactions or behaviour that they identified and considered potentially suspicious or unusual.

353 From February 2017, the AMLCO had oversight of the implementation of SCA's SMR obligations, which included providing support and guidance on the SMR process from time to time (for example, advising whether or not an SMR should be filed in a particular instance or whether any additional information should be included in an SMR). The AMLCO was also responsible for ensuring that all SMRs were reported to the AUSTRAC CEO (electronically) in the approved form, containing all requisite information, within three business days of the suspicion being formed. All information relating to a potentially suspicious matter was to be recorded on the customer's profile in the iTrak system, and records of customers' gaming patterns and history were to be retained within the Jade System.

TTRs

354 At all relevant times throughout the Relevant Period, threshold transactions were captured by the Bally Cage System (for transactions performed at cashiers) and Bally CMP System (for transactions performed at gaming tables). These transactions would then be extracted from those systems via the Microsoft BizTalk Server. The Microsoft BizTalk Server allowed the transactional data to be communicated to the Jade System, creating an Excel spreadsheet modelled on the spreadsheet reporting template in the AUSTRAC online environment.

355 The information extracted from the Bally Cage and Bally CMP System was to be presented as an Excel spreadsheet report to be reviewed by the Cage Manager, to confirm that the transactions identified in the report should be submitted to AUSTRAC as a threshold transaction. From February 2017, the spreadsheet was to then be provided to the AMLCO (or their delegate) as a complete list of threshold transactions for submission to AUSTRAC within 10 business days. Since all transactions in the Bally Cage System were automatically processed as cash transactions (unless the relevant Cage staff member manually selected the transaction to be processed in a different type of tender set), the Cage Manager would also review the spreadsheets to ensure that non-qualifying transactions (i.e., non-cash transactions) were removed.

356 From February 2017, the AMLCO had oversight of the implementation of SCA's TTR obligations and delegated the day-to-day review of threshold transactions to the AML Analyst / AML Advisor / AML Compliance Manager (as applicable at the relevant time). Prior to February 2017, all TTR transactions were required to be reviewed by the Compliance Manager or delegate prior to submission.

IFTIs

357 All incoming transfers from the SCEG Customer account channel, SCA Customer account channel or via an inter-company transfer were recorded in the Bally Cage System and credited to or debited from the relevant customer's FMA. A daily review of these transactions was undertaken by the Cash Handling Shift Manager (or Acting Cash Handling Shift Manager) to determine which of the transactions were received from or being sent to an overseas destination for the purpose of, amongst other things, identifying each transaction that required reporting to AUSTRAC as an IFTI.

358 The Cash Handling Shift Manager (or Acting Cash Handling Shift Manager) was responsible for preparing an IFTI report and submitting the report to AUSTRAC online and had received training on reviewing IFTIs, which was documented. From 2017, common scenarios that triggered an IFTI reporting obligation were set out in the Standard Part A Programs. Typically reports were submitted at the end of the day in which the relevant transaction occurred. Copies of submitted IFTI reports were to be forwarded to the AML Analyst or AML Compliance Manager for checking.

359 Records of IFTI reports were manually entered in the iBase system until January 2021 and could be searched using the customer's name. From January 2021, IFTI reports were recorded and managed in the Jade System with the AML team being responsible for oversight of every report submitted to AUSTRAC.

360 From February 2017, the Cage Manager was responsible for ensuring that all IFTIs were reported to the AUSTRAC CEO (electronically) in the approved form within 10 business days of the instructions being provided to facilitate the transaction. Prior to February 2017, the Cash Handling Manager was responsible. The International Business Player Accounts Manager (SCEG) was responsible for promptly providing the Cage Manager with any relevant information to allow SCA to complete an IFTI where appropriate.

SMRs, TTRs and IFTIs

361 At each scheduled meeting of the SCA AML/CTF Senior Management Group during the Relevant Period, the AMLCO was required to report on SMRs, TTRs and IFTIs. For example, with respect to SMRs, the report contained the number of SMRs lodged with AUSTRAC since the last AML/CTF Senior Management Group meeting, provided a summary of the subject matter of the SMRs and, from May 2017, the number of observation reports received from frontline employees and how many resulted in the lodgement of an SMR. Also from May 2017, confirmation that SMRs, TTRs and IFTIs were lodged within the statutory timeframe was included.

F.8.4 Non-compliance with the AML/CTF Act and AML/CTF Rules

362 From 7 December 2016 to 17 November 2022, the Standard Part A Programs did not fully comply with the requirements of sub-paragraph 8.9.1(2) of the AML/CTF Rules and section 84(2)(c) of the AML/CTF Act with respect to SCA's reporting obligations pursuant to sections 41, 43 and 45 of the AML/CTF Act. As a result of the deficiencies identified below at paragraphs 363 to 366 with respect to SCA's systems and controls relating to compliance with its AML/CTF Reporting Obligations, between 7 December 2016 and 17 November 2022, SCA contravened section 84(2)(c) of the AML/CTF Act.

363 The Standard Part A Programs did not include adequate assurance processes regarding SCA's AML/CTF Reporting Obligations.

SMRs

364 With respect to SCA's SMR reporting obligations under section 41 of the AML/CTF Act:

a. notwithstanding the systems and controls and the guidance and training that were in place with respect to identifying suspicious conduct and preparing SMRs (as described at paragraph 351 above), SCA did not provide the AMLCO or the AML Analyst / AML Advisor / AML Compliance Manager (as applicable at the relevant time) with specific guidance or training in relation to SMR reporting obligations;

b. SCA's escalation processes with respect to unusual or suspicious matters were inappropriate as they were based on an overreliance on manual processes which could be affected by inconsistent identification and human error (see paragraphs 352 to 353 above with respect to those processes). For example, in a review dated August 2022 SCA received feedback that some staff were unsure of common casino typology indicators that should result in the submission of an observation report;

c. deficiencies in SCA's TMP (as described in paragraphs 318 to 321) meant that SCA was unable to consistently monitor its customers to identify suspicious or unusual activity within the meaning of section 41 of the AML/CTF Act;

d. SCA did not have adequate policies or procedures in place to consistently identify and report suspicious matters relating to designated services provided by SCA through the SCEG Customer account channel; and

e. SCA's provision of designated services via EZYPlay Guest Cards, which were issued anonymously, including in circumstances where multiple cards could be issued to a single customer, impacted SCA's ability to include accurate customer information in SMRs.

TTRs

365 With respect to SCA's TTR obligations under section 43 of the AML/CTF Act:

a. where a junket representative or junket player was conducting a threshold transaction on a junket operator's FMA, the TTR was reported against the junket operator's name, not the name of the junket representative or junket player. This made it difficult for AUSTRAC and its law enforcement partners to fully understand the role of different parties to the transaction, including what transactions took place, the source of the funds, who instructed the movement of the funds, the recipient of the funds and further details of the transaction; and

b. the TTR process relied on data sourced from the Bally CMP System (as summarised above at paragraphs 354 to 355). From 1 July 2015 to 9 August 2021, the Bally CMP System recorded all transactions as cash transactions. As such, significant manual review was required to be undertaken by SCA staff to identify the relevant threshold transactions for reporting to AUSTRAC, which could be prone to inconsistent identification and human error. In addition, not all transaction types were exported from the Bally CMP System to the Jade System for threshold transaction reporting.

IFTIs

366 With respect to SCA's IFTI reporting obligations under section 45 of the AML/CTF Act:

a. the process to identify IFTIs for reporting was labour-intensive and based on a manual review of data (as summarised above at paragraphs 357 to 359 above);

b. there was no documented process in place for SCA to obtain IFTI information from SCEG personnel in circumstances where SCA customers had transferred funds through the SCEG Customer accounts, despite the International Business Players Accounts Manager (SCEG) being responsible for this process (see paragraph 360 above). The absence of a documented process impacted SCA's ability to ensure consistent reporting of IFTIs to AUSTRAC;

c. until 26 October 2020, the practice of occasionally aggregating customer deposits into SCA Customer accounts and SCEG Customer accounts meant that SCA may, in certain instances, have incorrectly reported IFTIs to AUSTRAC; and

d. during the Relevant Period, SCA adopted a 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. As a result, these IFTIs were reported to AUSTRAC by SCA as transfers to New Zealand, which obscured the final destination of the funds. This practice made it difficult for AUSTRAC to fully 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.

367 The steps SCA has taken to uplift and enhance its AML/CTF function and compliance with respect to its reporting obligations are set out at paragraphs 507 to 512 below.

F.9 Applicable Customer Identification Procedures (ACIPs)

F.9.1 SCA's obligations in relation to ACIPs

368 At all times during the Relevant Period, SCA was required to have a Standard Part B Program which complied with the requirements set out at paragraphs 81 to 82 above.

F.9.2 SCA's Standard Part B Programs and ACIP

369 At all times during the Relevant Period, SCA included a Standard Part B Program in its AML/CTF Programs (the Standard Part B Programs, as defined at paragraph 85b above).

370 Notwithstanding the steps and procedures set out at paragraphs 371 to 389, between 7 December 2016 and 17 November 2022, SCA's Standard Part B Programs did not sufficiently comply with the requirements of paragraphs 4.1.3, 4.2.5, 4.2.8, 4.13.1 and 4.13.3 of the AML/CTF Rules for the reasons described in paragraphs 390 to 394. As a result of the deficiencies identified below in its Standard Part B Programs, between 7 December 2016 and 17 November 2022, SCA's Part B Programs did not comply with sections 81 and 84(3)(b) of the AML/CTF Act.

371 From 7 December 2016, SCA's Part B Program was set out in sections 20 to 25 of the 2015 Standard Part B Program and sections 16 to 20 of the 2017-2021 Standard Part B Program:

a. sections 20 to 23 of the 2015 Standard Part B Program and subsections 11 to 14 and 18 to 22 of section 16 of the 2017-2021 Standard Part B Programs set out the circumstances in which the minimum KYC information, such as the customer's full name and either their date of birth or residential address should be collected from the customer and verified, and that any information should be recorded (with the Bally CMP System specified in the 2017-2021 Standard Part B Programs);

b. subsections 15 to 17 and 23 of section 16 of the 2017-2021 Standard Part B Programs set out the circumstances in which additional KYC information about the

customer should be requested from the customer, and stated that any additional information collected from the customer should be recorded in the Bally CMP System;

c. subsection 24 of section 16 of the 2017-2021 Standard Part B Programs set out the process to be undertaken where a discrepancy in a customer's information was identified, including that discrepancies were to be referred to the AMLCO and that the customer was to be subject to further enquiries;

d. subsection 25 of section 16 of the 2017-2021 Standard Part B Programs required that documentation for verification purposes be current at the time of receipt from the customer, and to the extent that the same documentation was to be relied upon to verify a customer's KYC information in respect of subsequent transactions, it should also be current at the time those subsequent transactions were undertaken;

e. subsections 4 to 6 of section 17 of the 2017-2021 Standard Part B Programs set out the circumstances in which KYC information was to be collected where an agent purported to act on a customer's behalf, including where there was an authority for the agent to act on that customer's behalf;

f. subsections 6 to 9 of section 18 of the 2017-2021 Standard Part B Programs set out the circumstances in which KYC information would be collected for transactions involving a beneficial owner;

g. subsections 6 and 7 of section 19 of the 2017-2021 Standard Part B Programs set out the circumstances in which customers would be screened for PEP status;

h. subsections 8 to 10 of section 19 of the 2017-2021 Standard Part B Programs set out how customers should be categorised if PEP screening returned a positive result;

i. subsection 11 of section 19 of the 2017-2021 Standard Part B Programs set out the circumstances in which certain PEPs were to be the subject of source of wealth and source of funds enquiries; and

j. subsections 12 to 14 of section 19 of the 2017- 2021 Standard Part B Programs set out the circumstances and process by which SCA was to consider whether to continue the provision of designated services to a customer who had been identified as a PEP.

372 The Standard Part A Programs also included sections that supported the Standard Part B Programs (although they were not referred to in the Standard Part B Programs and did not exclusively apply to the Standard Part B Programs).[33] The Standard Part B Programs were also supported by a number of SOPs and forms (although these procedures were not referred to in the Standard Part B or Standard Part A Programs).[34]

[33] Subsections 6 to 30 of section 3 of the 2017-February 2021 Standard Part A Programs, and subsections 6 to 29 of section 3 of the June-October 2021 Standard Part A Programs, which considered the ML/TF risk posed by the nature, size and complexity of the business and type of ML/TF risk, customer types, types of designated services, designated service delivery, and dealing with foreign jurisdictions; section 14 of the 2015 Standard Part A Program and subsections 3 to 5 of section 12 of the 2017-2021 Standard Part A Programs, which provide for the review and update of documentation used to verify minimum KYC requirements and occupation details for OCDD purposes, and refers to the collection of additional KYC information; section 17 of the 2015 Standard Part A Program and subsections 5 to 14 of section 14 of the February-October 2021 Standard Part A Programs, which set out the circumstances where ECDD would be applied, and information collected.

[34] 'Acceptable Identification' SOP (from around October 2018); Acceptable Non-Photographic ID' SOP (from around June 2019); 'Onboarding New Junket Operator' SOP (from around August 2019); the 'PEP Screening' SOP dated 17 September 2019; the 'Accepting Digital Identification' SOP (from around August 2020); International Business – Significant Cash Transactions and Source of Funds' SOP (from around August 2020); General Source of Wealth Inquiries' SOP (from July 2021); the 'Unusually Large Electronic Transfers ($300k domestic/$1m international)' SOP (from July 2021); the Patron Credentials Disclosure Form (from November 2021); a Source of Funds Declaration Form (from December 2019); and Source of Wealth Declaration Form (from July 2021).

ACIP procedures

373 At all times during the Relevant Period, SCA's Standard Part B Programs included ACIP procedures that included the:

a. collection and verification of minimum KYC information;

b. collection of additional KYC information;

c. collection and verification of KYC information for agents of customers;

d. collection and verification of KYC information for PEPs; and

e. procedures for dealing with PEP screening.

Collection and verification of minimum KYC information

374 During the Relevant Period, sections 20 and 21 of the 2015 Standard Part B Program, and subsections 11 and 12 of section 16 of the 2017-2021 Standard Part B Programs, identified the circumstances in which SCA was to collect and verify minimum KYC customer information. Specifically, subsection 11 of section 16 of the 2017-2021 Standard Part B Programs provided that KYC information was to be collected from customers in the following situations:

i. purchase or redemption of gaming chips ≥$10,000;

ii. redemption of a jackpot or cancelled credits ≥$10,000;

iii. exchange of foreign currency ≥$1,000;

iv. establishment of an FMA; and

v. all transactions in relation to an FMA.

375 Subsection 13 of section 16 of the 2017-2021 Standard Part B Programs provided that SCA staff were to collect minimum KYC information from a customer before the provision of a designated service. To verify the minimum KYC information collected, the customer was required to supply a suitable form of photo identification prior to the designated service being provided to the customer for the first time.

376 All KYC information collected from customers (including for junkets) was to be recorded in the Bally CMP System.

Collection of additional KYC

377 Any additional customer information provided (including additional verification documents) was to be recorded in the Bally CMP System. For example, a customer may be asked to provide details about their occupation. However, it was not mandatory for the customer to provide their occupation details, and if provided, the information was not verified, unless the customer was subject to SCA's ECDD process or was a PEP. Designated services could, in certain instances, still be provided to the customer in the absence of that information.

378 As described at paragraph 340 above, prior to 23 December 2019, SCA collected source of funds information from customers on an ad hoc basis. On 23 December 2019, SCA first introduced a requirement to obtain source of wealth and source of funds information from its customers by way of a Source of Funds Declaration Form. However, the requirement extended only to International Business customers presenting more than $100,000 in cash. No supporting documentation was required. This process was extended in July 2021 to all

domestic SCA customers who made an inward EFT of $300,000 or more and for international customers who made an inward EFT of $1 million or more. These customers were required to provide supporting evidence for their stated source of wealth. Refusal to complete the Source of Funds Declaration Form required that the funds be returned and the AML team be advised as soon as possible.

379 In July 2021, SCA also requested all of its Black tier loyalty program members (SCA's highest loyalty program tier), regardless of the ML/TF risk they posed, to complete a Source of Wealth Declaration Form and provide supporting documentation.

380 As described at paragraph 275 above, junket operators were required to complete a GFDF when presenting cash to buy-in on behalf of a junket.

Collection and verification of KYC for agents of a customer

381 SCA's customers typically made transactions on their own behalf. However, where an agent purported to act on behalf of a customer, SCA's Standard Part B Programs required that SCA:

a. collect and verify the minimum KYC information of the agent, as described at paragraphs 82c and 374 above;

b. record this information in the Bally CMP System under the name of the agent;

c. confirm with the customer that the agent was authorised to act on the customer's behalf; and

d. record the relationship between the customer and the agent in the Bally CMP System.

382 As described at paragraphs 164 to 165 above, from 14 February 2017, junket operators could provide written authorisation via a Funds Authorisation Form to allow a junket representative to act on their behalf.

Identification of PEPs

383 During the Relevant Period, SCA's Standard Part B Programs required its customers (including those on junkets) to be screened for PEP status where the customer transacted at or over $10,000 in the purchase or redemption of chips, jackpot / cancelled credits or exchanged foreign currency greater than $1,000. Further, from February 2017 to the remainder of the Relevant Period, mandatory PEP screening was also undertaken for all individual customers who:

a. established an FMA through membership in the casino's loyalty program;

b. visited in their capacity as a junket organiser or junket representative;

c. participated on a junket program as a player; or

d. had been accorded a high or significant risk by SCA.

384 In relation to the regularity of the screening, customers were to be PEP screened using the Dow Jones database via the Jade system (where data or information collected under ACIP would be updated and reviewed), on the following schedule:[35]

[35] Subsection 7 of section 19 of the 2018-2021 Standard Part B Programs. Subsection 7 of section 19 of the 2017 Standard Part B Program had slightly different language and stated that "[o]nce a customer has undertaken a Designated Service … and has been assessed for PEP status, they will be automatically rescreened each year'. Section 15 of the 2015 Standard

a. under the 2015 Standard Part A and Part B Programs, customers who returned a negative screening result, were still active customers and were rated moderate risk required re-screening at least every two years and customers who were rated high risk were to be re-screened annually; and

b. under the 2017-2019 Standard Part B Programs, until June 2017, customers who had been screened were to be re-screened annually. From June 2017, customers rated moderate risk or higher were to be re-screened annually.

ACIP procedure for PEPs

385 The 2017-2021 Standard Part B Programs required that enquiries be made of all domestic PEPs who were classified as high or significant risk, international organisation PEPs and foreign PEPs to determine their source of wealth and source of funds. Where public records were unhelpful in identifying this information, the PEP was to be invited to complete a Source of Funds Declaration Form.

386 Once source of wealth and/or source of funds enquiries had been completed, the matter was to be referred by the AMLCO to the General Manager to determine whether or not the provision of designated services should be established, or continued, with respect to the relevant customer.

Discrepancy with information

387 Where a discrepancy in information arose in the process of collecting KYC information it would be recorded in the Bally CMP System. Unless the discrepancy could be explained by an obvious typographical error or an official change of name, the discrepancy was required to be referred to the AMLCO to consider whether there were any indicators of suspicious behaviour that might warrant an SMR.

388 If a suspicion arose in relation to the authenticity of the identification provided, the matter was to be reported to the AMLCO for further enquiry. In such cases, the transaction was not to be completed until the AMLCO had authenticated the documentation.

Customer risk ratings

389 As described at paragraph 100 above, customer risk ratings were set by default as 'low'. A customer's risk rating could be elevated from the default risk rating having regard to a number of factors, including customer type and betting behaviours. Any additional KYC information collected during ECDD processes was to be added to a customer's profile in the Bally CMP System and reflected in their risk rating.

F.9.3 Non-compliance of SCA's Part B AML/CTF Programs

390 In designing its Standard Part B Programs, SCA did not adequately consider the risks in paragraph 4.1.3 of the AML/CTF Rules, including in relation to its customers' source of wealth and source of funds information (paragraph 4.1.3(2)), the nature and purpose of the business relationship with its customers, namely junket customers (paragraph 4.1.3(3)) or all of the designated services it provided to its customers (paragraph 4.1.3(5)). As such, SCA did not have proper regard to all of the factors in paragraph 4.1.3 of the AML/CTF Rules, and, in doing so, SCA's Standard Part B Programs were not sufficiently aligned to the ML/TF risk posed by its customers. Specifically, between 7 December 2016 and 17 November 2022, SCA's Standard Part B Programs:

Part A Program stated that '[a]ll customers who have undergone a negative PEP check and who are still active customers rated as a moderate risk shall be rescreened at least once every two years and those who are rated high risk or above, shall be rescreened annually to determine whether their PEP status has changed".

a. did not include adequate systems and controls to identify customers who were high risk at the time ACIP was being carried out;

b. did not contain clear processes and procedures to ensure that at the time that ACIP was carried out a customer's risk rating was elevated from the default rating of low risk in accordance with the Risk Allocation Criteria set out in SCA's Standard Part A Programs;

c. did not contain adequate systems and controls to collect and analyse information with respect to source of wealth or source of funds;

d. did not include adequate risk-based systems and controls to consider the nature and purpose of the business relationship with customers who were junket operators, junket representatives and junket players;

e. did not include adequate risk-based systems and controls to consider the risks posed by designated services under items 6, 7, 31 and 32, table 1, section 6 of the AML/CTF Act and item 13, table 3, section 6 of the AML/CTF Act; and

f. there was no specific procedure for, or specific reference in the Standard Part B Programs to, the ML/TF risk posed by the foreign jurisdictions with which SCA dealt.

391 Contrary to the requirements of paragraphs 4.2.5 and 4.2.8 of the AML/CTF Rules, the Standard Part B Programs did not include appropriate risk-based systems and controls for determining whether, in addition to the minimum KYC information to be collected and verified about a customer, any other KYC information was to be collected and verified about a customer. For example:

a. 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;

b. while there were some limited procedures for the collection and verification of additional KYC information, these procedures were not triggered at the time ACIP was conducted, except from 2017 when foreign or international organisation PEPs had been identified;

c. while SCA's Standard Part B Programs included procedures to request occupation details, there was no requirement for customers to provide this information and, if provided, it did not need to be supported by documentation; and

d. from 2017, SCA's Standard Part B Programs provided that source of wealth and source of funds information enquiries should be made for certain categories of PEPs. However, under the Standard Part B Programs there was no obligation for the customer to supply this information or to provide documentary evidence to support any information provided. The failure to obtain adequate source of wealth or source of funds information at the time of ACIP, on a risk-basis, meant that designated services could have been provided to customers in circumstances where SCA may not have reasonably assessed the ML/TF risk of this.

392 SCA's Standard Part B Programs set out the circumstances where a customer was required to be identified, but they did not align with all of the circumstances in which a customer was required to be identified in accordance with the AML/CTF Act and the AML/CTF Rules. For example:

a. the Standard Part B Programs did not require the collection and verification of customer information in circumstances where a customer exchanged foreign currency by way of foreign drafts below AUD$1,000, noting that the exemption in paragraph 14.4 of the AML/CTF Rules applied to physical currency and travellers' cheques only; and

b. there were no appropriate risk-based procedures in the Standard Part B Programs to apply ACIP to prospective customers who were receiving items 6, 7, 31 or 32, table 1, section 6 of the AML/CTF Act designated services. For example, 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.

393 In relation to the identification of PEPs:

a. the Standard Part B Programs did not include appropriate risk management systems to comply with the requirement in paragraph 4.13.1 of the AML/CTF Rules. While SCA's Standard Part B Programs provided that PEPs could be identified through screening:

i. for the reasons identified in paragraph 384, the screening processes were inadequate due to the insufficient regularity of the screenings;

ii. from 2017, the screening was not triggered by non-cash transactions including through the SCA and SCEG Customer account channels; and

iii. customers playing uncarded could not be consistently screened; and

b. the Standard Part B Programs did not include adequate risk management systems to ensure that the steps in paragraph 4.13.3 of the AML/CTF Rules were adequately undertaken in all circumstances. The Standard Part B Programs did not include or incorporate appropriate risk management procedures and guidance regarding PEPs. Specifically, they did not include procedures to obtain senior management approval before establishing or continuing a business relationship with the customer, or to establish the PEP's source of wealth and source of funds or require ECDD to be undertaken.

394 In the circumstances set out at paragraphs 390 to 393, SCA's Standard Part B Programs did not sufficiently comply with paragraphs 4.1.3, 4.2.5, 4.2.8, 4.13.1 and 4.13.3 of the AML/CTF Rules during the Relevant Period. As a result of these deficiencies, SCA contravened sections 81 and 84(2)(c) of the AML/CTF Act.

F.10 SCA's November 2022 Program

395 From July 2021, SCA engaged an external AML consultant (as described above at paragraph 121) to enhance and improve its October 2021 AML/CTF Program. This is set out in further detail in Section H. Following the work SCA undertook with this external consultant, SCA worked to uplift the October 2021 AML/CTF Program and its overarching AML/CTF framework.

396 On 17 November 2022, the SCA Board approved an updated Standard Part A Program. The Standard Part B Program was not amended at that time from the version in force between 28 October 2021 and 17 November 2022, as it was in the process of being amended. On 8 June 2023, the updated Standard Part B Program was approved by the SCA Board. As a result, SCA's current AML/CTF Program is comprised of the Standard Part A Program approved by senior management and the SCA Board on 17 November 2022, and the Standard Part B Program approved by senior management and the SCA Board on 8 June 2023.

397 Part A of the November 2022 Standard Program contains systems and controls that are intended to identify, mitigate and manage the ML/TF risk that SCA may reasonably face with respect to the provision of designated services by SCA. The risk-based systems and controls are set out in various Standards (**Part A Standards**). The Part A Standards are core policy documents which support Part A of the November 2022 Standard Program by prescribing the requirements that SCA employees must follow to implement and operationalise that program and providing additional content about the relevant processes, systems and/or controls that SCA has put in place to comply with its obligations under the AML/CTF Act and AML/CTF Rules.

398 As at 18 November 2022:

a. SCA had conducted an enterprise-wide AML/CTF risk assessment (completed in May 2022) which identified that:

i. its AML/CTF control operational effectiveness was either sub-optimal or not assessed; and

ii. the SCA Board and senior management approval and oversight framework was adequately designed but the framework required enhancement to ensure it was operationally adequate.

b. SCA was developing or intending to develop, but had not yet completed, approved or implemented, the following Part A Standards to align Part A of the November 2022 Standard Program to the 2022 Risk Assessments:

i. ML/TF Risk Assessment Standard;

ii. Customer Risk Rating Standard;

iii. Threshold Transaction Monitoring Standard;

iv. International Funds Transfer Instruction Reporting Standard;

v. Suspicious Matter Reporting Standard;

vi. Transaction Monitoring Standard;

vii. AML/CTF Risk Awareness Training Standard;

viii. Employee Due Diligence Standard; and

ix. ECDD Standard.

(collectively, the **Pending Part A Standards**).

399 As such, as at 18 November 2022, SCA's controls under Part A of the November 2022 Standard Program were not sufficiently aligned to the 2022 Risk Assessments, in circumstances where the Pending Part A Standards had not been completed or approved at the time the SCA Board approved the Standard Part A Program in November 2022.

400 Between 13 and 14 December 2022, SCA approved and implemented the Pending Part A Standards. Once the Pending Part A Standards were approved and implemented, SCA's systems and controls under Part A of the November 2022 Standard Program were aligned to the 2022 Risk Assessments.

F.11 Conclusion

401 By reason of the matters at paragraphs 86 to 400, between 7 December 2016 and 14 December 2022 each of the Standard Part A Programs did not comply in material respects with the requirements of sections 84(2)(a) and 84(2)(c) of the AML/CTF Act or the requirements of paragraphs 8.1.3, 8.1.4, 8.1.5(1), 8.1.5(3), 8.1.5(4), 8.1.5(5), 8.4.1, 8.9.1(2), 15.5, 15.6, 15.7, 15.9, 15.10 and 15.11 of the AML/CTF Rules.

402 By reason of the matters admitted at paragraphs 368 to 394, between 7 December 2016 and 14 December 2022, each of the Standard Part B Programs did not comply in material respects with section 84(3)(b) of the AML/CTF Act and paragraphs 4.1.3, 4.2.5, 4.2.8, 4.13.1 and 4.13.3 of the AML/CTF Rules.

403 By reason of the matters admitted at paragraphs 401 to 402, during the Relevant Period, SCA provided designated services to customers without having adopted or maintained a compliant AML/CTF Program, contrary to section 81 of the AML/CTF Act.

G. SCA'S CONTRAVENTIONS OF SECTION 36 OF THE AML/CTF ACT

G.1 SCA's obligations in relation to section 36 of the AML/CTF Act

404 At all times during the Relevant Period, SCA was required by section 36(1) of the AML/CTF Act to:

a. monitor its customers in relation to the provision of designated services at or through SCA's permanent establishment 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 its permanent establishment in Australia might (whether inadvertently or otherwise) involve or facilitate money laundering; and

b. do so in accordance with the AML/CTF Rules.

405 At all times during the Relevant Period, SCA was required by the AML/CTF Rules to:

a. have regard to the nature, size and complexity of its business and the type of ML/TF risks it might reasonably face, including the risk posed by customer types;

b. include appropriate risk-based systems and controls in its Standard Part A Programs 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 in its Standard Part A Programs a TMP that:

   i. included appropriate risk-based systems and controls to monitor the transactions of its customers;

   ii. had the purpose of identifying, having regard to ML/TF risk, any transaction that appeared to be suspicious within the terms of section 41 of the AML/CTF Act; and

   iii. had regard to complex, unusual large transactions and unusual patterns of transactions, which had no apparent economic or visible lawful purpose;

d. include in its Standard Part A Programs an ECDD Program that complied with the requirements of the AML/CTF Rules;

e. apply the ECDD Program when:

i. SCA determined under its risk-based systems and controls that the ML/TF risk was high;

ii. a designated service was provided to a customer who was, or who had a beneficial owner who was, a foreign PEP; or

iii. a suspicion had arisen for the purposes of section 41 of the AML/CTF Act; and

f. undertake the measures specified in paragraphs 15.10(2) and 15.10(6) of the AML/CTF Rules in the event that a customer was a foreign PEP.

G.2 SCA's systems and controls

406 SCA's systems and controls relating to its monitoring of its customers for the purpose of it meeting its section 36 obligations under the AML/CTF Act with respect to the designated services provided by SCA are discussed in detail at:

a. Section F.4 in relation to junkets;

b. Section F.6 in relation to the TMP;

c. Section F.7 in relation to ECDD;

d. Section F.8 in relation to reporting obligations; and

e. Section F.9 in relation to ACIP/its Standard Part B Programs.

G.3 Higher Risk Customers

407 Each of the 56 customers set out in Appendix A was a customer of SCA on and from the relevant date listed in Column B of Appendix A and was provided with designated services by SCA at various times during the Relevant Period (**Higher Risk Customers**). The Higher Risk Customers were provided with their last designated service from SCA on the dates identified in Column C of Appendix A and were formally banned by SCA from entering the SCA casino on the dates identified in Column D of Appendix A.

408 SCA contravened section 36(1) of the AML/CTF Act by failing to appropriately monitor each of the 56 Higher Risk Customers.

409 During the Relevant Period, higher ML/TF risks arose in respect of each of these 56 Higher Risk Customers, because:

a. 10 customers were junket operators at various times during the Relevant Period.[36] As identified at paragraph 243, the provision of designated services to junket operators involved higher ML/TF risk. Over the Relevant Period, the combined buy-in for the junket programs associated with these 10 junket operators was $75,070,835 with a combined turnover of approximately $716,154,000, resulting in an overall casino loss to SCA of approximately $3,021,000.[37] The turnover for the junket programs run by

[36] Customers 1-10.

[37] The 'overall casino loss' or 'overall casino win' does not represent the actual profit or loss derived by SCA from this precise customer segment. SCA does not allocate expenses at an individual customer-by-customer level, with some minor exceptions, and therefore SCA does not record profit (or loss) attributable to the company at an individual customer-by-customer level. As a consequence, SCA is not able to identify, with precision, the net profit or net loss it generated from a particular customer or customer group. Any such figure would differ to the 'overall casino loss' or 'overall casino win', as it would be impacted by further deductions to account for operating expenses. In the absence of the precise customer-by-customer data required to calculate the net profit after tax and net loss after tax figures, the 'overall casino win' or 'overall casino loss' figures have been used throughout the SAFA as this information is recorded against the customer at an individual customer-by-customer level.

these 10 junket operators ranged from around $2,105,662 (Customer 10) to $330,262,152 (Customer 3).

b. Eight customers were individual commission players at various times during the Relevant Period.[38] Designated services provided to individual commission players involved a higher level of ML/TF risk owing to the size of the transactions involved. Over the Relevant Period, the combined buy-in for the ICPs associated with these eight customers was approximately $140,119,650[39] with a combined turnover of approximately $1,357,834,177, resulting in an overall casino win to SCA of approximately $29,908,000.[40]

c. 46 customers were provided designated services outside of being a junket operator, or playing as part of an ICP.[41] Over the Relevant Period these 46 customers had a total buy-in of $220,903,287,[42] with a combined turnover[43] of approximately $1,437,386,882, resulting in an overall casino win to SCA of approximately $23,379,000.[44] Designated services provided to these 46 customers involved a higher level of ML/TF risk owing to the size of the transactions involved.

d. Two customers were foreign PEPs.[45] One of those customers was not recognised as a foreign PEP by SCA, despite there being public information available prior to the Relevant Period that the customer was a member of a foreign political body.[46]

e. 36 customers were connected to other SCA customers in respect of whom SCA had formed suspicions at various times during the Relevant Period for the purpose of section 41 of the AML/CTF Act.[47]

f. 31 customers were involved (by receipt or transfer) in transactions of large sums totalling approximately $120,100,000, at various times over the Relevant Period.[48] The types of transactions involving large sums included:

    i. transfers of large values to or from other SCA customers in circumstances where SCA was not always aware of, or did not understand, the purpose of the transfer. For example, on 25 April 2019, Customer 2 transferred $380,000 from their SCA FMA to another customer's SCA FMA. SCA noted that the other customer was not onsite and the SCA host could not confirm any reasoning for this transfer, other than that Customer 2 had requested it. SCA completed the transfer;

    ii. large financial transactions involving domestic or international third parties (in some circumstances, the third parties were unknown to SCA). For example, on 2 May 2017, SCA received a deposit of $600,000 into its bank account by an

38 Customers 2, 11,16-17 and 20-23.

39 The estimated customer buy-in totals have been calculated using customer data stored in the Bally CMP system. This includes, amongst other data, data recorded against the customer as 'Chip In'. 'Chip In' data represents the dollar value in chips that a customer has brought to the table which are chips that have already been purchased, or won by a customer, and used by a customer for prior game play. As the 'Chip In' data records chips presented at a gaming table by a customer it is not truly representative of new chip purchases or customer buy-in, which may result in the total estimated buy-in amount included in this SAFA being overstated

40 Refer to footnote 37.

41 Customers 2, 10-13, 15-17, 21-25 and 27-59.

42 Refer to footnote 39.

43 Main gaming floor and VIP (non-program/commission) customer turnover for table game play was calculated by SCA using a combination of assumptions that were derived from averages and estimates applicable to the table game being played by the customer. As a result, for table gaming conducted on the main gaming floor or as a VIP (non-program/commission) customer the turnover amount which SCA recorded against a customer's profile does not necessarily accurately reflect a customer's actual turnover or gaming activity.

44 Refer to footnote 37.

45 Customers 1 and 11.

46 Customer 1.

47 Customers 1-3, 8-9, 11-12, 14-15, 17, 21, 24-25, 27-42, 44-47, 52, 54 and 55.

48 Customers 1-12, 14-17, 20, 22-25, 29, 33, 38, 43-45, 49, 51, 53 and 57.

Australian company. The money deposited into the SCA account was for use by Customer 3's junket. On receipt of the deposit, SCA conducted a company search, which identified that the company was owned by an overseas company. SCA was unable to find a public link between Customer 3's junket and the overseas company. SCA therefore questioned Customer 3, who stated that the Australian company was a finance company of which they were a customer. However, SCA was unable to verify this information, despite the information provided by Customer 3. SCA processed the deposit, and the funds were transferred to Customer 12's FMA at a SCEG New Zealand casino, for use on Customer 3's junket. This matter was the subject of an SMR submitted to AUSTRAC on 4 May 2017; and

iii. large financial transactions from one SCA customer's FMA to another SCA customer's FMA at the SCA casino, where a signed funds authorisation form was provided to SCA. For example, on 4 November 2019 Customer 10 received $488,000 into their FMA from another Australian casino. On 7 November 2019, those funds were transferred to another SCA customer and used for a junket program buy-in at the SCA casino.

g. 30 customers transferred large amounts of money into, out of and within the SCA casino during the Relevant Period through international channels (including the SCEG Customer account channel) and the SCA Customer account channel and at values that gave rise to a higher ML/TF risk. The transactions totalled approximately $94,200,000.[49] For example:

i. on 27 March 2018, Customer 1 transferred $698,287 from a bank account overseas to SCA's bank account to settle an outstanding amount owed to SCA; and

ii. on 11 June 2019, SCA accepted instructions from Customer 8 to transfer approximately $2,100,000 from the customer's FMA at the SCA casino to the customer's bank account overseas. These funds were Customer 8's winnings from a junket program Customer 8 operated at the SCA casino. These funds were transferred by SCA through the SCEG Customer account channel to enable the customer to receive the funds in HKD.

h. 35 customers engaged in transactions identified by SCA as indicative of known ML/TF typologies and vulnerabilities at various times during the Relevant Period. These transactions were indicative of structuring and/or exchanging of CVIs in amounts that were not commensurate with play, transactions where there was no evidence of play or quick turnover of funds without betting, the layering of funds, loan sharking and the use of third parties to conduct transactions.[50] These transactions totalled approximately $11,690,000. For example:

i. on 28 August 2019, Customer 21 presented at a cashier at the SCA casino alongside an associate. The associate then exchanged $30,000 of cash for chips. During the exchange, Customer 27 approached the cashier window and placed an unknown amount of cash into the associate's bag. The associate then gave Customer 21 $10,000 of the $30,000 chips. Over the next hour, the associate did not use the remaining $20,000 chips for gaming, and later collected an additional $12,350 of gaming chips from Customer 21. The associate then exchanged the total of $32,350 in chips for cash at a cashier window. The associate, Customer 21 and Customer 27 then departed the SCA casino together. SCA noted that the associate was a student with minimal

[49] Customers 1-12, 15-17, 20, 22-25, 29, 30, 33, 38, 43-45, 49, 51, 53 and 57.

[50] Customers 2, 11, 17, 20, 21, 24, 27-42, 44-51 and 54-58.

recorded play, and that the associate, Customer 21 and Customer 27 had previously been reported to AUSTRAC in 2017 for a similar exchange. SCA suspected that this transaction was related to the loan sharking business that SCA suspected Customer 27 operated;[51]

ii. on 2 August 2020, Customer 29 was seen to pass an unknown amount of cash to Customer 36. The customers separately proceeded to exchange $7,000 (Customer 36) and $5,000 (Customer 29) in cash for chips. Customer 29 then approached Customer 36, and Customer 36 handed Customer 29 an unknown number of chips. Customer 29 then engaged in gaming activity for several hours. Customer 36 did not have any rated gaming activity on either 2 August 2020 or 3 August 2020. Following a frontline observation report and a surveillance review of the incident, SCA formed a suspicion that Customer 29 had utilised Customer 36 as a third party to structure a pair of transactions to avoid the reporting requirement. SCA stated that Customer 29 had a history of utilising third parties to assist in transaction structuring;[52]

iii. on 12 March 2021, Customer 24 deposited $250,000 in cash into their FMA at the SCA casino. 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. This transaction is indicative of minimal or no gaming activity; and

iv. in or around September 2021, SCA reviewed the bank statements of Person 26. SCA's review of Person 26's bank statements indicated that, between 20 June 2020 and 15 April 2021, Person 26 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 identified that Person 26 may have been utilised as a money mule for a network of money laundering or money concealing activities.[53]

i. 54 customers engaged in large cash transactions of over $10,000 in and/or out of the SCA casino at various times during the Relevant Period.[54] In relation to the transactions involving these customers, SCA submitted 3,646 TTRs to AUSTRAC during the Relevant Period detailing cash transactions of approximately $194.8 million. For example:

i. on 27 January 2018, Customer 11 made a cash deposit of $300,000 into their FMA at the SCA casino; and

ii. on 25 January 2019, Customer 20 engaged in cash transactions at the SCA casino totalling $5,818,180.

j. Nine customers transacted with cash that appeared suspicious, including cash in plastic bags, cash bundled together with rubber bands, cash that was dirty or wet, and counterfeit cash, in transactions totalling over $200,000.[55] For example:

i. on 10 June 2017, SCA identified that Customer 27 had handed a shopping bag to Customer 21 containing $60,000 in cash on SCA's premises. Customer 21

[51] On 30 August 2019, SCA submitted an SMR to the AUSTRAC CEO in relation to this incident.

[52] On 6 August 2020, SCA submitted an SMR to the AUSTRAC CEO in relation to this incident.

[53] On 5 October 2021, SCA submitted an SMR to the AUSTRAC CEO in relation to this matter.

[54] Customers 1-13, 15-17, 20-25, 27-49 and 51-59.

[55] Customers 11, 21, 27, 29, 31, 35, 39, 40 and 43.

then exchanged the cash for a $60,000 CPV at a cashier window at the SCA casino, which was then exchanged for casino chips at a gaming table. Customer 21 then immediately left the gaming table and gave the $60,000 in chips to Customer 27, who proceeded to exchange the chips at a cashier window at the SCA casino. On 13 June 2017, SCA submitted an SMR to the AUSTRAC CEO in relation to this incident and advised that both parties would continue to be monitored; and

ii. on 4 October 2018, SCA observed that Customer 39 had conducted a $9,000 chip buy-in at the SCA Cage with cash covered in dirt. Customer 39 then went to a gaming table and completed a second buy-in of $4,000 with cash, which they handed to Customer 38 (their spouse). Customer 39 subsequently completed a third buy-in of $7,000 at another gaming table. Customer 39 did not game with the $16,000 worth of chips in their possession, instead, about an hour after the multiple buy-ins, Customer 39 discreetly handed an unknown and unverified amount of chips to Person 7. SCA had concerns about the state the cash was in, the multiple buy-ins with little to no gaming activity and third-party exchanges. On 9 October 2018, SCA submitted an SMR to the AUSTRAC CEO in relation to this incident and advised that each of the parties would continue to be closely monitored.

k. SCA submitted approximately 120 SMRs to AUSTRAC in relation to the Higher Risk Customers over the Relevant Period. 59 of those SMRs related to more than one Higher Risk Customer. The SMRs submitted to AUSTRAC related to transactions involving 42 of the Higher Risk Customers which SCA had identified as being indicative of structuring, layering and/or refining, and/or large and unusual transactions and patterns of transactions which had no apparent economic or visible lawful purpose.[56]

l. 17 customers were the subject of enquiries made by law enforcement agencies to SCA or information shared by law enforcement agencies with SCA at various times during the Relevant Period.[57] In relation to two customers, SCA came into receipt of this information after the last designated service was provided to the customer.[58] For example:

i. on 23 August 2018, a law enforcement agency informed SCA that Customer 41 and Customer 42 were associated with a prostitution syndicate and they could be attending SCA to launder funds obtained through the syndicate;

ii. on 29 November 2017, SCA received information from a law enforcement agency that Customer 45 was suspected of dealing with proceeds of crime worth more than $1 million and SCA held concerns that Customer 44 was sharing funds with Customer 45; and

iii. 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 regarding Customer 16 from law enforcement.

m. SCA was aware of information suggesting that 21 customers were connected to organised crime, or that allegations of criminal conduct had been made against the customer or the customer had been charged, arrested, prosecuted, previously

[56] Customers 2, 3, 11, 12, 15-17, 20, 21, 24, 25, 27-42 and 44-58.

[57] Customers 1, 3, 5, 11, 12, 13, 16, 24, 41-46, 51, 53 and 57.

[58] Customers 3 and 12.

convicted or imprisoned in connection with offences, including in some cases dealing with the proceeds of crime and money laundering, prior to SCA issuing a ban to those customers.[59] In relation to three of the customers, SCA became aware of the information after it had provided the customer with its last designated service but prior to SCA formally banning the customer.[60] For example:

i. On or around 21 July 2021, Jade identified that Customer 43 was the subject of a conviction from 2004 concerning their involvement in a drug trafficking syndicate. Jade also identified prior drug trafficking convictions dating back to 1983.

ii. At the time, SCA considered its relationship with Customer 43 and due to the age of the offences and the customer's wealth (which SCA formed the view was plausible) determined to retain the customer but escalated them to high risk.

iii. On 5 May 2022, SCA engaged with a law enforcement agency to discuss some of SCA's customers, including Customer 43 who was described during the meeting as being an established figure in organised crime, with a long history of association with drug trafficking and drug importation.

iv. Notwithstanding the correspondence from the law enforcement agency and the further due diligence that SCA undertook at this time to consider the ML/TF risk of providing designated services to the customer, SCA continued to provide designated services to Customer 43 until at least 26 October 2022.

n. SCA approved CCFs in respect of eight of the customers with limits ranging from $20,000 to $8,100,000.[61]

o. SCA facilitated third party deposits to the FMAs of 14 of the customers (see paragraphs 166 and 231), including by:[62]

i. transfer from an FMA held by a third party;

ii. transfer from a bank account via the SCA Customer account channel;

iii. depositing funds into an FMA via the SkyCity New Zealand channel; and

iv. transfer from a bank account via the SCEG Customer account channel. SCA introduced a SOP which provided that after June 2021 third party deposits (via telegraphic transfer) into SCEG Customer accounts to be transferred to another customer's FMA were no longer accepted (other than in limited circumstances). In September 2022, SCA introduced guidance for staff about the process for third party payment rejection where third party deposits (via telegraphic transfer) were made into the SCEG Customer account channel.

410 Sub-paragraphs 409a to409c above refer to combined turnover, which resulted in casino wins or losses. As stated above at paragraph 63, the turnover figures referenced in this SAFA measure turnover generated by customer gaming activities across the Relevant Period. It does not represent turnover that would not have necessarily arisen but for the contraventions admitted in this SAFA (the extent of which is not known).

[59] Customers 1, 5, 11-12, 16, 29-35, 40-43, 45-46, 52 and 57-58.

[60] Customers 11-12 and 34.

[61] Customers 1, 4-8, 11 and 16.

[62] Customers 1-3, 7, 10-12, 14-17, 20, 25 and 45.

G3.1 Non-Compliance with section 36

411 As a result of the matters referred to at paragraphs 407 to 409 above, at various times during the Relevant Period:

a. designated services provided to 56 Higher Risk Customers at the SCA casino posed higher ML/TF risks; and

b. in contravention of section 36(1) of the AML/CTF Act, SCA did not conduct appropriate risk-based OCDD with respect to each of the 56 Higher Risk Customers, with a view to identifying, mitigating and managing the ML/TF risk posed by the provision of designated services to those customers.

412 In particular:

a. SCA did not elevate 19 of the customers' risk ratings to 'high risk' within a reasonable period of time after each customer had demonstrated conduct which gave rise to a higher ML/TF risk.[63] Of those 19 customers, 14 were assigned a 'high risk' rating more than one year after they demonstrated high risk conduct;[64]

b. SCA did not identify three of the customers as high risk before 7 December 2022, where those customers had demonstrated conduct warranting elevation of the customer's risk rating to 'high risk';[65]

c. SCA did not carry out adequate ECDD measures with respect to 53 of the customers in circumstances where:[66]

i. SCA had formed a suspicion with respect to those Higher Risk Customers for the purposes of section 41 of the AML/CTF Act; or

ii. SCA had rated a customer as 'high risk'; or

iii. the customer was a foreign PEP; and

d. SCA did not obtain from the customer or appropriately consider information concerning the source of funds and/or source of wealth in relation to 50 of the customers.[67] These customers continued to receive designated services in circumstances where SCA did not hold appropriate source of wealth and/or source of funds information, or, where that information or stated occupation was available, it was incommensurate with their gaming activity. For example:

i. on 1 August 2019, SCA undertook ECDD in relation to Customer 49. The ECDD undertaken was limited to open-source checks, which did not identify any additional information about Customer 49 beyond that which SCA already held. At the time, SCA did not make any additional enquiries in relation to Customer 49's source of wealth or source of funds (beyond the open-source checks by SCA), in circumstances where SCA should have been aware that the customer's level of gaming (between 7 December 2016 to the end of FY19, SCA had recorded a combined turnover of approximately $5,257,000 for Customer 49 against a combined buy-in of approximately $1,855,525)[68] did not appear to be commensurate with their stated occupation ('mechanical

[63] Customers 3, 5, 7, 14, 20, 22, 34-35, 39, 40-42, 46, 49, 53 and 56-58.

[64] Customers 3, 5, 7, 20, 22, 33-35, 39-42 and 57-58.

[65] Customers 4, 9 and 13.

[66] Customers 1-3, 5-8, 10-12, 14-17, 20-25 and 27-59.

[67] Customers 1-12, 15-17, 21-25 and 27-56.

[68] Refer to footnote 39.

engineer'). As a result, the steps taken to obtain and consider additional source of wealth and/or source of funds information in relation to Customer 49 were inadequate;

ii. at all times on and from 7 December 2016, SCA had identified that Customer 2 was the president of Company 2. It was estimated that Company 2 generated an annual revenue of $834,000 (based on a company that provides commercial data, analytics and insights for businesses). Customer 2 was also a junket operator. The last designated service provided to Customer 2 was on 10 March 2021. However, SCA did not request that Customer 2 provide additional source of wealth information until 9 August 2021. This is notwithstanding that from January 2017 SCA had submitted 30 SMRs to the AUSTRAC CEO (where in some of the SMRs, SCA identified that it suspected Customer 2 and their associates were engaging in potential money lending activities and other activities indicative of ML/TF typologies), and SCA had recorded from 7 December 2016 to the end of FY21 combined turnover of approximately $31,526,000 against a combined buy-in of approximately $5,822,900[69] for Customer 2, other than through junket programs or ICPs. On 9 August 2021, SCA terminated its relationship with Customer 2 until an assessment of their Source of Wealth Declaration Form was completed. On or around 16 August 2021, Customer 2 declined to provide SCA with source of wealth information and as a result the relationship with the customer remains terminated; and

iii. see Customer 41's case study below at paragraphs 429 to 436;

e. in relation to 31 customers that were escalated to senior management for consideration, insufficient regard was given by senior management to the higher ML/TF risk associated with those customers, including in relation to the customer's source of wealth and/or source of funds, the information known or obtained about the customer, and/or the customer's known risk profile, when determining whether the business relationship with those customers should continue.[70] Relevantly:

i. 27 customers were included in a Transaction Monitoring Overview Report provided to senior management for consideration, and/or were escalated to senior management for consideration because of a particular transaction or other matters.[71] For example, a May 2021 Transaction Monitoring Overview Report recorded that between 22 and 28 February 2021, Customer 23 received three cheques from SCA totalling $1 million from commission play and table game wins. This was in circumstances where SCA recorded Customer 23's occupation as 'Rail Manager' from May 2016, and in the 2021 financial year Customer 23's combined buy-in on ICPs escalated to over $3,300,000, from just over $54,000 in the 2019 financial year and no buy-in in the 2020 financial year.[72] The minutes of the May 2021 AML/CTF Senior Management Group do not record any discussions relating to Customer 23. SCA did not request additional source of wealth information from Customer 23 until 23 June 2021, which Customer 23 did not provide. Notwithstanding that the last designated service provided to the customer was on 19 April 2021, Customer 23 was not barred by SCA until in or around June 2022; and

ii. in relation to four customers escalated to senior management for consideration, senior management approved the continuation of a business relationship or approved the continuation of designated services on at least one occasion for

[69] Refer to footnote 39.

[70] Customers 1-3, 5, 6, 8, 10-12, 14, 16, 17, 22-24, 27, 29, 35, 37-39, 43-45, 47, 49, 51-53, 57 and 58.

[71] Customers 2, 3, 5-6, 8, 10, 11-12, 14, 16-17, 23, 27, 29, 35, 37-39, 44-45, 47, 49, 51-53, 57 and 58.

[72] Refer to footnote 39.

each of those four customers.[73] This decision was made despite the customers engaging in conduct indicating higher ML/TF risks as set out in paragraph 409. For example, on 1 October 2021, the SCA AML Compliance Manager escalated Customer 24 to senior management on the basis that Customer 24 represented a significant level of risk. The risk rating escalation followed the receipt of a warrant served on SCA by a law enforcement agency concerning Customer 24 and an attempt by Customer 24 to make a $1 million cash deposit on their FMA at the SCA casino. Between 1 and 5 October 2021, senior management determined to continue its relationship with Customer 24 on three occasions. Senior management decided not to bar the customer from the SCA casino on the basis that the law enforcement inquiry was at a preliminary stage and that SCA would not accept the requested transaction from the customer until further notice. Despite receiving a further inquiry from a law enforcement agency and becoming aware that a law enforcement agency had seized $1 million in cash from Customer 24's home during this period, it was not until February 2022 that SCA issued a ban in respect of Customer 24. The ban was made following further communications from the law enforcement agency that Customer 24's statutory declarations as to their source of wealth and source of funds more than likely contained false information.

G.4 Higher Risk Customer case studies

413 The following three case studies illustrate how some of the Higher Risk Customers demonstrated the high risk factors described in paragraph 409 above, but where SCA did not appropriately monitor those customers for the purposes of section 36 of the AML/CTF Act.

G.4.1 Customer 1 – Junket Operator

414 Customer 1 was a customer of SCA between 14 June 2016 and 7 October 2020 (when SCA provided the last designated service to the customer). On 7 October 2020, the AML/CTF Senior Management Group temporarily suspended SCA's business relationship with Customer 1, pending the findings of the ongoing investigation into Customer 1 by the NSW Independent Liquor & Gaming Authority (**ILGA**). On 22 March 2022, SCA issued a ban in respect of Customer 1 pursuant to section 27AA of the Casino Act on the basis that Customer 1 was part of the Suncity Junket and had been the subject of adverse media. At no time between 7 October 2020 (when SCA temporarily suspended Customer 1) and 22 March 2022 (when SCA formally banned Customer 1) were any designated services provided to Customer 1.

415 The total combined turnover of the junkets operated by Customer 1 between financial year 2018 and financial year 2020 was approximately $120.08 million with buy-in of approximately $23.2 million,[74] resulting in a casino loss to SCA of least $6 million. Many of the junket players on Customer 1's junket programs posed higher ML/TF risks, including Customer 2, Customer 13 and Customer 14.

416 On 18 October 2016, Customer 1 was elevated to 'high risk'. SCA was aware that Customer 1 was a Suncity junket operator, and that Customer 1 was the founder and chairman of the Suncity Group and its subsidiaries. By August 2016, SCA senior management was also aware from a third party report dated 30 May 2016 that, among other things, Suncity had allegedly made illegal campaign contributions to a candidate for a foreign political office and that funds stolen from an overseas central bank were allegedly deposited into accounts held by Suncity at an overseas casino. The report identified a number of ML/TF risks in respect of

[73] Customers 1, 22, 24 and 43.

[74] Refer to footnotes 39 and 43.

the Suncity junket, including that Customer 1 was a foreign PEP, and that some adverse information was contained in publicly available media articles.

417 By 7 December 2016, there were online publications naming Customer 1 as a person linked to overseas organised crime syndicates. From 2017, publicly available media reports named Customer 1 and the company Suncity as having engaged in proxy betting, online gambling and underground banking. It was not until 27 July 2019 that members of the SCA and SCEG senior management team became aware of media reports which linked Suncity to an overseas crime syndicate and 8 August 2019 that SCA became aware of the media allegations relating to Suncity's association with proxy betting and online gambling. If SCA had been aware of these media articles at the time they were published, it would have been required to take these into account in considering the ML/TF risks posed by conducting business with Customer 1.

418 Between December 2017 and March 2020, Customer 1 operated and funded 12 junket programs at the SCA casino. SCA provided Customer 1, in their capacity as junket operator, with significant amounts of credit upon request, with lines of credit ranging from $300,000 to $8,100,000 to run the junket programs. At various points during the Relevant Period, Customer 1 also had access to monthly lines of credit ranging up to NZD$25 million. Pursuant to a signed Funds Authorisation Letter, Customer 1 also made some of the Suncity lines of credit available to another Suncity junket operator, for the purpose of operating Suncity junket programs (which was subject to a special condition requiring the other Suncity junket operator to seek authorisation from the Suncity Group cage department, which was part of the Suncity Group, prior to performing any transaction with those funds).

419 SCA also provided designated services to Customer 1 by remitting large amounts of money through high risk channels, including the SCEG Customer account channel, the SkyCity New Zealand channel and the SCA Customer account channel. For example:

a. on 28 March 2018, SCA received $698,287 from an overseas bank account on behalf of Customer 1. The funds were transferred to buy back an outstanding cheque; and

b. on 22 January 2019, a foreign company connected to Suncity deposited HKD$4,876,545 (AUD$873,917) into a SCEG Customer account. A SCEG New Zealand casino then transferred the funds to SCA, and the funds were made available to Customer 1 in the amount of $873,917 and were used to repay an outstanding line of credit for a Suncity junket.

420 In October 2019, SCA became aware of media articles which reported that Customer 1 had been banned from entering Australia. The articles also reported that Suncity denied that Suncity or Customer 1 were being investigated by authorities in Australia.

421 In August 2019, a member of the International Business team (a division of SCEG) met with Suncity and asked them to comment on the adverse media coverage. Suncity denied all the allegations. Based on the meeting, the team member found no grounds to recommend terminating the business relationship with the Suncity junket and Customer 1. In November 2019, SCEG senior management renewed Customer 1's junket agreement. Following SCEG senior management's decision, SCA also continued its business relationship with Customer 1, and in November 2019 and March 2020 Customer 1 operated Suncity junkets at the SCA casino.

422 Between 7 December 2016 and 22 March 2022, SCA did not take appropriate steps to formally end its relationship with Customer 1 or to understand whether Customer 1's source of wealth and/or source of funds were legitimate, for the purposes of section 36 of the AML/CTF Act. Further, until 7 October 2020 (when SCA temporarily ceased its relationship with the customer and provided them with their last designated service) SCA did not appropriately monitor Customer 1's transactions on a risk-basis as a result of the deficiencies in SCA's TMP, for the purposes of section 36 of the AML/CTF Act.

G.4.2 Customer 21 – Individual Commission Player

423 SCA provided designated services to Customer 21 between 15 June 2015 and 31 March 2021. On 22 March 2022, SCA banned Customer 21 from attending the SCA casino. By 7 December 2016, SCA understood that Customer 21's occupation was a 'restaurant entrepreneur'. From 23 December 2016, SCA understood that Customer 21 was the owner of a 'sushi shop'. Between 2016 and 2021, SCA recorded turnover of approximately $19,482,000 for Customer 21. This included play on ICPs and non-commission play.

424 In the financial year 2019, Customer 21 entered into two ICPAs with SCA and had a total buy-in of $233,000,[75] with total turnover of $3,601,796, resulting in an overall casino win to SCA of $164,050.[76] Customer 21 also received commissions of approximately $19,826.

425 Between 23 December 2016 and 15 March 2021, SCA gave the AUSTRAC CEO seven SMRs with respect to Customer 21. Following the SMR dated 23 December 2016, Customer 21 was elevated to high risk by SCA. The SMRs indicated that Customer 21 had engaged in large and unusual transactions at the SCA casino, including suspicious transactions with other higher-risk customers and transactions that were indicative of ML/TF typologies and vulnerabilities such as structuring and loan sharking. For example:

a. on 23 December 2016, SCA submitted an SMR to AUSTRAC in relation to suspicious gambling activity concerning Customer 21 and Customer 27 on 22 December 2016. In that incident, SCA staff observed that Customer 21 had exchanged $100,000 in CPVs for casino chips, which were then transferred over the course of an hour in $5,000 stacks to Customer 27;

b. on 21 April 2017, SCA submitted an SMR to AUSTRAC after Customer 21 engaged in a number of suspicious cash and chip exchanges at the SCA casino alongside other customers including Customer 2 and Customer 27. SCA concluded that Customer 21 had potentially assisted the customers to engage in prohibited money lending; and

c. on 9 February 2021, SCA submitted an SMR to AUSTRAC after Customer 21 engaged in a number of suspicious cash and chip exchanges at the SCA casino alongside three other customers. SCA concluded that Customer 21 was using the other customers to conduct threshold transactions on their behalf in order to avoid reporting requirements.

426 Between 7 December 2016 and 31 March 2021, transactions by Customer 21 and their associates at the SCA casino included: large and unusual transactions, which had no apparent economic or visible lawful purpose; suspicious cash and chip exchanges which Customer 21 tried to disguise (following which SCA concluded that Customer 21 had assisted other customers to engage in prohibited money lending); large amounts of cash and cash that appeared suspicious (including cash given to Customer 21 by Customer 27 in a shopping bag), and transactions indicative of ML/TF typologies including using third parties to avoid reporting requirements.

427 On 12 September 2019, SCA's records show that ECDD was undertaken with respect to Customer 21. However, when the ECDD was undertaken, SCA did not take adequate steps to understand whether Customer 21's source of wealth and/or source of funds were legitimate, in particular, where the customer's stated occupation was the owner of a 'sushi shop' and the customer's level of gaming activity did not appear to be commensurate with that stated occupation. Despite this, at no time did SCA seek additional source of funds or source of wealth information from Customer 21.

---

[75] Refer to footnote 39.

[76] Refer to footnote 37.

428 Between 7 December 2016 and 22 March 2022, SCA did not take appropriate steps to understand whether Customer 21's source of wealth and/or source of funds were legitimate, or appropriately monitor Customer 21's transactions on a risk-basis as a result of the deficiencies in SCA's TMP, for the purposes of section 36 of the AML/CTF Act.

G.4.3 Customer 41 – Domestic customer

429 SCA provided designated services to Customer 41 between 30 July 2018 and 9 October 2021. Between August 2018 and October 2021, Customer 41 had a total buy-in of $2,455,615[77] with total turnover of $8,775,740, resulting in an overall casino win to SCA of $228,346.[78]

430 Customer 41 was connected to other customers at the SCA casino who posed high ML/TF risks, such as Customer 40, Customer 42 and Customer 58.

431 On 27 August 2018, SCA submitted an SMR to AUSTRAC in relation to Customer 41 and some of their known associates, including Customer 42. The SMR related to three incidents that occurred on 30 July 2018 and 9 August 2018, where SCA staff observed suspicious cash and chip exchanges between Customer 41 and other customers which were indicative of structuring. The SMR stated that, on 23 August 2018, SCA received information from a law enforcement agency that an illegal escort syndicate could potentially be attending the SCA casino to launder funds. The SMR indicated that due to Customer 42's involvement in two of the three incidents, and after conducting open source checks, SCA formed the suspicion that Customer 41 and their associates may be part of an illegal escort syndicate and were potentially laundering funds gained from that syndicate. Under paragraph 32 of section 3 and Schedule 1 of SCA's 2018 Standard Part A Program, these events required Customer 41's risk rating to be elevated to 'high risk'.

432 Notwithstanding the information from the law enforcement agency and the identified structuring of transactions which occurred in August 2018, Customer 41's risk rating was only elevated to 'high risk' by SCA on 31 December 2020. As a result, Customer 41 was provided with designated services for over two years while the customer was not recorded as being a higher risk and should have been.

433 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 'housewife' or 'home duties'. Customer 41's gambling activity was not commensurate with their stated occupation. Under paragraph 32 of section 3 and Schedule 1 of SCA's 2018-2019 Standard Part A Program, this should have triggered Customer 41's risk rating to be elevated to 'high risk' and for ECDD to be undertaken. Despite this, as identified above, Customer 41 was not rated 'high risk' until 31 December 2020.

434 Despite Customer 41's gaming activity being incommensurate with their stated occupation, SCA did not seek additional source of wealth information from the customer until at least 24 August 2021. This request was made following the submission of an SMR to the AUSTRAC CEO on 24 August 2021, which identified that the customer's gaming activity was incommensurate with their stated occupation. In response to this request, on 16 September 2021, Customer 41 completed a Source of Wealth Declaration Form. In the form, Customer 41 provided minimal information and claimed that their parent and ex-partner fully supported their gaming. On 18 November 2021, ECDD was subsequently undertaken in relation to Customer 41, which found that Customer 41 had provided inadequate information in their Source of Wealth Declaration Form.

435 At no time between 27 August 2018 and 16 September 2021 did SCA take appropriate steps to fully understand whether Customer 41's source of wealth and/or source of funds were

[77] Refer to footnote 39.

[78] Refer to footnote 37.

legitimate or appropriately monitor Customer 41's transactions on a risk-basis as a result of the deficiencies in SCA's TMP, for the purposes of section 36 of the AML/CTF Act.

436 On or around 9 December 2021, SCA banned Customer 41 from attending the SCA casino due to inadequate information regarding their source of wealth.

G.5 Customers who transacted through the SCEG Customer account channel

437 Each of the 65 customers set out in Appendix B were customers of SCA at various times during the Relevant Period (**SCEG Channel Customers**).

438 At various times during the Relevant Period, SCA provided designated services to each of the SCEG Channel Customers within the meaning of table 1 and table 3, section 6 of the AML/CTF Act when transactions were made to the SCEG Channel Customers' FMAs through the SCEG Customer account channel.

439 Payments through this channel carried higher ML/TF risks, for reasons which include:

a. SCA did not take adequate steps to understand the source of funds relevant to the transaction;

b. in some instances, third party transactions (including both telegraphic and cash deposits) were made to a SCEG Channel Customer's FMA through the SCEG Customer account channel where SCA did not record the identity of the third party;

c. payments through this channel were not face-to-face and money could be made available to a SCA customer's FMA without formal cross-border transfer of funds;

d. transfers through this channel could be made in foreign currencies; and

e. transactions involving the SCEG Channel Customers sometimes involved the transfer of large amounts of money for or on behalf of some of the Higher Risk Customers.

440 At various times during the Relevant Period, SCA facilitated transactions on behalf of the SCEG Channel Customers through the SCEG Customer account channel, in both Australian dollars and foreign currencies. Between 12 December 2016 and 15 July 2022, the SCEG Channel Customers accessed approximately AUD$29.16 million[79] through the SCEG customer account channels, including transactions through the Horizon Tourism account channel totalling $1,300,000. The Horizon Tourism account channel posed particularly high ML/TF risks, including because the accounts were not transparent as their connection to SCA was not apparent on their face.

441 SCA's TMP did not adequately monitor the transactions through the SCEG Customer account channel to an FMA. For the reasons above, SCA did not adequately monitor the SCEG Channel Customers with a view to identifying, mitigating and managing the ML/TF risk posed by these customers.

G.6 Contraventions

442 By reason of the matters set out at paragraphs 407 to 441 above, during the Relevant Period, SCA contravened section 36(1) of the AML/CTF Act by failing to appropriately monitor each of the 56 Higher Risk Customers and each of the 65 SCEG Channel Customers in relation to the provision of designated services:

[79] This figure is the summation of the two different currencies (AUD and HKD). The parties have used the historical daily exchange rate provided by the Reserve Bank of Australia to calculate this conversion.

a. with a view to identifying, mitigating and managing the ML/TF risk that SCA reasonably faced; and

b. in accordance with Chapter 15 of the AML/CTF Rules.

H. FACTS RELEVANT TO RELIEF

H.1 Nature and extent of the contraventions

H.1.1 Section 81 of the AML/CTF Act – AML/CTF Programs

443 From 7 December 2016 to 14 December 2022, SCA contravened section 81 of the AML/CTF Act by providing designated services in circumstances where its Standard Part A Programs did not, for the reasons described at paragraphs 401 to 403, fully comply with the requirements of the AML/CTF Act and AML/CTF Rules. Each time SCA provided a designated service during that period, it contravened section 81 of the AML/CTF Act. The contraventions are significant in number but too numerous to quantify. The maximum penalty for each contravention of the AML/CTF Act during the Relevant Period ranges from $18 million to $22.2 million.

Part A – Program failures with respect to identification, mitigation and management of ML/TF risk

444 SCA's contraventions relating to its AML/CTF Program failures were serious because:

a. The ML/TF risk of SCA's business was high. The vulnerability of the casino industry to ML/TF risk was well-known and the subject of typologies and guidance published by relevant authorities, from time to time, including AUSTRAC.

b. The AML/CTF Act reposed a high degree of trust in SCA to identify, mitigate and manage the ML/TF risk of its own business.

c. Part A of an AML/CTF program is the framework through which boards and senior management understand their ML/TF risk and determine their ML/TF risk appetite. It is the framework through which boards and senior management determine the risk-based controls they will apply to mitigate and manage the ML/TF risk they choose to accept. SCA's failure to implement an appropriate Part A program meant that SCA was not in a position to be able to appropriately identify, mitigate and manage the ML/TF risk reasonably faced by SCA, or satisfactorily fulfil its obligations under the AML/CTF Act.

d. In the absence of appropriate ML/TF risk management, a number of high-risk practices, channels and customer relationships evolved at SCA which exacerbated the already high ML/TF risk of designated services.

e. SCA was required to assess the ML/TF risk of all designated services it provided – both gaming and financial. The requirement to carry out and maintain current ML/TF risk assessments of designated services is central and foundational to an AML/CTF program and to the AML/CTF Act.

f. Having failed to properly assess and understand all of its ML/TF risk across its business, SCA's Standard Part A Programs were incapable of appropriately mitigating and managing some of the high ML/TF risk it faced.

g. In order for SCA's Standard Part A Programs to appropriately mitigate and manage its higher ML/TF risk and have appropriate risk-based systems and controls, as required by the AML/CTF Act, SCA was required to ensure it comprehensively assessed and identified the ML/TF risk it reasonably faced across its business.

h. SCA failed to adequately identify, mitigate and manage the higher ML/TF risk of providing designated services through the junket channel until it banned dealing with junkets on 12 April 2021. Junkets presented higher ML/TF risk due to the large amounts of money involved which were often moved across borders. Junkets also often lacked transparency and provided a level of anonymity to players and the source(s) of their funds. Between 7 December 2016 and 2 January 2021, SCA generated $26 million in gross revenue from junkets.

i. SCA's Standard Part A Programs were not subject to an appropriate approval and oversight framework.

j. In the absence of appropriate risk-based controls in SCA's Standard Part A Programs that were sufficiently aligned to the ML/TF risk that SCA reasonably faced with respect to the provision of designated services it provided, money could be moved into and out of the SCA casino and within the SCA casino, in ways that lacked transparency as to the source and ownership of funds. This made SCA vulnerable to the risk of criminal exploitation.

k. SCA's failure to adequately identify and manage the ML/TF risk of its business and to adequately monitor these transactions for suspicious activity has resulted in the loss of opportunity to detect, trace and disrupt possible unlawful activity, including possible money laundering.

445 The deficiencies in SCA's Standard Part A Programs persisted throughout the Relevant Period and were systemic.

446 SCA has implemented changes to the operation of its Standard Part A Program as part of its AML Enhancement Program (**AML EP**). Amendments to SCA's Standard Part A Programs are described further in Section H.8. While the AML EP is ongoing, the steps SCA has taken to date have reduced (and in some cases eliminated, for example with respect to junkets) its exposure to ML/TF risk.

Part A – Transaction monitoring program (TMP)

447 For the reasons set out at paragraphs 318 to 321, the deficiencies in SCA's TMPs meant that it did not fully comply with the AML/CTF Act or the AML/CTF Rules. These contraventions were serious because:

a. The AML/CTF Act reposes a high degree of trust in a reporting entity to monitor transactions of its customers having regard to the ML/TF risk of its own business.

b. Appropriate risk-based transaction monitoring is central to ensuring that matters that may be suspicious for the purposes of section 41 of the AML/CTF Act are identified and reported to the AUSTRAC CEO and, consequently, law enforcement. Appropriate risk-based transaction monitoring is central to SCA's understanding of its own ML/TF risk, including emerging risks.

c. The deficiencies in SCA's TMPs were systemic and persisted over a number of years:

i. SCA's TMPs were not aligned to an appropriate ML/TF risk assessment.

ii. SCA's TMPs did not appropriately cover all designated services provided by SCA – both financial and gaming. For example, SCA did not appropriately monitor designated services provided through the SCEG Customer account channel.

iii. SCA's TMPs relied on manual and observational processes (as described at paragraph 321). Those manual and observational processes, whilst forming an

important aspect of SCA's TMPs to support its automated processes, were not adequate, having regard to the nature, size and complexity of the business that SCA operated and the types of ML/TF risk that arose from that business.

iv. Insufficient resourcing in the AML team had an impact on SCA's ability to consistently monitor the transactions of its customers.

v. SCA's TMPs did not include adequate risk-based procedures to consistently monitor all customer transactions that may been indicative of well-known ML/TF typologies and vulnerabilities.

vi. SCA's TMPs did not include or incorporate appropriate risk-based systems and controls for assurance. Accordingly, SCA did not have in place appropriate risk-based systems and controls to ensure that SCA's TMPs were being applied correctly, operating as intended, and remained aligned to SCA's ML/TF risk.

vii. Limitations with the information management systems used by SCA had an impact on SCA's ability to effectively monitor all ML/TF risk arising from transactions with its customers.

viii. SCA did not appropriately monitor payment flows to and from SCA through the SCA Customer account channel, SCEG Customer account channel and SkyCity New Zealand channel. Nor did SCA appropriately monitor transactions, including cross-border transactions through high risk junket channels. These failures exposed the Australian financial system and the Australian community to ML/TF risk.

d. The deficiencies in SCA's TMPs impacted SCA's ability to appropriately monitor the transactions of its customers, including approximately $3.5 billion in turnover for the 56 Higher Risk Customers, for suspicious activity. This resulted in the loss of opportunity to detect, trace and disrupt possible unlawful activity, including possible money laundering, and to report suspicious matters to AUSTRAC and, consequently, law enforcement.

448 SCA has implemented changes to the operation of its TMP as part of its AML EP. Amendments to SCA's TMP are described further in Section H.8.

Part A – ECDD Program

449 For the reasons set out at paragraph 343, the deficiencies in SCA's ECDD Programs meant that it did not fully comply with the AML/CTF Rules throughout the Relevant Period. These contraventions were serious because:

a. The nature of SCA's business meant that it was exposed to and dealt with high ML/TF risk customers, which included junket operators, junket players, international VIP customers, high rollers and foreign PEPs. The high ML/TF risks posed by these customer types were well-known and the subject of typologies and guidance published by the relevant authorities, from time to time, including AUSTRAC.

b. During the Relevant Period, the deficiencies in SCA's ECDD Programs meant that it was not capable of appropriately identifying and escalating customers who posed a higher ML/TF risk to be the subject of ECDD, where required by the AML/CTF Act and the AML/CTF Rules.

c. During the Relevant Period, SCA's application of the ECDD process was ad hoc and discretionary, with no written process or procedure setting out the relevant measures to be undertaken when completing ECDD based on the level of ML/TF risk faced. This

impacted SCA's ability to consistently comply with its ECDD and OCDD obligations under the AML/CTF Act and the AML/CTF Rules.

d. During the Relevant Period, SCA's ECDD Programs did not include appropriate systems, controls and procedures to ensure that source of wealth and source of funds information was obtained, analysed and recorded for the purposes of carrying out ECDD. This, in turn, created a risk of inhibiting the ability of Australian law enforcement agencies and AUSTRAC to trace money to its source and undertake associated law enforcement investigations, prosecutions and recovery of proceeds of crime.

e. SCA's ECDD Programs were not supported by appropriate information management and record keeping such that SCA did not always have a full view of a customer's transactions and risk profile when conducting ECDD on a customer that had previously been subject to ECDD.

f. SCA's Standard Part A Programs did not set out specific criteria against which senior management could appropriately determine whether to approve continuing a business relationship with a customer, including whether to continue providing that customer with designated services. This impacted SCA's ability to consistently comply with its ECDD and OCDD obligations under the AML/CTF Act and the AML/CTF Rules, and in some instances, SCA continued an ongoing relationship with a customer in circumstances where it did not have adequate regard to the ML/TF risk posed by that customer, or the consideration of that risk was delayed. These failures exposed SCA to the risk of being exploited by organised crime.

450 SCA has implemented changes to the operation of its ECDD Program as part of its AML EP. Amendments to SCA's ECDD Programs are described further in Section H.8.

Part A – Systems and controls for SMR, TTR and IFTI reporting

451 For the reasons set out at paragraphs 363 to 366, the deficiencies in relation to the systems and controls which SCA had designed and implemented for the purpose of complying with its reporting obligations meant that it did not fully comply with the AML/CTF Act and the AML/CTF Rules. These contraventions were serious because:

a. As a result of the failure to include appropriate systems and controls in the Standard Part A Programs to ensure compliance with the obligation to report under sections 41, 43 and 45 of the AML/CTF Act, AUSTRAC and law enforcement agencies were denied financial intelligence to which they were entitled. This undermines the objectives of the AML/CTF Act and impacts the ability of AUSTRAC and law enforcement to carry out their functions. In particular, failure to provide required reports or required information to AUSTRAC inhibits law enforcement investigations, prosecutions and the recovery of proceeds of crime.

b. TTRs relating to transactions on junket programs at the SCA casino were likely to be reported under the junket operator's name (as described at paragraph 365a above). This made it difficult for AUSTRAC and law enforcement agencies to fully understand the role of different parties to the transaction, any potentially suspicious activity or the transaction generally.

c. SCA's lack of a documented process to obtain the relevant information for transactions which were processed to SCA through the SCEG Customer account channel, and the occasional practice of aggregating customer deposits into SCA Customer accounts and SCEG Customer accounts, in certain instances, could have resulted in SCA submitting IFTIs to AUSTRAC containing incorrect information.

452 SCA has implemented changes to the operation of its systems and controls for SMR, IFTI and TTR reporting as part of its AML EP. Amendments to SCA's systems and controls for SMR, IFTI and TTR reporting are described further in Section H.8.

Part B – ACIP

453 For the reasons set out at paragraph 390 to 393, the deficiencies in SCA's Standard Part B Programs meant that it did not sufficiently comply with the AML/CTF Rules. These contraventions were serious because:

a. The nature of SCA's business meant that it was exposed to and dealt with high ML/TF risk customers, which included junket operators, junket players, international VIP customers, high rollers and foreign PEPs. The high ML/TF risks posed by these customer types were well-known and the subject of typologies and guidance published by the relevant authorities, including AUSTRAC.

b. There was a lack of clear processes and procedures in the Standard Part B Programs to ensure that at the time ACIP was carried out, a customer's risk rating would be elevated from the default rating of 'low risk' in accordance with the Risk Allocation Criteria set out in SCA's Standard Part A Programs.

c. Not elevating the customer's risk rating at the time ACIP was conducted had an impact on identifying whether additional KYC information should have been collected from the customer and verified at the time. As a result, SCA at times provided designated services in circumstances where it had not given full consideration to the ML/TF risk posed by potential high risk customers. This impacted SCA's ability to appropriately manage and mitigate the ML/TF risk related to those customers.

d. SCA's Standard Part B Programs did not include appropriate risk management systems to identify whether a customer was a PEP. This impacted SCA's ability to understand the ML/TF risks posed by PEPs and to effectively manage and mitigate the high ML/TF risks related to those customers.

e. SCA did not have adequate systems and controls to collect and analyse source of wealth and source of funds information. This impacted SCA's ability to fully understand the ML/TF risk posed by a customer to whom it provided designated services and to effectively manage and mitigate the ML/TF risk related to those high risk customers. For example, this failure impacted SCA's ability to identify unusual or suspicious transactions, such as unusually high turnover or losses.

f. The deficiencies with SCA's Standard Part B Programs persisted for a number of years and were systemic.

g. Deficiencies in KYC information inhibit the ability of law enforcement and AUSTRAC to trace money to its source. This, in turn, can inhibit law enforcement investigations, prosecutions and the recovery of proceeds of crime.

454 SCA has implemented changes to the operation of its Standard Part B Program as part of its AML EP. Amendments to SCA's Standard Part B Program are described further in Section H.8.

H.1.2 Section 36 of the Act – Ongoing customer due diligence

455 SCA contravened section 36 of the AML/CTF Act during the Relevant Period.

456 SCA failed to adequately monitor 56 Higher Risk Customers and 65 SCEG Channel Customers in contravention of section 36(1) of the AML/CTF Act. These contraventions were serious because:

a. SCA regularly dealt with high risk customers, including junket customers, international VIP customers and high rollers. The high ML/TF risk posed by these customer types were well-known and the subject of typologies and guidance published by relevant authorities, from time to time, including AUSTRAC.

b. SCA's failure to conduct appropriate OCDD for the 56 Higher Risk Customers and 65 SCEG Channel Customers was systemic and occurred over a number of years. This failure exposed SCA and the Australian community to risks of serious organised crime.

c. SCA's failure to conduct appropriate OCDD for the 56 Higher Risk Customers and 65 SCEG Channel Customers meant that SCA continued ongoing relationships with customers in circumstances where it did not have adequate regard to the ML/TF risk posed by those customers, or the consideration of the risk was delayed.

d. SCA provided designated services to 56 Higher Risk Customers at various times between 7 December 2016 and 26 October 2022. The 56 Higher Risk Customers had turnover of approximately $3.5 billion and generated an estimated gross revenue of approximately $45.7 million for SCA.

e. SCA was aware of information suggesting that 21 of the 56 Higher Risk Customers were connected to organised crime or that allegations of criminal conduct had been made against the customer or the customer had been charged, arrested, prosecuted, previously convicted or imprisoned in connection with offences, including in some cases dealing with the proceeds of crime and money laundering. In relation to three of the customers, SCA became aware of the information after it had provided the customer with its last designated service but prior to SCA formally banning the customer (see paragraph 409m).

f. Had SCA appropriately monitored its customers, it may have identified activity indicative of ML/TF typologies sooner. Had this activity been identified sooner, it could have been investigated and, where determined to be suspicious, reported to AUSTRAC and law enforcement sooner, through SMRs. Had suspicious activity been identified sooner, SCA would have been in a position to undertake additional steps to identify, mitigate and manage the ongoing risks.

457 In relation to 31 of the Higher Risk Customers that were escalated to senior management for consideration, insufficient regard was given by senior management to the higher ML/TF risk associated with those customers, including in relation to the customers' source of wealth and/or source of funds, the information known or obtained about the customer, and/or the customer's known risk profile, when determining whether business relationships with those customers ought to continue.

H.2 Loss and damage suffered

458 SCA operates in an industry known, internationally and within Australia, to pose high ML/TF risk. As a result of the contraventions set out at Sections F and G above, SCA provided designated services, including facilitating the movement of money into and out of the SCA casino, in the absence of having in place appropriate AML/CTF controls to adequately identify, manage and mitigate the ML/TF risk of providing these services. In providing these designated services, SCA facilitated the provision of designated services to the 56 Higher Risk Customers with turnover in the amount of approximately $3.5 billion from a total buy-in of approximately $436.1 million[80] and generated an estimated gross revenue of approximately $45.7 million for SCA.

[80] Refer to footnote 39.

459 By facilitating the movement of hundreds of millions of dollars a year across the Relevant Period, and turnover in the billions of dollars, without appropriate AML/CTF controls, SCA:

a. exposed its banking partners and other financial institutions in transaction chains to ML/TF risk;

b. exposed the Australian and global community and financial system to systemic ML/TF risk over many years, including where SCA was at risk of being exploited by organised crime;

c. was exposed to the risk of money laundering, in particular where adequate risk-based controls were not in place to enable SCA to understand the sources of money moving through high risk channels or whether there was a risk that money was illicit; and

d. facilitated the movement of significant amounts of money through high risk and non-transparent channels (see, for example, paragraphs 409f and 409g). Transactions through these channels had the potential to be indicative of ML/TF typologies or vulnerabilities.

460 As noted in paragraph 456c above, on and from 7 December 2016, SCA provided designated services to 56 Higher Risk Customers without carrying out adequate risk-based OCDD. In the absence of appropriate risk-based systems and controls to identify, mitigate and manage ML/TF risk, SCA continued in business relationships with these Higher Risk Customers where SCA did not have appropriate regard to the ML/TF risk posed by each customer, or the consideration of the risk was delayed.

461 As noted in paragraph 456b, a further 65 SCEG Channel Customers were permitted to transact between 12 December 2016 and 15 July 2022 in circumstances where SCA did not adequately monitor the customers' transactions. In total, AUD$29.16 million[81] was accessed for gaming by those customers once funds (as applicable) had been credited to their FMAs. Had SCA conducted appropriate risk-based customer due diligence, including appropriate risk-based transaction monitoring, the ML/TF risk posed by these customers could have been identified, mitigated and managed sooner.

462 In respect of the customers referred to in paragraph 456 above, as noted in that paragraph:

a. SCA's failures exposed SCA and the Australian community to ML/TF risk;

b. had SCA appropriately monitored these customers, it may have identified activity indicative of ML/TF typologies sooner;

c. had this activity been identified sooner, it could have been investigated and, where determined to be suspicious, reported to AUSTRAC and law enforcement sooner, through SMRs; and

d. had suspicious activity been identified sooner, SCA would have been in a position to undertake additional steps to better identify, mitigate and manage the ongoing risks of providing designated services to the customers.

463 Non-transparent movement of money and, as noted in paragraphs 449d and 453g above, deficiencies in KYC information may inhibit the ability of law enforcement and AUSTRAC to trace money to its source. This may inhibit law enforcement investigations, prosecutions and the recovery of proceeds of crime. Where money can be moved quickly and across borders, it can be even more difficult to trace and recover. These issues were compounded by SCA's

[81] This figure is the summation of the two different currencies (AUD and HKD). The parties have used the historical daily exchange rate provided by the Reserve Bank of Australia to calculate this conversion.

failures to ensure it had appropriate systems and controls to fully and accurately report SMRs, TTRs and IFTIs. SCA's conduct undermined the objectives of the AML/CTF Act.

464 The ML/TF management failures occurred in circumstances where SCA was operating a high turnover business. Between 7 December 2016 and 26 October 2022, SCA generated the revenue figures outlined in sub-paragraph 456d with respect to the 56 Higher Risk Customers.

465 By failing to comply with the AML/CTF Act and the AML/CTF Rules, SCA avoided expending funds that should have been invested in compliance including on IT, staffing and the development of AML/CTF controls. As noted in Section H.8, significant funds have now been invested in those areas.

466 The loss and harm caused by SCA's failings were significant for the reasons set out at paragraphs 458 to 465 above.

467 SCA's revenue and turnover from Higher Risk Customers who posed an elevated ML/TF risk were comparatively smaller than the revenue and turnover obtained from the high risk customers of Crown Melbourne and Crown Perth. Between 1 March 2016 and 1 March 2022, 60 high risk customers at Crown[82] had turnover in excess of $70 billion generating gross revenue to Crown of about $1.246 billion. Between 7 December 2016 and 22 October 2022, the 56 SCA Higher Risk Customers had a turnover of approximately $3.5 billion (ie, 5% of the turnover of Crown) resulting in estimated gross revenue to SCA of approximately $45.7 million (ie, 3.66% of the estimated gross revenue of Crown).

468 SCA's revenue from junkets was also significantly less than that earned by Crown Perth or Crown Melbourne. Between 1 March 2016 and 1 March 2022, Crown Melbourne generated $1,365 million in revenue from junkets, and Crown Perth's revenue from junket operations was approximately $320 million. Over the Relevant Period, SCA's revenue from junkets was approximately $26 million. Consequently, the broader risks to the Australian public and SCA's banking partners and other financial institutions resulting from SCA's conduct were, by comparison, less significant.

H.3 Prior contraventions

469 SCA has not previously been found to have engaged in any contravention of the AML/CTF Act or the AML/CTF Rules.

H.4 SCA and SCEG's size and financial position

470 Throughout the Relevant Period, SCA was incorporated in Australia and was a provider of designated services within the meaning of section 6 of the AML/CTF Act. At all material times, SCA held a casino licence under section 5 of the Casino Act and operated under the ALA. SCEG is the ultimate parent company of SCA and is dual listed on the Australian Stock Exchange and New Zealand Stock Exchange.

471 As a wholly owned subsidiary of SCEG, SCA's financial accounts are consolidated with SCEG (as its ultimate parent entity) and other companies within the SkyCity Entertainment Group of companies (**SCEG Group**).

472 The table below sets out the relevant reported financial results of SCA and the SCEG Group during the 2017 to 2023 financial years.[83]

---

[82] *Chief Executive Officer of the Australian Transaction Reports and Analysis Centre v Crown Melbourne Limited* [2023] FCA 782 at [160].

[83] FY2023 is outside the Relevant Period of these Proceedings.

$millions (AUD)	FY17	FY18	FY19	FY20	FY21	FY22	FY23
SCA							
Gaming revenue	$121.2	$146.7	$123.1	$100.6	$143.8	$135.1	$162.5
Non-gaming revenue	$21.9	$21.3	$19.8	$17.9	$33.9	$46.4	$63.1
Other Revenue	$0.1	$0.6	$0.2	$7.8	$15.4	$0.1	$2.8
Total Revenue	$143.2	$168.6	$143.1	$126.3	$193.2	$181.5	$228.4
EBITDA[84]	$11.6	$46.6	$21.9	-$57. 7	$32.3	$18.3	-$60.5
EBIT	-$4.0	$31.0	$6.6	-$74.5	$11.2	-$12.6	-$91.3
NPAT	-$7.1	$15.5	-$2.4	-$77.7	-$4.8	-$24.1	-$108.5
SCEG Group[85]							
Total Revenue	$877.8	$749.7	$772.3	$1,064.7	$887.9	$597.8	$847.3
EBITDA	$290.4	$284.9	$279.7	$329.6	$292.8	$90.7	$151.8
EBIT	$106.4	$210.6	$204.6	$247.7	$210.3	$2.1	$68.8
NPAT	$42.4	$155.8	$135.8	$222.8	$145.4	-$31.4	$7.3

473 As at the end of FY22 and FY23, SCA's net assets were negative AUD$17.1 million and negative AUD$125.6 million respectively and the SCEG Group had net assets of NZD$1.571 billion and NZD$1.530 billion respectively.

H.5 SCA's size and financial position compared to other casinos

474 With reference to casino revenues, SCA is relatively small compared to the casino market leaders in Australia. The below tables compare key financial metrics, at the individual casino level and the group-wide level, for SCA, Crown Perth and Crown Melbourne and the SCEG

[84] Earnings before interest, taxes, depreciation and amortisation.

[85] NZD figures in this table and the tables at paragraphs 476 and 479 have been converted to AUD using the average monthly historical data available from the Reserve Bank of Australia.

Group and the Crown Resorts Group (neither SCEG nor the Crown Resorts Group were alleged to have contravened the AML/CTF Act or AML/CTF Rules).

475 **Revenue (individual casinos)**[86]

Revenue $millions (AUD)	FY17	FY18	FY19	FY20	FY21	FY22
Crown Perth	$830.1	$839	$808.8	$607.5	$740.9	N/A
Crown Melbourne	$1,994.8	$2,217.5	$2,133.7	$1,580.9	$567.5	N/A
SCA	$155.8	$168.6	$143.1	$126.3	$193.2	$181.5
SCA % of Crown Perth	18.8%	20.1%	17.7%	20.8%	26.1%	N/A
SCA % of Crown Melbourne	7.8%	7.6%	6.7%	8%	34%	N/A

476 **Revenue (group-wide):**

Revenue $millions (AUD)	FY17	FY18	FY19	FY20	FY21	FY22
Crown Resorts Group	$3,345.2	$3,085.3	$2,929.2	$2,237.2	$1,536.8	N/A
SCEG Group	$877.8	$749.7	$772.3	$1064.7	$887.9	$597.8
SCEG Group % of Crown Resorts Group	26.2%	24.3%	26.4%	47.6%%	57.7%	N/A

477 **Revenue derived from junket operations:**

Casino	Period[87]	Revenue $millions (AUD)	SCA % of junket revenue against other Australian casinos
SCA	7 December 2016 to 12 April 2021	$26	N/A
Crown Perth	March 2016 to March 2022	$320	8.1%
Crown Melbourne	March 2016 to March 2022	$1,365	1.9%

[86] The revenue included in this table, with exception to FY17, relates to the total reported revenue (ie including gaming and non-gaming financials) for SCA, Crown Perth and Crown Melbourne as noted in its annual reports. For FY17, the table refers to the normalised/theoretical revenue for SCA, Crown Perth and Crown Melbourne as noted in its annual reports. The normalised/theoretical revenue has been used for FY17 only as for Crown Perth and Crown Melbourne there is no public information readily accessible for that period which separates reported revenue at the individual casino level. The table excludes the financial data for FY22 for Crown Perth and Crown Melbourne as there is no public information readily accessible for that period following the acquisition by Blackstone.

[87] Note: The period relates to the start of the relevant period in the respective AUSTRAC proceedings against SCA, Crown Perth and Crown Melbourne to the last date the respective entities provided designated services to a junket program.

478 **EBITDA (individual casinos):**[88]

EBITDA $millions (AUD)	FY17	FY18	FY19	FY20	FY21	FY22
Crown Perth	$257.3	$221.5	$244.6	$154.2	$231.8	N/A
Crown Melbourne	$570.6	$586	$615	$381.8	-$100.6	N/A
SCA	$11.6	$46.6	$21.9	-$57.7	$32.3	$18.3
SCA % of Crown Perth	4.5%	21%	9%	N/A[89]	13.9%	N/A
SCA % of Crown Melbourne	2%	8%	3.6%	N/A[90]	N/A[91]	N/A

479 **EBITDA[92] (group-wide):**

EBITDA $millions (AUD)	FY17	FY18	FY19	FY20	FY21	FY22
Crown Resorts Group	$790.3	$792.4	$849.7	$504.6	$114.1	N/A
SCEG Group	$290.4	$284.9	$279.7	$329.6	$292.8	$90.7
SCEG Group % of Crown Resorts Group	36.7%	36%	32.9%	65.3%	256.6%	N/A

480 The comparatively smaller size and scope of SCA's business operations against Crown Melbourne and Crown Perth means that both the number of contraventions and the revenue and turnover associated with those contraventions are commensurately lower. For example:

a. on average SCA's:

i. reported revenue was approximately 20.6%[93] the size of Crown Perth and approximately 9.3%[94] the size of Crown Melbourne; and

ii. reported EBITDA was approximately 4.9%[95] the size of Crown Perth and approximately 2.7%[96] the size of Crown Melbourne;

---

88 The EBITDA included in this table relates to the reported EBITDA (ie including gaming and non-gaming financials) for SCA, Crown Melbourne and Crown Perth as noted in its annual reports. The table excludes the financial data for FY22 for Crown Perth and Crown Melbourne as there is no public information readily accessible for that period following the acquisition by Blackstone.

89 As SCA's reported a negative EBITDA for FY20 a comparison of the size of SCA's EBITDA against Crown Perth's EBITDA for that financial year has not been provided.

90 As SCA's reported a negative EBITDA for FY20 a comparison of the size of SCA's EBITDA against Crown Melbourne's EBITDA for that financial year has not been provided.

91 As Crown Melbourne reported a negative EBITDA for FY21 a comparison of the size of SCA's EBITDA against Crown Melbourne's EBITDA for that financial year has not been provided.

92 The EBITDA included in the table below relates to the total reported EBITDA (ie including gaming and non-gaming financials) for the SCEG Group and Crown Resorts Group as noted in its annual reports. The table excludes the financial data for FY22 for Crown Resorts Group as there is no public information readily accessible for that period following the acquisition by Blackstone.

93 The average has been calculated using the reported revenue for Crown Perth and SCA across FY18 to FY21 and the normalised revenue for FY17.

94 The average has been calculated using the reported revenue for Crown Melbourne and SCA across FY18 to FY21 and the normalised revenue for FY17.

95 The average has been calculated using the reported EBITDA for Crown Perth and SCA across FY17 to FY21.

96 The average has been calculated using the reported EBITDA for Crown Melbourne and SCA across FY17 to FY21.

b. by way of comparison of the extent of the section 36 contraventions against each of the Crown Melbourne and Crown Perth and SCA:

   i. Crown Melbourne and Crown Perth collectively admitted to 546 contraventions of section 36 of the AML/CTF Act; and

   ii. SCA has admitted to 121 contraventions of section 36 of the AML/CTF Act; and

c. with respect to the section 81 contraventions against each of Crown Melbourne and Crown Perth, and SCA, in both cases the contraventions are too numerous to quantify. However, the comparative size between Crown Melbourne and Crown Perth and SCA means the number of contraventions by SCA are commensurately fewer.

481 See the discussion of SCA's revenue from junkets, relative to Crown Perth and Crown Melbourne, at paragraph 468 above.

H.6 Board and senior management involvement

482 The contraventions, as set out in this SAFA, were not a consequence of any deliberate intention to contravene the AML/CTF Act. At all times, the SCA Board and senior management sought to ensure that SCA would comply with its obligations under the AML/CTF Act.

483 SCA acknowledges that at all times during the Relevant Period the AML/CTF Act and AML/CTF Rules required that a reporting entity's Standard Part A program must be subject to the ongoing oversight of each reporting entity's board and senior management. As part of this oversight, SCA's Board and senior management were responsible for oversight of the management of ML/TF risks faced by its business in accordance with the AML/CTF Act and the AML/CTF Rules.

484 Between 7 December 2016 and 14 December 2022, as a result of the matters described at paragraphs 148 and 149, SCA did not comply with sections 84(2)(a) and 84(2)(c) of the AML/CTF Act and paragraph 8.4 of the AML/CTF Rules.

485 Since November 2021, SCA's Boards and senior management have overseen a range of measures directed at improving SCA's board governance and oversight of its AML/CTF Program, SCA's AML/CTF function and the identification, mitigation, and management of SCA's ML/TF risk, including the measures outlined in Section H.8. These improvements have been implemented to address, amongst other things, the shortcomings set out at paragraphs 148 and 149. The steps undertaken to date have demonstrated a commitment by SCA to uplift its AML/CTF compliance framework.

H.7 Cooperation with AUSTRAC and contrition

486 At all times during and since the Relevant Period, SCA has maintained a cooperative and constructive relationship with AUSTRAC, including cooperating fully with AUSTRAC's enforcement investigations, requests for information, and other requirements. SCA has shared information and reports with AUSTRAC concerning its compliance and programs of reform, including during various onsite visits by AUSTRAC both throughout and following the Relevant Period.

487 Prior to and during the Relevant Period, AUSTRAC undertook compliance assessments or reviews on three occasions, which focused on discrete parts of SCA's AML/CTF Programs. The purpose of the AUSTRAC compliance assessments is to assess compliance with specific obligations under the AML/CTF Act and/or the AML/CTF Rules. These were not audits by AUSTRAC nor were they a comprehensive statement of SCA's compliance with the AML/CTF Act or the AML/CTF Rules. As part of these assessments and reviews, AUSTRAC sought limited information from SCA. In 2019, AUSTRAC commenced a further

review of SCA's compliance, which led to a broader investigation and subsequently the Proceeding. SCA cooperated fully with AUSTRAC on each occasion that it conducted these compliance assessments and reviews.

488 SCA has also engaged constructively with AUSTRAC in relation to responding to the pleadings and particulars within its SOC. In particular, and in addition to the remediation, corrective measures and enhancements discussed in Section H.8, SCA has:

a. continued to work cooperatively with AUSTRAC on matters relating to AUSTRAC's ongoing supervisory role and in the conduct of the Proceeding; and

b. following the commencement of the Proceeding:

i. expressed contrition and its desire to work with AUSTRAC to resolve the Proceeding;

ii. communicated with AUSTRAC in relation to the mediation and participated in the mediation process; and

iii. admitted to contraventions of the relevant sections of the AML/CTF Act (sections 36 and 81) at an early stage.

489 SCA otherwise:

a. acknowledges that ML/TF undermines the integrity of the Australian financial system and impacts the Australian community's safety and wellbeing;

b. acknowledges that it, as a casino offering designated services, plays a key role in combating ML/TF and safeguarding the community against ML/TF risk;

c. accepts its accountability for the admitted contraventions, and expresses deep regret for those contraventions; and

d. acknowledges the significant impact that deficiencies in its systems and processes can have on efforts to combat ML/TF.

490 To demonstrate SCA's commitment to and leadership in ML/TF risk management, and in addition to the matters set out in Section H.8 below, SCA has taken steps to uplift its relationships with law enforcement agencies and remediate its AML/CTF compliance. Examples of some steps taken by SCA include:

a. in April 2022, appointing a dedicated role within its business that is responsible for engaging with law enforcement agencies regarding matters relevant to ML/TF risk management;

b. being a member of the Australia/NZ Financial Crime Gambling Industry Forum, comprising key casino and gambling organisations. The purpose of the Forum is to drive industry engagement on ML/TF risk management, and other financial crime risks, as well as to facilitate a consistent industry; and

c. participating in the Fintel Alliance Casino Working Group aimed at identifying and responding to the ML/TF risk within casinos. The Working Group brings together financial crime leads from law enforcement, AUSTRAC and other government agencies with representatives of Australian casinos.

H.8 Remediation, corrective measures and enhancements

491 From July 2021, SCA took steps to complete a review of the adequacy and effectiveness of its AML/CTF function and AML/CTF Program and recommend any changes. The completion of this review resulted in the development of SCA's AML EP. SCA has regularly briefed AUSTRAC on its program of reform and enhancement, including through periodic progress briefings and the provision of key documents such as:

a. SCA's risk assessments for its November 2022 Program;

b. the outcomes and SCA's response to internal reviews considering its AML/CTF controls; and

c. the approved standards and SOPs underpinning the November 2022 Program.

492 The briefings that have been provided to AUSTRAC are summarised below and divided into the following categories:

a. internal and external reviews in response to the AUSTRAC enforcement investigation;

b. AML EP;

c. enhancements to risk-based systems and controls; and

d. enhancements to governance, oversight, resourcing and training.

493 As is common with remediation of this scale, the process is ongoing. For this reason, as at the date of this SAFA, AUSTRAC has not yet been in a position to conduct a comprehensive assessment of SCA's remediation or its effectiveness. However, the steps taken to date have shown SCA's commitment to uplifting its AML/CTF Program.

H.8.1 Internal and external reviews

494 In March 2020, SCA engaged an external consulting firm to conduct an independent review of SCA's AML/CTF Program in purported compliance with paragraph 8.6 of the AML/CTF Rules. Due to delays associated with COVID-19, the report was finalised on 6 August 2021 and covered the period from August 2018 (the date of completion of the previous independent review performed in purported compliance with paragraph 8.6 of the AML/CTF Rules) to 28 February 2021 (**August 2021 Report**).

495 The August 2021 Report identified several areas warranting further consideration by SCA, namely, AML/CTF training, ECDD, risk assessment, IFTI reporting, employee due diligence and OCDD. The AML EP included workstreams to respond to the matters raised in the August 2021 Report.

496 In response to the commencement of AUSTRAC's enforcement investigation and the concerns raised by AUSTRAC with respect to SCA's compliance with its obligations arising under the AML/CTF Act and the AML/CTF Rules, SCA commenced an internal review of its AML/CTF function. This review was conducted in parallel with formally retaining an external consulting firm on 8 July 2021 to:

a. review and advise SCA on the adequacy and effectiveness of SCA's AML/CTF function and AML/CTF Program, having regard to the requirements of the AML/CTF Act and AML/CTF Rules; and

b. recommend to SCA any changes to SCA's AML/CTF function and AML/CTF Program.

497 On 9 September 2021, the external consulting firm finalised its AML/CTF Compliance Review Report (**September 2021 Report**). The September 2021 Report identified a range of matters for SCA to consider and address to enhance its AML/CTF function and to address concerns raised by AUSTRAC through the enforcement investigation.

H.8.2 AML Enhancement Programme

498 Following receipt of the September 2021 Report and, having regard to the outcomes of the internal review, SCA's AML/CTF team, working with the external consulting firm that created the September 2021 Report, took steps to complete a comprehensive review of its AML/CTF function. This program, known as the AML EP is a management led reform program with SCA Board oversight, which was a roadmap for the proposed enhancements/improvements to be made to SCA's AML/CTF Programs. The AML EP was finalised and submitted to the SCA Board for approval in November 2021.

499 The AML EP set out six initiatives relating to AML governance, AML risk assessments, AML diagnostics and assurance, AML framework hierarchy (documentation), AML systems and people and culture and included a detailed timeline for delivery of the key milestones and deliverables for each of the six initiatives to enhance SCA's AML/CTF function. The AML EP was designed to lift the maturity of the SCA AML/CTF Program and broader AML/CTF function across certain key areas.

500 The issues identified in the August 2021 Report were considered by SCA in conjunction with the issues identified in the September 2021 Report. The issues raised in the August 2021 Report also informed the work undertaken as part of the AML EP.

501 SCA has made investments in developing its AML EP since November 2021. SCA's investment has assisted it responding to the matters raised in the August 2021 Report, the September 2021 Report and the 2022 Report (as described at paragraph 509 below).

502 Through the AML EP, SCA has taken steps to uplift its AML/CTF Program, processes, systems and people to address identified compliance concerns. The AML EP led to the SCA Board and senior management approving and implementing the November 2022 Program which includes updated Standard Part A and Standard Part B Programs that were based on feedback provided by the external consulting firm who issued the September 2021 Report and sought to respond to the deficiencies identified in the Proceeding.

H.8.3 Enhancements to risk-based systems and controls

Risk assessments

503 SCA engaged the external consulting firm that issued the September 2021 Report to prepare a new ML/TF risk assessment. As set out at paragraphs 121 to 122, in May 2022, SCA introduced the 2022 ML/TF Risk Assessment Methodology and the 2022 Risk Assessments which provide a framework to identify and assess the ML/TF risk reasonably faced by SCA.

504 Following the completion of the 2022 Risk Assessments, SCA redesigned its AML/CTF Program to align with the ML/TF risk identified. This included the design of a range of new SOPs to support revised risk-based systems and controls. The SOPs provided practical guidance on the processes and procedures to implement the new risk-based systems and controls. A revised Standard Part A Program was adopted in November 2022 and all supporting Standards were approved and implemented in December 2022. A revised Standard Part B Program was approved and adopted in June 2023. Additional supporting Standards for the Standard Part B Program were adopted in August 2023.

TMP

505 Since December 2022, SCA has taken steps to uplift its risk-based systems and controls with respect to its TMP. For example, in or around early 2023, SCA undertook an end-to-end review of its TMP and associated systems. As a result of that review, SCA implemented restrictions on cash amounts that a customer can transact with in a single day, being not more than $5,000, and implemented new Jade system alerts. SCA also introduced three new SOPs from May 2023 to provide practical guidance for its TMP.

ECDD

506 Since December 2022, SCA has taken steps to uplift its risk-based systems and controls with respect to its ECDD Program. This includes two SOPs introduced from May 2023 to provide guidance to SCA's Financial Crime Analysts regarding the ECDD process.

Reporting obligations

507 In November 2020, SCA implemented an automatic extraction process for IFTIs, with the intention of limiting the risk of human error and ensuring IFTIs were reported within the required 10 day period.

508 Since October 2021, SCA has taken steps to uplift its systems and controls with respect to the reporting of SMRs, including undertaking an end-to-end review of its SMR reporting, updating its SMR reporting forms and implementing SMR guidelines for SCA's Financial Crime team to use to assist with identifying and reporting suspicious matters.

509 On 16 March 2022, SCA engaged an external consulting firm to undertake an end-to-end review of its processes for IFTI and TTR reporting to identify risks, inefficiencies or issues. This was in response to two of the recommendations set out in the September 2021 Report. The external consulting firm provided a final draft report to SCA on 5 September 2022 (**2022 Report**).

510 The 2022 Report identified four key 'control gaps' with respect to IFTIs as well as TTRs, but overall, found that "*the sample-based review has not identified any instances where SCA has missed an IFTI or TTR."* The 2022 Report identified 16 observations, grouped into six observation themes, predominantly relating to deficiencies in the systems and processes supporting TTR and IFTI reporting.

511 The six observation themes were mapped to ten specific recommendations to enhance SCA's ITFI and TTR processes. The recommendations in the 2022 Report informed the remediation work undertaken as part of the AML EP workstreams.

512 On 12 May 2023, SCA implemented a 'Financial Crime – Periodic Sample Testing for IFTIs and TTRs for compliance with standards held by AUSTRAC' SOP to address the sample testing requirements as specified by section 11 of the November 2022 Program.

H.8.4 Enhancements to governance, oversight, resourcing and training

Governance and Oversight

513 Through the AML EP, SCA has taken steps to enhance the oversight of its AML/CTF obligations by the SCA Board and senior management. For example, SCA has:

a. formally established the AMLCO as the point of contact between frontline SCA staff who raise AML compliance issues, and the SCA Board and AML/CTF Committee;

b. established clearer processes for the escalation of issues relating to the Standard Part A Program or other relevant AML/CTF matters to the AML/CTF Committee, and,

where appropriate, the SCA Board, to ensure that relevant and adequate information is being provided to allow and facilitate the assessment of ML/TF risk and development of mitigation strategies;

c. created a requirement that input is obtained from relevant stakeholders in preparing the reports that are provided to the SCA Board. SCA has identified that these key stakeholders will typically include the Financial Crime Management team, the AML Enhancement Programme Director and the SCA Board Company Secretary; and

d. taken steps to ensure that appropriate responsibilities have been assigned to the resources who are responsible for assisting SCA with discharging its AML/CTF obligations.

Resourcing

514 In June 2021, the 'AUSTRAC Enforcement Investigation Steering Committee' (**AUSTRAC Steerco**) was established, consisting of members of SCA's and SCEG's Senior Leadership Team. The external consulting firm that issued the September 2021 Report also spoke to the AUSTRAC Steerco in relation to the recommendations to be made in that report, identifying the initial areas for remediation efforts.

515 In September 2021, the AUSTRAC Enforcement Investigation Steering Committee was renamed the 'AML Enhancement Programme Steering Committee' (**AML EP Committee**) to reflect the redefined focus of the Committee on overseeing the implementation of the AML EP. Amongst other functions, the AML EP Committee focused on developing a proactive response to AUSTRAC's concerns in relation to SCA's AML/CTF compliance. In doing so, the AML EP Committee oversaw recruitment processes for the additional roles created in SCA's AML team, and liaised with external advisors to address AML compliance concerns and to develop remediation plans.

516 In October 2021, SCA filled the newly created role of 'General Manager AML & CTF – Adelaide' (**GM AML/CTF**). The GM AML/CTF was responsible for implementing the AML EP, amongst other things.

517 SCA has also significantly increased its funding for its AML department (which is in addition to its investment for the AML EP). In particular, SCA has recently invested $1.42 million in FY23 and a further $2.66 million in costs for FY24 (comprising actual costs to 30 April 2024 and forecast costs for the remainder of FY24). This investment has seen SCA's resourcing for financial crime and legal and compliance increase from four fulltime employees at the inception of the AML EP to 24 fulltime employees as follows:

a. 14 full-time employees in the Financial Crime department;

b. four full-time employees in the Customer Compliance team, which is a dedicated resource for CDD;

c. two full-time employees in the Legal and Compliance team; and

d. four dedicated full-time employees for the AML EP, who are also responsible for the continued upfit of SCA's AML/CTF Program.

Training

518 In response to the September 2021 Report, SCA uplifted its AML/CTF Program by implementing the following mandatory training:

a. AML/CTF risk awareness training, with the level of training provided dependent on the nature of the employee's role and exposure to ML/TF risk;

b. all staff employed were required to undertake AML/CTF refresher training annually; and

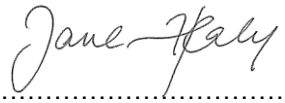
c. AML/CTF training was to be completed within a certain time frame from induction.

519 In December 2021, SCA Directors, SCA's Senior Leadership Team and the SCEG Group's Senior Leadership Team participated in AML training sessions and by December 2021, AML risk assessment training had been delivered to relevant areas of the business in Adelaide. Since December 2021, AML training has been provided by way of e-training modules.

H.9 Other facts relevant to deterrence

520 SCA is currently the subject of an investigation under section 22(2) of the Casino Act. The investigation concerns the suitability of SCA to continue to hold a casino licence under the Casino Act and the suitability of SCEG to continue to be a close associate of SCA (**Independent Inquiry**). The Independent Inquiry is currently adjourned pending resolution of the Proceeding. However, on 29 May 2023, the South Australian Commissioner for Liquor and Gambling directed SCA, pursuant to section 10 of the *Gambling Administration Act 2019* (SA), to establish a comprehensive program of work to ensure SCA was meeting its AML/CTF and gambling harm minimisation obligations. On 25 August 2023, the Commissioner approved the appointment of consultancy firm, Kroll Australia Pty Ltd (**Kroll**), as the Independent Monitor to review SCA's AML/CTF Program and host responsibility enhancement programmes and, if required, make amendments to those enhancement programmes; monitor the implementation of those enhancement programmes by SCA and SCA's compliance with its AML/CTF and gambling harm minimisation obligations; and report to the Commissioner in relation to such matters. As at 30 April 2024, the Independent Inquiry (including the appointment of Kroll) has cost SCA approximately $5 million, with a further $764,000 forecasted to 30 June 2024.

Date: 17 May 2024



……..

Jane Healy

AGS Lawyer

For and on behalf of the Australian Government Solicitor

Lawyer for the Applicant

……..

Richard Harris

Solicitor for the Respondent

SCHEDULE 1 – ML/TF VULNERABILITIES AND TYPOLOGIES

A. Structuring

1 Structuring is the deliberate division of a large amount of cash into smaller deposits to avoid the reporting threshold in section 43 of the AML/CTF Act. Section 43 of the AML/CTF requires a reporting entity to give the AUSTRAC CEO a report of a transaction in circumstances where a reporting entity provides (or commences to provide) a designated service to a customer and the provision of the service involves a threshold transaction. A threshold transaction is defined under section 5 of the AML/CTF Act as meaning a transaction involving the transfer of physical currency, where the total amount transferred is not less than $10,000.

B. Cuckoo smurfing/smurfs

2 Cuckoo smurfing is a method of money laundering used by criminals to move funds across borders and make money generated by their illegal activities appear to have come from a legitimate source. Cuckoo smurfing is facilitated by professional money laundering syndicates who work with a corrupt remitter based overseas, as follows:

(a) the corrupt remitter accepts an instruction from a customer to make a payment to an Australian-based beneficiary customer;

(b) the corrupt remitter hijacks the money transfer to the Australian-based beneficiary by replacing the funds the subject of that transfer with (different) funds which are sourced from criminal activity;

(c) a smurf or third party agent deposits cash into Australian bank accounts on behalf of a money laundering syndicate controller; and

(d) the international transfer is offset without the physical movement of funds.

3 A 'smurf' or a 'third party agent' is an individual conducting cash deposits into Australian bank accounts on behalf of a money laundering syndicate controller. Junket operators may act as remitters and may facilitate cuckoo smurfing.

C. Offsetting

4 Offsetting enables an international transfer of value to occur without actually transferring money. This is possible because the arrangement involves a financial credit and debit (offsetting) relationship between two or more persons operating 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.

D. Loans or credit

5 Loans or credit can 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.

E. Third parties

6 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.

F. Minimal or no gaming activity

7 Money deposited with a casino or exchanged for CVIs (including chips and tickets) and then withdrawn with minimal or no gaming activity may indicate ML/TF activity, despite the money

appearing to have a legitimate origin. Little money is risked in this scenario. Gaming losses sustained by a customer, even if minimal, can give the incorrect appearance that the customer is engaging in genuine gaming activity.

G. High turnover or high losses

8 Gaming 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.

9 Gaming 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.

10 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 is 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.

H. Specific casino games

11 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 describes the mathematical advantage that a game, and therefore the casino, has over the customer with play over time.

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

13 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.

I. Misuse of CVIs

14 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. Individuals may also purchase CVIs from other customers using illegitimate funds and winnings, which are subsequently claimed from the Cage.

J. Bank cheques

15 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.

K. Bill stuffing

16 Bill stuffing involves a customer putting cash into an electronic gaming machine, collecting tickets with nominal gaming activity and then cashing out or asking for a cheque.

L. Refining

17 Refining can be indicative of ML/TF activity. Refining involves changing an amount of money from smaller denomination bills into larger denomination bills.

M. Loan sharking

18 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.

N. Parking

19 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 funds outside the banking system and to hide funds from law enforcement and relevant authorities.

O. Chip Dumping/ intentional losses

20 Chip dumping describes the act of intentionally losing money to another player at a table game, to facilitate a transfer of money between the players.

P. Even Money Betting

21 Even money betting involves two or more customers placing opposite equal bets on even money wagers in the same game. The customer with the winning bet is then able to cash out the funds as winnings. This is also known as ‘parallel betting’.

Appendix A

Customer Number (Column A)	Date on which the customer first became a customer of SCA (Column B)	Date of last designated service provided to the customer by SCA (Column C)	Date of ban (Column D)[97]
Customer 1	14 June 2016	7 October 2020	22 March 2022
Customer 2	2 July 2015	10 March 2021	9 August 2021
Customer 3	13 December 2013	12 July 2017	23 March 2022
Customer 4	7 August 2015	24 February 2017	23 March 2022
Customer 5	6 August 2017	16 April 2021	22 March 2022
Customer 6	11 March 2019	2 March 2021	29 March 2022
Customer 7	29 July 2015	17 March 2020	22 March 2022
Customer 8	28 December 2018	11 June 2019	31 March 2022
Customer 9	24 August 2017	28 August 2017	22 March 2022
Customer 10	21 December 2013	29 June 2021	29 March 2022
Customer 11	16 March 2015	13 November 2018	22 March 2022
Customer 12	1 July 2012	24 July 2017	4 September 2020 (s 44 barring, expiring 5 September 2025)
Customer 13	15 October 2016	13 July 2019	22 March 2022
Customer 14	25 August 2017	17 December 2018	30 September 2020 (s 44 barring)
Customer 15	27 September 2016	26 April 2018	22 March 2022
Customer 16	22 July 1999	23 August 2018	22 November 2019 (s 125 barring for indefinite period)
Customer 17	2 June 2014	18 August 2021	9 August 2021
Customer 20	27 June 2015	27 July 2019	9 December 2022
Customer 21	15 June 2015	31 March 2021	22 March 2022
Customer 22	7 January 2016	12 September 2022	As at 28 October 2022, Customer 22 remained a customer of SCA and had not been banned.
Customer 23	12 April 2014	19 April 2021	1 June 2022
Customer 24	10 November 2012	21 December 2021	2 February 2022
Customer 25	12 March 2017	11 October 2021	29 March 2022
Customer 27	22 April 1994	19 July 2021	30 July 2021
Customer 28	27 April 2013	20 September 2019	9 August 2021
Customer 29	28 October 2007	25 March 2021	31 March 2021
Customer 30	7 September 2004	6 August 2021	9 August 2021
Customer 31	5 June 2001	9 August 2021	9 August 2021
Customer 32	17 June 2005	9 August 2021	9 August 2021
Customer 33	10 December 2002	6 August 2021	9 August 2021
Customer 34	13 July 2010	13 March 2020	22 March 2022
Customer 35	19 August 2009	19 March 2021	24 August 2021
Customer 36	15 July 2019	6 August 2021	9 August 2021

[97] Unless made evident otherwise, a reference to a barring date in this column is a reference to a barring pursuant to section 27AA of the Casino Act. Where known, the barring date is the start date of the most recent barring relating to the customer.

Customer Number (Column A)	Date on which the customer first became a customer of SCA (Column B)	Date of last designated service provided to the customer by SCA (Column C)	Date of ban (Column D)[97]
Customer 37	6 September 1999	7 August 2021	29 March 2022
Customer 38	25 September 2003	5 December 2019	9 August 2021
Customer 39	9 July 2014	17 November 2019	12 December 2022
Customer 40	3 January 2018	25 November 2021	26 November 2021
Customer 41	30 July 2018	9 October 2021	9 December 2021
Customer 42	21 February 2016	3 October 2022	8 October 2022
Customer 43	5 February 2014	26 October 2022	13 December 2022
Customer 44	18 March 2017	14 January 2020	29 March 2022
Customer 45	10 October 2017	26 July 2018	18 July 2019
Customer 46	19 June 2015	10 May 2021	29 March 2022
Customer 47	16 July 2011	6 January 2022	1 June 2022
Customer 48	6 May 2004	3 August 2021	9 August 2021
Customer 49	19 June 2012	3 December 2021	27 January 2022
Customer 50	1 June 2016	4 March 2020	10 May 2022
Customer 51	17 May 2018	6 April 2021	17 December 2021
Customer 52	6 February 2014	17 May 2022	31 May 2022
Customer 53	15 December 2000	12 August 2021	8 September 2021
Customer 54	3 October 2005	9 August 2021	9 August 2021
Customer 55	16 January 2019	29 June 2021	23 March 2022
Customer 56	22 December 2015	31 October 2019	29 March 2022
Customer 57	17 March 2007	2 July 2021	8 September 2021
Customer 58	10 April 2017	11 June 2021	16 June 2021
Customer 59	10 February 2011	26 July 2018	22 October 2021

Appendix B

Customer Number
Customer 60
Customer 61
Customer 62
Customer 63
Customer 64
Customer 65
Customer 66
Customer 67
Customer 68
Customer 69
Customer 70
Customer 71
Customer 72
Customer 73
Customer 74
Customer 75
Customer 76
Customer 77
Customer 78
Customer 79
Customer 80
Customer 81
Customer 82
Customer 83
Customer 84
Customer 85
Customer 86
Customer 87
Customer 88
Customer 89
Customer 90
Customer 91
Customer 92
Customer 93
Customer 94
Customer 95
Customer 96
Customer 97
Customer 98
Customer 99
Customer 100
Customer 101
Customer 102
Customer 103
Customer 104
Customer 105
Customer 106
Customer 107

Customer 108
Customer 109
Customer 110
Customer 111
Customer 112
Customer 113
Customer 114
Customer 115
Customer 116
Customer 117
Customer 118
Customer 119
Customer 120
Customer 121
Customer 122
Customer 123
Customer 124
Customer 125