AUSTRAC

Typologies and Case Studies Report 2007

Australian Government
Australian Transaction Reports and Analysis Centre

Acknowledgement: The valuable contribution of reporting entities, AUSTRAC's designated agencies, the Financial Action Task Force (FATF), Asia/Pacific Group on Money Laundering (APG) and Egmont Group of Financial Intelligence Units in producing this document is acknowledged.

Foreword

The AUSTRAC *Typologies and Case Studies Report 2007* is a key publication aimed at assisting you in complying with the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (the AML/CTF Act).

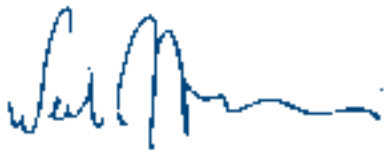
This report gives you an inside perspective into current money laundering and terrorism financing typologies, methodologies, and indicators. It has been specifically designed to help you better understand the potential risks your business faces.

The AML/CTF Act has given AUSTRAC an expanded role as Australia's AML/CTF regulator. In this role, AUSTRAC is tasked with ensuring compliance with the AML/CTF Act, Regulations and Rules.

This report is part of a raft of tools created by AUSTRAC to assist you in complying with the AML/CTF Act. These include AML/CTF Rules and guidance notes, the AUSTRAC Regulatory Guide, regulatory policies and a self assessment questionnaire to help you to understand, self-assess and monitor your compliance progress.

AUSTRAC recognises the responsibility we have in providing current and well informed guidance and feedback to you. This responsibility is reflected within AUSTRAC's *2007–2010 Business Strategy* as a core agency priority.

Thank you to our Australian and international partners who have assisted us in preparing this report.



Neil J Jensen PSM
Chief Executive Officer, AUSTRAC

Contents

Foreword		1
Glossary of terms		4
Introduction		**5**
1	Preamble	5
2	Methodology	6
3	Designated service case index	7
4	Money laundering methodologies	8
5	Indicators	10
Case studies		**13**
Case 1	Structuring of cash transactions to launder money	13
Case 2	Depositing altered cheques to undertake fraud	14
Case 3	Bonds used in cold calling of bank drafts scam	15
Case 4	Laundering the proceeds of internet banking theft	16
Case 5	Multiple purchases of banks' drafts used to launder funds	17
Case 6	Drug proceeds concealed by third parties	18
Case 7	Debit cards used in laundering process	19
Case 8	Scented cash implicates drug offenders	20
Case 9	Drug network undertakes multiple structured wire transfers	21
Case 10	Third parties used to send bank drafts offshore	22
Case 11	Company directors generate false receipts to evade tax	23
Case 12	Multiple pre-paid cards used to withdraw funds offshore	24
Case 13	Broker used to facilitate money laundering	25
Case 14	Stockbroker used to assist drug dealing client	26
Case 15	Fraud money invested in securities market	27
Case 16	Cash couriers used to launder funds	28
Case 17	Businessman defrauds Commonwealth and sends funds offshore	29
Case 18	'Nightclubbers' used to send funds offshore	30
Case 19	Wire transfers used as primary source of funding drugs	31
Case 20	Wire transfers and e-gold payments used to purchase stolen bank details	32
Case 21	Drug proceeds converted into casino chips by third parties	33
Case 22	The use of life insurance single premium policies	34

Case 23	Early surrender of life insurance policy to evade creditors	35
Case 24	Life insurance as a cover for tax fraud	36
Case 25	Money launderers use the insurance industry to clean their funds	37
Case 26	Criminal funds laundered through payment of insurance premiums	38
Case 27	Drug trafficker launders funds through purchase of life insurance policy	39
Case 28	Understated income siphoned to overseas bank accounts	40
Case 29	Smuggling of gold to evade tax	41
Case 30	Retail gold purchases serves as direct method of laundering	42
Case 31	Purchasing and reselling of precious metals and jewellery for settling of illegal alternative remittance payments	43
Case 32	Gold suppliers implicated in drug proceeds	44
Case 33	Currency exchange business used to launder funds	45
Case 34	E-gold account used to facilitate internet fraud	46
Case 35	Stored value cards sent offshore to withdraw crime proceeds	47
Case 36	Bank drafts purchased in third party names to evade tax	48
Case 37	Syndicate travels to offload drug proceeds through money exchange	50
Case 38	CEO assists in structuring of traveller's cheques	51
Case 39	Financial adviser involved in drug distribution network	52
Case 40	Overseas nationals purchase winning jackpots with illegal proceeds	53
Case 41	Casino used as preferred method to launder millions	54
Case 42	Bank employee gambles millions from clients' accounts	55
Case 43	Proceeds of drugs used to purchase chips and claim funds as winnings	56
Case 44	Criminal attempts to launder fraud proceeds through the diamond market	57
Case 45	Financial controller launders funds through bookmaker	58
Case 46	Drug proceeds used to repay finance loans	60
Case 47	Solicitor coordinates u-turn transactions to legitimise funds	62
Case 48	Structured bank drafts to purchase property	63
Case 49	Gatekeepers used in web of criminal activity	64
Case 50	Layering funds to evade tax	66
Case 51	Phantom vessel insured to launder funds	67
Appendix		**68**

Glossary of terms

AML/CTF Act	Anti-Money Laundering and Counter-Terrorism Financing Act 2006
AUD	Australian dollars
BNI	Bearer Negotiable Instrument
DPP	Director of Public Prosecutions
FIU	financial intelligence unit
FTR Act	Financial Transaction Reports Act 1988
ID	identification
IFTI	international funds transfer instruction
MDMA	methylenedioxymethamphetamine (ecstasy)
PAYG	Pay As You Go
SMR	Suspicious Matter Report
SUSTR	Suspicious Transaction Report
USD	United States of America dollars

Introduction

1 Preamble

The *Financial Transaction Reports Act 1988* (FTR Act) provided AUSTRAC with a mandate to provide financial intelligence to assist law enforcement, revenue and national security agencies within Australia. The FTR Act also provided AUSTRAC with the functions of oversight, education and compliance of 'cash dealers' who had obligations under the legislation.

Reforms commenced in Australia in the aftermath of events such as September 11, 2001 and October 12, 2002 (first Bali bombing) along with the growing global awareness of the impact of money laundering and terrorism financing. The reform process led to the enactment of the *Anti-Money Laundering and Counter-Terrorism Financing Act* 2006 (AML/CTF Act) on December 12, 2006. The objects of the AML/CTF Act strongly focus on Australia's commitment to fulfil its international obligations to combat money laundering and terrorism financing. The AML/CTF Act has expanded AUSTRAC's mandate and placed increased obligations on current and new 'reporting entities'.

The AML/CTF Act differs from the FTR Act in its adoption of a risk-based approach by reporting entities. Reporting entities are required to develop an AML/CTF Program with the aim to identify, mitigate, and manage risks the reporting entity may face, that involve or facilitate money laundering and terrorism financing.

A further key objective of the FTR Act and the AML/CTF Act is the reporting of certain financial transactions. The greater the quality, accuracy, and timeliness of reports, the greater the value they become to the detection, deterrence, and disruption of criminal and terrorist activity. The most unique and potentially valuable report is the Suspect Transaction Report (SUSTR) under the FTR Act or Suspicious Matter Report (SMR) under the AML/CTF Act. A robust regime of reporting high quality, relevant suspect financial activity is of major benefit to AUSTRAC's financial intelligence unit's (FIU) role and the work of Australian law enforcement, revenue and national security agencies.

In both of these endeavours, AUSTRAC recognises the critical responsibility it has to provide current and well informed guidance and feedback; a responsibility that is highlighted within AUSTRAC's *2007 – 2010 Business Strategy* as a core agency priority. The AUSTRAC *Typologies and Case Studies Report 2007* and similar reports to be produced by AUSTRAC on an ongoing basis form one component of this strategy.

2 Methodology

This report was generated from the following research material:

- sanitised case material from Australian law enforcement, revenue and national security agencies
- existing AUSTRAC strategic and typology research
- international typology and case study reports including Financial Action Task Force (FATF), Asia/Pacific Group on Money Laundering (APG) and Egmont Group of Financial Intelligence Units
- open source research.

The report initially identifies some key methodologies and indicators in operation within the Australian environment. Evidence of these methodologies and indicators are then expressly demonstrated through actual investigations that have been sanitised for use by AUSTRAC. The majority of case studies have assisted or been instrumental to identifying major crime and money laundering.

It is important to note that this cross-section is limited only to case study examples that have been approved for use in the public forum. AUSTRAC continues to work with law enforcement, revenue and national security agencies to obtain further examples of money laundering and terrorism financing activity for external use. Hence, this report is not an exhaustive list of methods being used to facilitate money laundering and/or the financing of terrorism in Australia.

To provide valuable information in the context of AML/CTF risk each case study has been deconstructed to highlight areas of relevant risk categorisation. The categories are as follows:

- Offence – The crime or civil proceeding involved within each case (not the actual charges laid)
- Customer – The type of customer/s that was/were involved in perpetration of the offence/s (either individual, business, foreign entity)
- Industry – The industry category through which transactional activity was conducted (in some cases multiple industries have been affected)
- Channel – The specific method through which the offenders conducted transactional activity (predominantly either in person or via electronic means or through an intermediary)
- Jurisdiction – The location (whether domestic or overseas) in which the money laundering or transactional activity was facilitated (case text may also include nominated country information where available)
- Designated service[1] – The specific Designated service category, that has been used to enable the commission of the offence
- Indicators – The red flag activity contained within each case example.

[1] For the purposes of this report, designated services under Section 6 of the AML/CTF Act have been grouped by AUSTRAC into 20 categories containing like activities. This provides more effective analysis and cross reference.

3 Designated service case index

The following table provides a reference to case studies outlined in this report that involve AML/CTF Act designated services. A person provides designated services when they provide one or more of the services listed in section 6 of the AML/CTF Act. As indicated, AUSTRAC has grouped like services for ease of use and analysis. Some of these services may have few or no case examples linked to them as they were not previously reportable transactions under the FTR Act. Case examples highlighting the misuse of designated service categories may also be pending approval for publication. Further evaluation of case materials in Australia and from overseas is being conducted to provide case studies where there are limited or no cases at this time.

Designated service categories	AML/CTF Act Section 6 – Item numbers	Case study number
Accounts	1-3	1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 15, 18, 19, 20, 22, 24, 26, 27, 28, 29, 31, 33, 34, 35, 41, 42, 44, 45, 46, 47, 49, 50
Money on deposit	4, 5	8, 40
Loan services	6, 7, 48, 49	36, 39, 46
Debt instruments	8, 9, 17, 34, 36	3, 5, 10, 36, 37, 42, 48
Leasing service	10-13	
Accounts – chequebook facility	14, 15	2, 14, 22, 27, 40, 46, 48, 49, 50, 51
Trust accounts - chequebook facility	16	
Accounts – debit card facility	18, 18A, 19, 19A	7
Trust accounts – debit card facility	20, 20A	
Payment orders and stored value cards	21-24, 27, 28	7, 12, 34, 35
Electronic funds transfer	29, 30	3, 4, 6, 9, 11, 13, 15, 16, 17, 18, 19, 20, 26, 28, 29, 36, 44, 45, 47, 49, 50, 51
Designated remittance arrangement	31, 32	4, 16, 17, 18, 20, 21, 31
Deals in securities markets	33, 35	13,14,15
Insurance and superannuation services	37-45	22, 23, 24, 25, 26, 27, 28
Custodial or depository service	46, 47	6
Foreign exchange services	25, 26, 50	18, 30, 33, 37, 38
Cash carrying and payroll services	51-53	28, 32, 37, 47
Australian financial services license	54	39
Bullion trading	Table 2 (1, 2)	28, 29, 30, 31, 32, 44
Gambling services	Table 3 (1-14)	21, 40, 41, 43, 45, 49

4 Money laundering methodologies

This section details the most common money laundering (ML) methodologies in Australia and overseas. These methodologies have been identified by AUSTRAC, and its partner agencies as having been utilised, or having the potential to be utilised within Australia, and overseas, to facilitate ML, and/or the concealment of funds.

False and fraudulent identification

The use of false and fraudulent names, and proof of identity documentation is considered a significant, and recurring vulnerability that contributes to the facilitation of criminal activity including ML and terrorist activities. Through the use of a false name and account, persons of interest/suspect persons can shift funds in a short time frame, with greater confidence of avoiding detection. False and fraudulent identification is a vulnerability for all reporting entities providing a designated service.

Structuring

Structuring, or smurfing as it is also known, is a ML technique which involves the distribution of a large amount of cash into a number of smaller deposits to evade threshold reporting requirements. Structuring is also used to layer funds into amounts in an attempt to avoid scrutiny through international wire transfers reporting. Common methods of structuring include:

- regularly depositing similar amounts of cash, which are below a country's reporting threshold disclosure limit
- the use of multiple financial institutions or branches of a financial institution often within short timeframes
- the use of third parties to deposit funds into single or multiple accounts.

Betting accounts

Due to the greater scrutiny and customer due diligence imposed by the AML/CTF Act and other related legislation on financial institutions, account operations such as betting accounts, provide further avenues to be used for the purpose of laundering funds. The frequent movements of funds between or to such accounts may be for the purpose of ML.

Debit and credit cards

Becoming more evident for the purpose of ML, these cards provide immediate access to funds. The transfer of money onto these cards can enable potentially large amounts of money to be accessed both domestically and internationally.

Debit cards and credit cards can be obtained in an individual's own name and for use by family members. This can present opportunities for the use of these cards to be exploited for criminal activity. This can be further execarbated where the cards have been obtained in false names. Automatic teller machines (ATMs) are frequently used in these instances to withdraw cash amounts.

False loans

Loans obtained in false names or for the purposes other than those for which they are intended can be used for ML purposes. Funds can be laundered by paying out the loan possibly in one large payment or repayments over a short period of time.

Stored value cards

Stored value cards whether 'open loop – reloadable' or 'closed loop – non reloadable' can be used in a number of ways for ML purposes. Closed loop cards in the form of a gift card can be purchased in bulk using illicit funds. The cards can then be used to purchase high-value goods, which are on-sold to complete the ML process. An open loop card can be used in a similar way to a debit card, with illicit funds added and withdrawn at retail stores and ATMs. Some stored value cards also have options for linked cards which can facilitate the transfer of funds between persons.

Superannuation funds

The misuse of superannuation funds can occur through the establishment of a self managed superannuation fund by a person who allows other persons to place illicit money into this fund. The money can be withdrawn from this superannuation fund and repaid to the person who placed money into the fund.

Rapid settlement of loans or investments

Loans and investments can provide possible vehicles for persons to layer illicit funds and then integrate those funds into other assets. A loan or other investment is obtained and is paid out in rapid time. Payments are made in structured cash amounts or structured domestic transfers. Such early payment is generally seen as an indication of good credit and a healthy income stream. The misuse of these services can be further exacerbated by:

- facilities and loans with little or no scrutiny of income
- limited scrutiny of an individual's financial history and means of repayment.

Large foreign currency exchange

One-off large foreign currency exchanges or deposit of a foreign currency may be of particular concern if it is considered atypical for the customer, or if the customer is not known to the reporting entity.

U-turn transactions

U-turn transactions involve the transfer of funds into Australia from one country and within a short timeframe those funds are transferred out of Australia to a different foreign country. Conversely, the funds may be sent out of Australia and then the funds, or a large proportion of them, are returned to Australia. A person's occupation or the lack of that information may raise further suspicions in these situations.

Large value financial instruments

Illicit funds may be used to purchase large financial instruments such as bank cheques. The ease of transfer of such instruments domestically and internationally can hinder the identification of the money trail. Another example may be attempts by criminals to falsely gain large value 'winners cheques' from gaming venues using illicit funds.

Cheque encashment

Cheques made out to cash or endorsed to other persons can hinder the money trail because of mulitiple recipients of the one cheque. Commingling these cheques with legitimate business funds can also hamper the money trail.

Commingling of funds

Commingling is the process of combining the proceedings of illicit activities for the purpose of disguising the funds. A criminal enterprise may use an established business to place illicit funds within legitimate business takings. This may indicate that the business has greater commercial activity than it actually does have. It is more difficult to identify this type of conduct in a cash business.

Remittance reconciliation and payment actions

Funds obtained from illicit activity may be commingled with legitimate remittance activity. This is often done through a number of cash deposits and subsequent wire transfers overseas. At the point of reconciliation of the transactions, a financial institution may identify the totality of the funds movement.

5 Indicators

The following is a list of indicators (red flags) identified within the case studies provided in this report. Indicators by themselves may not always be immediately indicative of suspect financial or criminal activity but may give rise to further monitoring and due diligence:

- activity was inconsistent with the customer's profile
- associations with multiple accounts under multiple names
- bank Drafts cashed in for foreign currency, e.g. Euros, USD
- cash deposited domestically with the funds subsequently withdrawn from ATMs offshore
- cheques issued to a family member of the person
- cash used to purchase large amounts of gold
- cheques made out regularly to companies and individuals not linked to the account
- deposit of gambling proceeds into a foreign bank account
- depositing multiple large amounts of cash and receiving multiple cheques drawn on that account
- early surrender of insurance policy incurring substantial loss
- elaborate movement of funds through different accounts
- frequent early repayments of loans
- frequent deposits of winning gambling cheques followed by immediate withdrawal of funds in cash
- frequent gaming activity with low returns but with higher chances of winning
- frequent transfers indicated as loans sent from relatives
- frequent remittance of bearer negotiable instruments, e.g. bank drafts offshore
- funds transferred to a charity fund
- gold transported by the individual but purchased with funds drawn from a company account
- high level of funds placed on stored value cards

- high volume of transactions within a short period
- investment cheques issued to a family member
- insurance policy being closed with request for the payment to be made to a third party
- instructing agent to transfer funds into third party accounts
- investment funds sent to countries of concern
- inserting funds into slot machines and immediately claiming those funds as credits
- insurance policy cashed outside the jurisdiction of purchase
- large amount of cash used to purchase insurance policy
- large sums credited into accounts from countries of concern
- large cash deposits used for investment
- large cash deposits into company accounts
- large amounts of currency exchanged for traveller's cheques
- large purchases of gold with the transportation of the gold conducted by the individual
- leaving large amounts of cash with a bookmaker and requesting a cheque in return
- large amounts of cash from unexplained sources
- multiple individuals sending funds to the one beneficiary
- multiple chip cash outs on the same day
- multiple cheques cashed into the one bank account
- multiple loans obtained over a short period of time with repayments made in cash
- multiple issue of stored value cards and debit cards which are accessed offshore
- multiple transactions of a similiar nature on the same day in different locations
- numerous bank drafts purchased domestically and subsequently deposited internationally
- obtained loan and repaid balance in cash
- purchasing high value assets (motor vehicles) followed by immediate resale with payment requested via cheque
- purchase of high value assets with cash e.g. diamond ring, bullion, motor vehicle, property
- purchase of an insurance policy followed by immediate surrender
- purchasing and cashing out casino chips with no gaming activity
- physical carriage of large amounts of cash/bearer negotiable instruments (BNIs) out of Australia
- regular sale of large amounts of precious metals and jewellery
- regular sale of large amounts of gold with payment received in cash
- purchase of multiple money orders
- regular use of stored value card to withdraw funds overseas
- regular insurance claims for less than the actual premium payments
- sale of large amounts of gold from an indivdual
- structuring of cash to purchase traveller's cheques
- structuring the placement of betting transactions
- structuring the purchase of bank drafts
- structuring of cash deposits / withdrawals
- structuring of chip cash outs

- structuring of wire transfers
- transfers from company accounts to private betting accounts
- third party present for all transactions but does not participate in the actual transaction
- transferring funds into third party accounts
- using third parties to undertake wire transfers
- use of an intermediary to make large cash deposits
- use of intermediary to make insurance policy payments
- unusually large transfer of money from an individual to a business
- use of gatekeepers, e.g. accountants and lawyers to undertake transactions
- use of internet banking to transfer illicit funds into accounts of associates
- use of multiple names to conduct similar activity
- use of an offshore company to pay the premiums for an insurance policy taken out privately by individuals
- use of safety deposit box to store large amounts of cash
- use of third parties to undertake structuring of deposits and wire transfers
- unexplained income inconsistent with economic situation
- u-turn transactions occurring with funds being transferred out of Australia and then portions of those funds being returned
- use of internet banking to frequently access Australian-based accounts internationally
- use of a remittance dealer to send a large amount of cash
- use of a remittance dealer to send large cash amounts overseas
- use of third parties to purchase gaming chips
- use of gatekeepers (accountant) to structure deposits and purchase real estate
- use of a third party to gamble proceeds through casinos
- use of companies to move funds under the guise of legitimate transactions
- use of non-resident accounts
- use of false and stolen identities to open and operate bank accounts
- withdrawal of a large amount of funds in cash
- wire transfers to tax haven countries
- wire transfers from third parties located in tax haven countries
- wire transfers used to purchase insurance policies.

Case studies

Case 1

Structuring of cash transactions to launder money

An Australian law enforcement agency arrested two people and charged them with two counts each of structuring transactions contrary to section 31(1) of the FTR Act. Investigations revealed that both defendants structured 19 separate cash withdrawals each under AUD10,000 from their bank account. Within eight days both defendants structured a further 125 cash deposits each under AUD10,000, into a joint account at a different bank.

AUSTRAC disseminated the intelligence to a law enforcement agency for further investigation. The intelligence showed clear structuring that allowed law enforcement to initiate their investigation and charge both people under the FTR Act. At the time of the arrests, investigators executed search warrants at the homes of the defendants and worked with the Commonwealth Director of Public Prosecutions (DPP) to restrain the sum of approximately AUD1.17 million pursuant to section 17 of the *Proceeds of Crime Act* (2002). These funds were restrained on the grounds that they were the instrument of the structuring offences.

Both defendants pleaded guilty to the structuring offences and appeared before the County Court two months later for sentencing. Both defendants agreed to forfeit approximately AUD1.17 million and were released on an AUD5,000 good behaviour bond for three years.

Offence	Money laundering (structuring)
Customer	Individual
Industry	Authorised deposit-taking institutions
Channel	Physical (face-to-face)
Jurisdiction	Domestic
Designated service	Accounts
Indicators	High volume of transactions within a short period Structuring of cash deposits / withdrawals

Case 2

Depositing altered cheques to undertake fraud

An overseas false identification syndicate transferred money between members and deposited altered cheques into the subject's account. The use of false identification allowed the individuals involved to conduct the transactions under multiple names in an attempt to avoid detection by law enforcement agencies. Other individuals also attempted to open accounts with altered cheques.

Offence	Fraud
Customer	Individual
Industry	Authorised deposit-taking institutions
Channel	Physical (face-to-face)
Jurisdiction	Domestic
Designated service	Accounts, accounts - cheque book facility
Indicators	Use of multiple names to conduct similar activity

Case 3

Bonds used in cold calling of bank drafts scam

Authorities received numerous complaints in regard to a cold calling fraud which had been targeting Australians. Victims had been approached to invest a total of AUD8 million in 'heating oil options', 'gasoline options' and 'gold bullion options' purportedly traded on non-existent foreign currency exchanges.

The unsuspecting investors had been instructed to remit funds into a number of company accounts located in Malaysia and Hong Kong. AUSTRAC information identified that a portion of the transmitted funds were being returned to Australian based beneficiary accounts. The account holders were identified as being a Malaysian businessman and an Australian student who both held accounts with major banking institutions. The student allegedly used the received funds to purchase AUD100,000 worth of bonds.

AUSTRAC information revealed that the activity had only been occurring for a short time before investigations began.

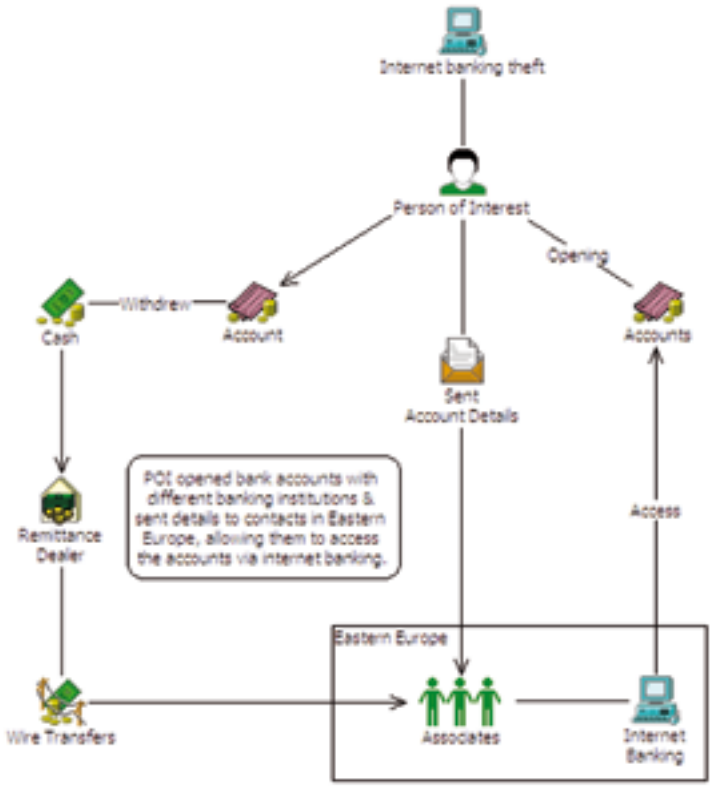
Offence	Fraud
Customer	Individual
Industry	Authorised deposit-taking institutions
Channel	Electronic
Jurisdiction	International – Malaysia, Hong Kong
Designated service	Accounts, debt instrument, electronic funds transfer
Indicators	Unexplained income inconsistent with economic situation U-turn transactions occurring with funds being transferred out of Australia and then portions of those funds being returned

Case 4

Laundering the proceeds of internet banking theft

Law enforcement arrested a person in Perth who was involved in laundering the proceeds of internet banking theft. A person stole funds over a period of 12 months and used multiple bank accounts to launder AUD60,000. In one instance, the person received AUD10,000, which was withdrawn from their bank account and sent to criminals in Eastern Europe using a remittance service. The person also opened a number of bank accounts with different banking institutions and sent the account numbers to contacts in Eastern Europe, allowing them to directly withdraw money via the internet from the Australian accounts.

Offence	Theft
Customer	Individual
Industry	Authorised deposit-taking institutions, remittance services
Channel	Electronic
Jurisdiction	Domestic, international – Eastern Europe
Designated service	Accounts, designated remittance arrangement, electronic funds transfer
Indicators	Use of internet banking to frequently access Australian based accounts internationally Use of a remittance dealer to send a large amount of cash Withdrawal of a large amount of funds in cash



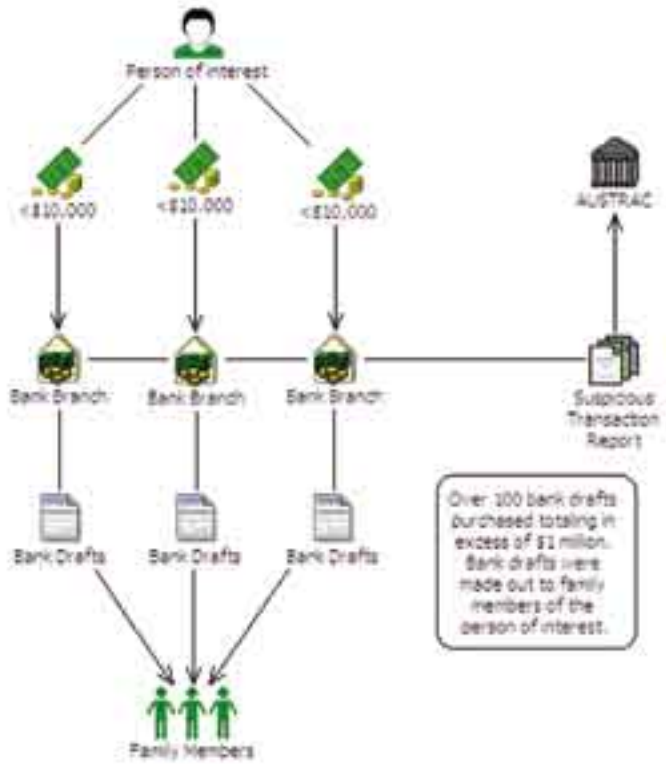
Case 5

Multiple purchases of banks' drafts used to launder funds

An investigation into an individual involved in the laundering of money was initiated by information held by AUSTRAC. Suspect Transaction Reports (SUSTRs) were reported to AUSTRAC detailing multiple purchases of international bank drafts using cash structured below the reporting threshold. The suspect would purchase multiple drafts from the same location on the same day before then moving on to other bank branches to repeat the process. Over 100 bank drafts were purchased totalling in excess of AUD1million. The drafts were made out to family members.

The suspect pleaded guilty to 33 counts of FTR offences and was convicted and sentenced to imprisonment for an aggregate of six months to be served by way of an intensive correction order.

Offence	Money laundering (structuring)
Customer	Individual
Industry	Authorised deposit-taking institutions
Channel	Physical (face-to-face)
Jurisdiction	Domestic
Designated service	Accounts, debt instruments
Indicators	Structuring the purchase of international bank drafts Multiple transactions of a similiar nature on the same day, in different locations



Case 6

Drug proceeds concealed by third parties

A dubious international mail package from Canada was intercepted as a result of intelligence developed by a law enforcement agency. On further inspection the package contained an illegal precursor drug used to manufacture amphetamines.

This information linked the addressee who had previously been convicted of a similar offence to the illegal importation. A search was conducted on the residence of the person and assets including cash, a diamond ring and a motor vehicle were confiscated in addition to further funds located in a safety deposit box.

Analysis of AUSTRAC information revealed that the suspect had opened several accounts under their own name and also in false names. Financial Transaction Reports (FTR) information also showed SUSTRs profiling structuring activity where the suspect was deliberately depositing cash under AUD10,000. The SUSTRs not only identified structuring activity, they also highlighted the alleged use of third parties to undertake structuring of deposits and wire transfers on behalf of the suspect.

Following the investigation the suspect pleaded guilty to one count of importing prohibited imports under the Commonwealth *Criminal Code 1995*, section 400.3 (1) and was sentenced to six years and two months with a non-parole period of four years. The suspect also pleaded guilty to a number of money laundering offences and the use of bank accounts in false names.

The cash and other items of property seized amounted to a total in excess of AUD350,000 forfeited to the Commonwealth.

Offence	Drug importation, structuring
Customer	Individual
Industry	Authorised deposit-taking institutions
Channel	Agent / third party, physical (face-to-face)
Jurisdiction	International - Canada
Designated service	Accounts, electronic funds transfer, custodial or depository service
Indicators	Associations with multiple accounts under multiple names Purchase of high value assets, e.g. diamond ring and motor vehicle Use of safety deposit box to store large amounts of cash Use of third parties to undertake structuring of deposits and wire transfers Structuring of cash deposits

Case 7

Debit cards used in laundering process

Following the dissemination of SUSTRs received by AUSTRAC to a law enforcement agency, an AUSTRAC alert was raised on a suspect and his associate. The FTR information related to a student who on a number of occasions loaded structured amounts of AUD9,900 to avoid reporting thresholds onto debit cards in his own name and that of his associate. The suspect had previously come to the notice of law enforcement agencies in relation to a cocaine seizure which he was alleged to have organised. Following further research and intelligence gathering a joint operation commenced involving multiple law enforcement agencies.

A further 15 SUSTRs were recorded on the AUSTRAC database, showing both the suspect and his associate conducting deposits of structured amounts onto debit cards. AUSTRAC information detected a further series of financial transactions linked to both targets. An assessment of FTR information was disseminated to the law enforcement agencies and assisted the investigation, resulting in the arrest of both targets.

The associate departed Brisbane for South America and returned to Brisbane from another South American destination 12 days later with approximately 5.8 kilograms of cocaine in his baggage. He later admitted that he had previously brought drugs into Australia on two occasions for a payment of AUD28,000 each time. He was arrested and charged with importing and possessing a prohibited import. The suspect was also charged with conspiracy to bring into Australia approximately 5.8 kilograms of cocaine, structuring and money laundering of almost AUD400,000. He was found guilty and sentenced to seven years imprisonment.

Offence	Drug importation, money laundering
Customer	Individual
Industry	Authorised deposit-taking institutions
Channel	Agent / third party, physical (face-to-face)
Jurisdiction	Domestic, international – South America
Designated service	Accounts – debit card facility, payment orders and stored value cards
Indicators	Structuring of cash deposits Activity was inconsistent with the customer's profile

Case 8

Scented cash implicates drug offenders

Several SUSTRs reported to AUSTRAC were referred to a state law enforcement agency assisting in subsequent investigations in the seizure of over 11 kilograms of cannabis. The SUSTRs provided details of numerous cash deposits and withdrawals. This, along with other information contained on the SUSTRs did not appear consistent with the customer profile. The investigating agency made enquiries with other agencies which assisted in gathering evidence that the people had no apparent lawful means of sourcing this amount of cash.

It was further noted on a number of the SUSTRs that the cash smelt strongly of marijuana. This led investigators to suspect that the persons may have been involved in large-scale cannabis dealing within Australia and possibly overseas.

A search warrant was obtained and executed on the suspects' premises at which time the cannabis, a large amount of cash and two vehicles were seized. Two persons were arrested and charged with various drug offences.

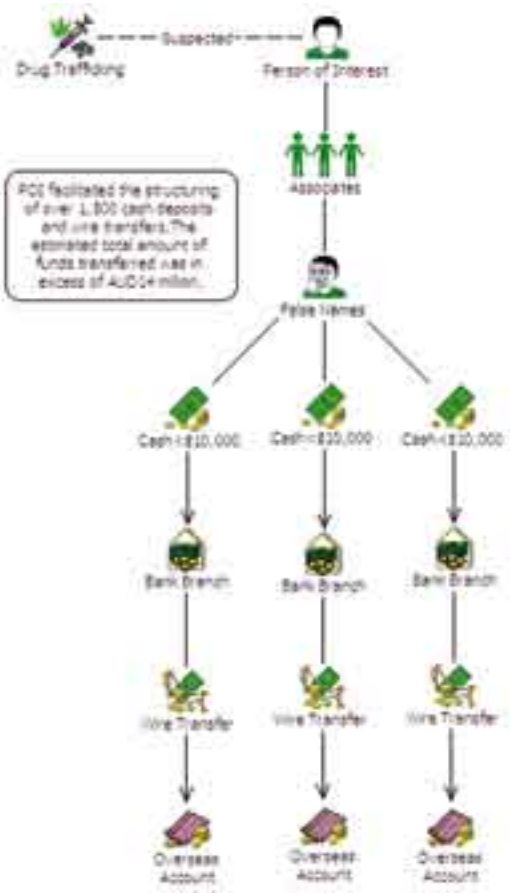
Offence	Drug possession
Customer	Individual
Industry	Authorised deposit-taking institutions
Channel	Physical (face-to-face)
Jurisdiction	Domestic
Designated service	Accounts, money on deposit
Indicators	Structuring of cash transactions which were from the proceeds of crime Cash inconsistent with customer profile

Case 9

Drug network undertakes multiple structured wire transfers

A person facilitated the structuring of over 1,500 cash deposits and wire transfers utilising a network of associates. The associates would travel from one bank branch to the next on the same day, making deposits using false names and addresses. The wire transfers were deposited into numerous overseas bank accounts controlled by local criminals in that jurisdiction. Each deposit would be under the AUD10,000 reporting limit in order to avoid AUSTRAC and law enforcement detection. The estimated total amount of funds transferred was in excess of AUD14 million. On occasion, in excess of AUD100,000 was sent overseas in one day.

Offence	Drug trafficking and money laundering
Customer	Individual
Industry	Authorised deposit-taking institutions
Channel	Physical (face-to-face)
Jurisdiction	International
Designated service	Accounts, electronic funds transfer
Indicators	Multiple transactions of a similar nature on the same day, in different locations Structuring of cash amounts and wire transfers



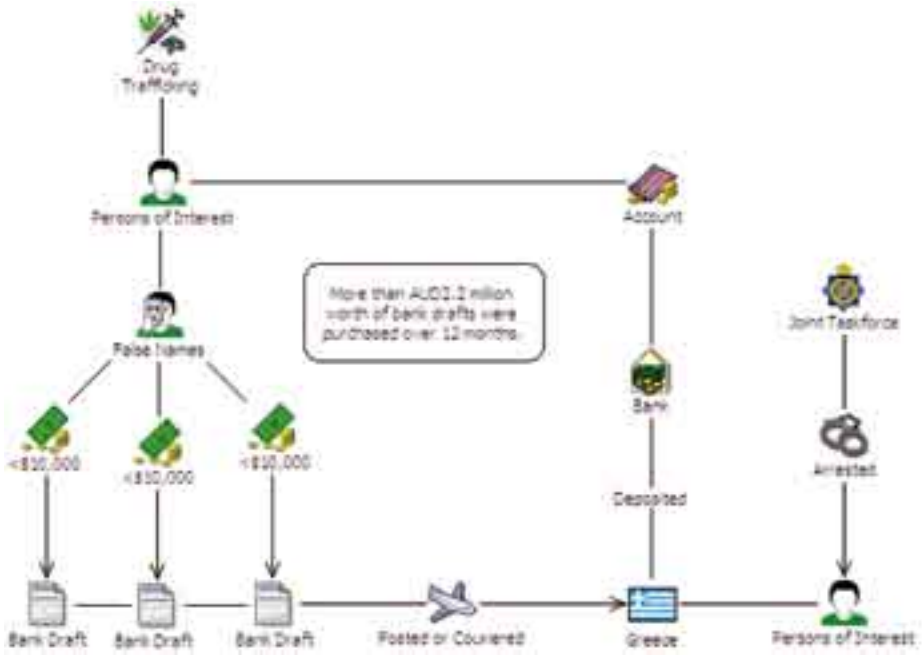
Case 10

Third parties used to send bank drafts offshore

A large number of bank drafts valued at between AUD8,000–9,000 were purchased in the names of a number of different entities on behalf of a person. More than AUD2.2 million worth of bank drafts were purchased over a 12 month period and it was suspected that these drafts were to be used for a large import of precursor chemicals into Australia. It was established that the drafts purchased in Australia were being presented at various banks in Greece and deposited into bank accounts of the person. A joint Australian, United States and Greek taskforce undertook search warrants and arrested three Australians in Greece. 100,000 MDMA tablets were seized and 1.2 million Euro restrained.

The drafts were being purchased below AUD10,000 in order to avoid the reporting threshold and were purchased under false names and made out to false payees. After the drafts were purchased, the purchasers would sign the draft over to the intended payee who was based in Greece. The drafts were then either posted or couriered to Greece and deposited into a Greek account by the intended recipient.

Offence	Drug trafficking
Customer	Individual
Industry	Authorised deposit-taking institutions
Channel	Physical (face-to-face)
Jurisdiction	International – Greece, United States, Australia
Designated service	Accounts, debt instruments
Indicators	Numerous bank drafts purchased domestically and subsequently deposited internationally Structuring the purchase of bank drafts Physical carriage of cash / BNIs out of Australia



Case 11

Company directors generate false receipts to evade tax

Directors of a company were involved in purchasing large quantities of duty free cigarettes and alcohol to sell on the domestic market contrary to their export-duty free status, thus avoiding tax obligations. By not paying any tax on the goods the company was able to markedly increase profits. The syndicate also generated false receipts that purported to come from an export company detailing their alleged cigarette exports. Investigations into the company confirmed that no such exports had ever been made.

Payment for the cigarettes was made to the delivery driver on a cash-on-delivery basis. A large number of the company's sales occurred over the internet from customers paying via credit card. Payments for these orders were made from one of two credit cards linked to Belize bank accounts. One of these cards was held in the company's name. The money in the Belize bank account was sent there by one of the directors using several false names from Australia, Belize, Hong Kong, and Vietnam. The director conducted structured wire transfers under false names and from company accounts. The funds were deposited at well known banks, with multiple transactions occurring on the same day at different bank locations, and all of the cash transfers were conducted in amounts of just under AUD10,000 to avoid the reporting threshold.

Offence	Tax / excise evasion
Customer	Business
Industry	Authorised deposit-taking institutions
Channel	Electronic
Jurisdiction	International – Belize, Hong Kong, Vietnam
Designated service	Accounts, electronic funds transfer
Indicators	Multiple transactions of a similar nature on the same day, in different locations Structuring of cash to facilitate offshore transfers Use of credit cards linked to interesting countries, e.g. tax havens Wire transfers to interesting countries, e.g. tax havens

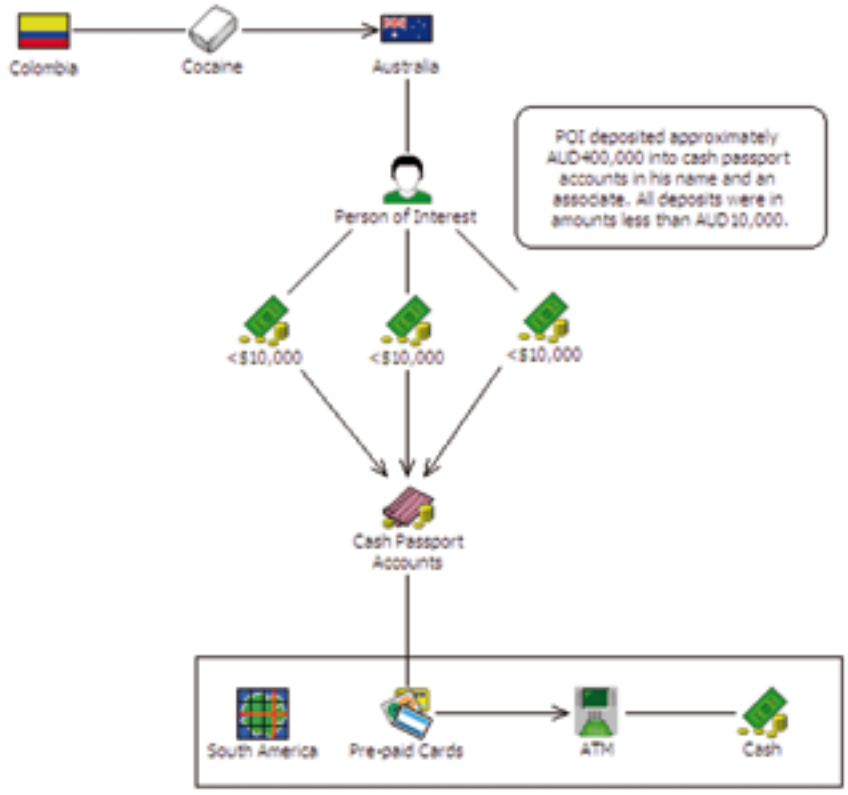
Case 12

Multiple pre-paid cards used to withdraw funds offshore

A person was part of a syndicate involved in the importation of cocaine from Colombia. The person opened an account which provided access to pre-paid cards. The account holder obtained multiple cards which enabled him and associates to obtain currency anywhere in the world.

It was established by investigators that the person had deposited approximately AUD400,000 into the account in his name and that of an associate. These deposits were all made in amounts of less than AUD10,000 to avoid the reporting threshold in Australia and then subsequently withdrawn in South America using various ATMs.

Offence	Drug importation
Customer	Individual
Industry	Authorised deposit-taking institutions
Channel	Physical (face-to-face)
Jurisdiction	International – South America
Designated service	Accounts, payment order and stored value cards
Indicators	Cash deposited domestically with the funds subsequently withdrawn from ATMs offshore High level of funds placed on stored value cards Multiple issue of stored value cards Structuring of cash deposits



Case 13

Broker used to facilitate money laundering

An account was opened in a particular country in a false name. Wire transfers from third parties located in tax haven countries were transferred into the account, almost always under the AUD10,000 reporting threshold. The customer faxed instructions to the broker to transfer money to third party accounts in the United States, including three different accounts at three different banks on the same day.

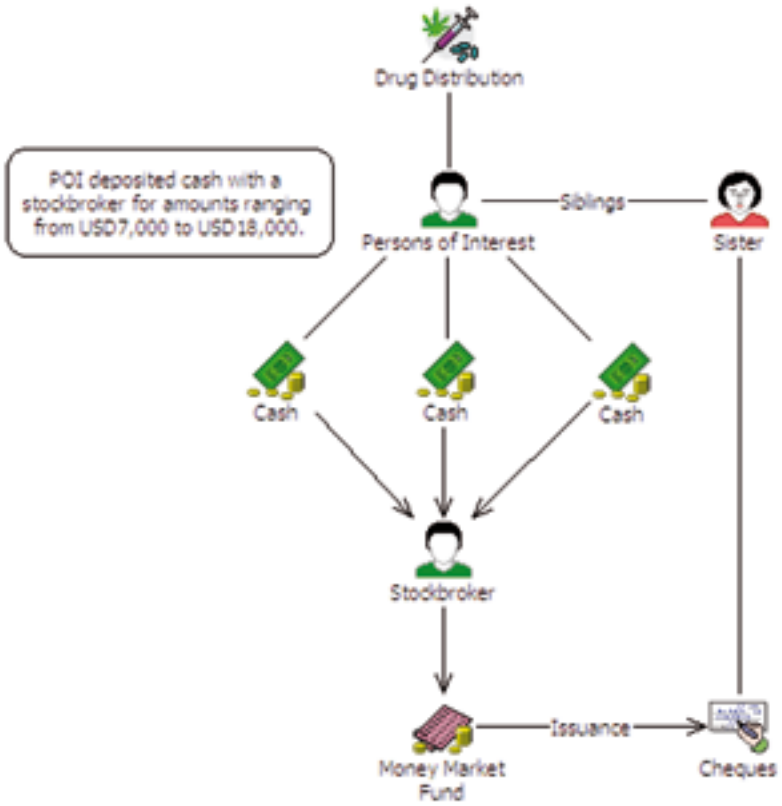
Offence	Money laundering
Customer	Individual
Industry	Securities and derivatives, authorised deposit-taking institutions
Channel	Agent / third party, fax
Jurisdiction	International
Designated service	Accounts, electronic funds transfer, deals in securities markets
Indicators	Instructing agent to transfer funds into third party accounts Multiple transactions of a similar nature on the same day, in different locations Structuring of wire transfers Wire transfers from third parties located in tax haven countries

Case 14

Stockbroker used to assist drug dealing client

A stockbroker in a particular country continuously accepted cash deposits from a client in the range of USD7,000-18,000. The funds were placed in the money market fund of the client's sister and withdrawn through the issuance of cheques. After the broker was arrested on unrelated embezzlement charges, the client's identity became known to law enforcement. When the police conducted a background check on the client, it was revealed that the stockbroker's client was a known drug dealer.[2]

Offence	Drug distribution and embezzlement
Customer	Individual
Industry	Securities and derivatives
Channel	Agent / third party, physical (face-to-face)
Jurisdiction	International
Designated service	Accounts - cheque book facility, deals in securities markets
Indicators	Investment cheques issued to a family member Large cash deposits used for investment



[2] Financial Action Task Force on Money Laundering (FATF), 'Report of Money Laundering Typologies 2002-2003., p. 12, viewed 03/01/2007, <*http://www.fatf-gafi.org/dataoecd/29/33/34037958.pdf*>.

Case 15

Fraud money invested in securities market

A brokerage firm opened several accounts for a group of 12 linked individuals, including a non-resident account that was used to record very large movements and apparently to centralise most of the suspected flows, which totalled more than USD18 million.

The launderers used the following two mechanisms:

- the accounts of some of the parties involved were credited with large sums received from countries of concern, which were invested in the stocks of listed companies in a particular country
- the accounts of the individuals concerned were credited with sums from regions of concern, which were transferred to the non-resident account (the first accounts were used as screens).

This securities buy/sell mechanism was used to filter the flows through the broker and subsequently the clearer and custodian. Once filtered, the funds were sent to locations in regions of concern and offshore financial centres.

This information showed that the co-opted broker had been used to launder the proceeds from various forms of frauds. The manager of the brokerage firm served as a relay for the criminal organisations involved.[3]

Offence	Fraud
Customer	Individual
Industry	Securities and derivatives
Channel	Agent / third party
Jurisdiction	International
Designated service	Accounts, electronic funds transfer, deals in securities markets
Indicators	Elaborate movement of funds through different accounts Investment funds sent to interesting countries Large sums credited into accounts from interesting countries Use of non-resident accounts

[3] Financial Action Task Force on Money Laundering (FATF), 'Report of Money Laundering Typologies 2002-2003', <*http://www.fatf-gafi.org/dataoecd/29/33/34037958.pdf*>.

Case 16

Cash couriers used to launder funds

AUSTRAC information identified a series of financial transactions where a person appeared to have been conducting them in such a way as to avoid the reporting threshold of the FTR Act. FTRs showed that more than AUD4 million was remitted by one person to accounts at two different banks in Asia.

After it received AUSTRAC's information, an Australian law enforcement agency commenced an investigation into the possible money laundering activities of the subject of these reports. The person was already known to law enforcement agencies.

After several months of investigation, information was received specifying that the person was collecting money from an associate then remitting the funds to Asia via a particular cash dealer.

The person was observed attending an associate's premises before driving towards the cash dealer's business premises. The person was intercepted and found to be in possession of approximately AUD50,000 cash. The person was subsequently arrested and during an interview, investigators learned that a resident in Asia paid the person a commission in return for the remittance of funds to Asia. It was further ascertained that packages of AUD100,000 cash were delivered within Australia and subsequently electronically remitted overseas through a series of structured transactions.

In court, the person pleaded guilty to one count of money laundering and one count of defrauding the Commonwealth and was found guilty on a second count of defrauding the Commonwealth. He was sentenced to a maximum of six months imprisonment for money laundering and 12 months imprisonment for defrauding the Commonwealth.

As a result of this investigation, a tax assessment of approximately AUD4 million was raised and more than AUD600,000 has been recovered.

Offence	Tax evasion, money laundering
Customer	Individual
Industry	Remittance services
Channel	Electronic
Jurisdiction	International - Asia
Designated service	Electronic funds transfer, designated remittance arrangement
Indicators	Large amounts of cash from unexplained sources Structuring of wire transfers Use of a remittance dealer to send large cash amounts overseas

Case 17

Businessman defrauds Commonwealth and sends funds offshore

A revenue agency initiated an operation after receiving a SUSTR referred to them by AUSTRAC. Suspicions were raised as the subject of the SUSTR, a small businessman, was found to be in receipt of a large amount of government funds.

AUSTRAC information was used to identify transactions conducted by the businessman, highlighting the fact that he was sending funds offshore to Africa. A further four SUSTRs were received by AUSTRAC, showing that the person was structuring his withdrawals in an attempt to avoid detection by AUSTRAC. These reports also indicated the person's intention to leave the country permanently for an overseas destination.

Under Section 16(4) of the FTR Act, the revenue agency served a notice on the cash dealer involved to gather more information regarding the person. As a result of further enquiries, it was found that the person had defrauded the Commonwealth of over AUD100,000. The revenue agency sought the assistance of an Australian law enforcement agency to arrest the person two days before he was due to leave Australia.

The person was charged with two counts of obtaining a financial benefit by deception under section 134.2(1) of the *Criminal Code 1995*. Subsequently, he was found guilty and was sentenced to one year's imprisonment on the first offence and two-and-a-half years imprisonment on the second offence, with a minimum term of 10 months to be served.

Without the cash dealer's report, their suspicions and consequently AUSTRAC's referral of the SUSTR, which highlighted the occurrence of an offence, the person would have remained undetected and would have left Australia.

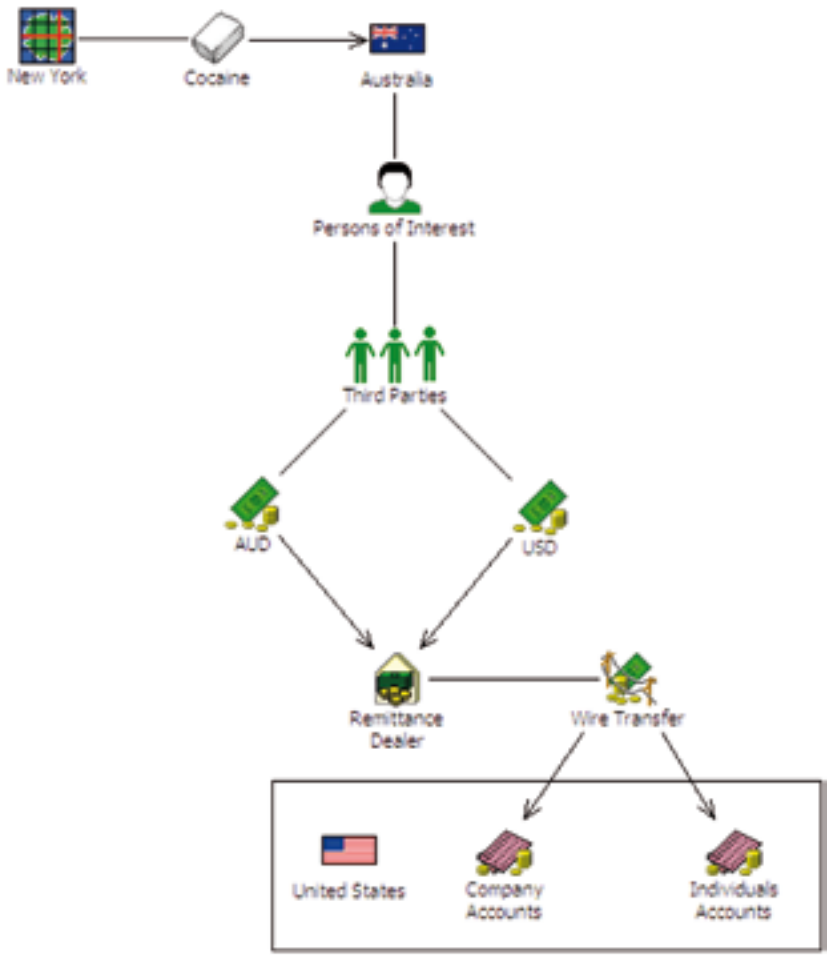
Offence	Structuring, fraud
Customer	Individual
Industry	Remittance services
Channel	Physical (face-to-face)
Jurisdiction	International - Africa
Designated service	Electronic funds transfer, designated remittance arrangement
Indicators	Structuring of cash withdrawals Unexplained wealth inconsistent with economic situation

Case 18

'Nightclubbers' used to send funds offshore

Persons of interest were involved in a cocaine importation secreted in clothing consignments from New York using a parcel courier service. Prior to each importation, wire transfers were sent to accounts in the United States (US). These transfers were conducted by individuals who were recruited by the persons of interest at night clubs to send money on their behalf. The funds were sent to individuals and company accounts held in the US in amounts ranging from AUD6,000-19,995. The currency of the transactions also alternated between USD and AUD.

Offence	Drug importation
Customer	Business, individual
Industry	Remittance services, money service businesses
Channel	Electronic
Jurisdiction	International
Designated service	Accounts, designated remittance arrangement, electronic funds transfers, foreign exchange services
Indicators	Alternating currency for transactions Use of multiple third parties to send wire transfers



Case 19

Wire transfers used as primary source of funding drugs

AUSTRAC information initiated a joint investigation that led to the seizure of narcotics imported from Europe. FTR information related to this investigation helped to identify the overseas based beneficiary of the funds transfers as the main source of the narcotics. Other Australian associates were also identified from FTR information as they were sending funds to the same beneficiary. Key information in the form of domestic and overseas addresses and accounts was also discovered from the FTRs.

The FTRs were significant in determining the involvement of the persons in the financing of the imported narcotics. In addition to this, a SUSTR lodged on one of the suspects confirmed links to persons associated with the narcotics seizure. As a result three persons were found guilty and one person pleaded guilty to being knowingly concerned with the importation of a prohibited import (MDMA) contrary to section 233B(1)(d) of the *Customs Act 1901*. The jail terms ranged from four months to nine years.

Offence	Drug trafficking
Customer	Individual
Industry	Remittance services
Channel	Electronic
Jurisdiction	International
Designated service	Accounts, electronic funds transfer
Indicators	Multiple individuals sending funds to the one beneficiary

Case 20

Wire transfers and e-gold payments used to purchase stolen bank details

Persons of interest were involved in the purchase of stolen bank account and credit card details from Russia and Eastern Europe via the internet. These were purchased through international funds transfer instructions (IFTIs) of approximately AUD2,000 and by way of e-gold payments. The principal person of interest was arrested on 26 fraud and computer crime offences in relation to using these bank details to withdraw funds without authorisation in internet transfers to accounts of associates. AUSTRAC searches revealed that a person in this syndicate had a history of alleged involvement in internet bank fraud through phishing.

A laptop seized at the arrest of the principal person revealed details of IFTIs transacted through remittance dealers and e-gold. Russian and other recipients identified from these transactions facilitated the identification of additional persons from AUSTRAC information.

Offence	Fraud and identity theft
Customer	Individual
Industry	Remittance services, authorised deposit-taking institutions
Channel	Electronic
Jurisdiction	International - Eastern Europe
Designated service	Accounts, electronic funds transfer, designated remittance arrangement
Indicators	Use of internet banking to transfer illicit funds into mules' accounts

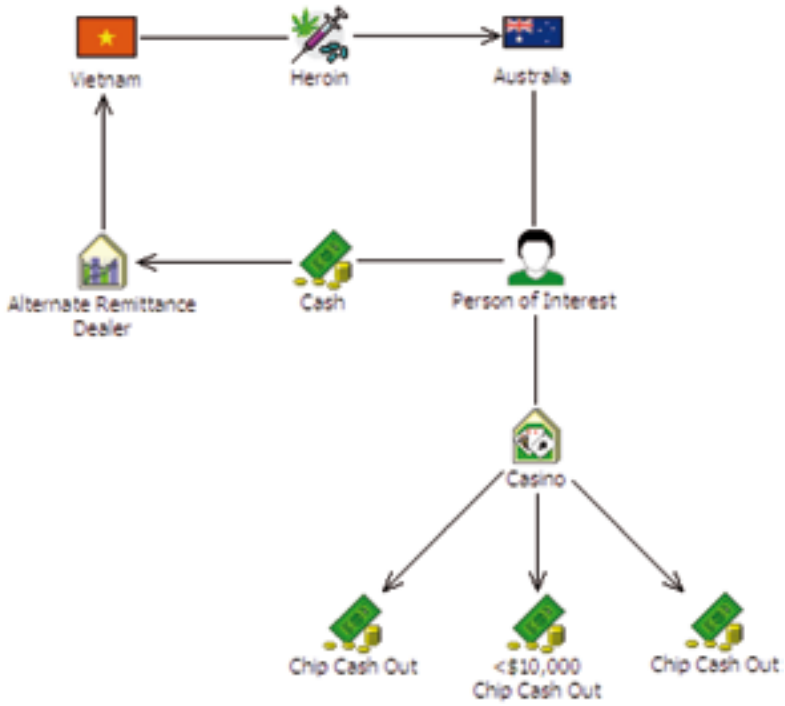
Case 21

Drug proceeds converted into casino chips by third parties

A person was involved in the importation and distribution of heroin into Australia from Vietnam. The person gambled a large proportion of the proceeds at casinos and used third parties to purchase gaming chips on his behalf. Reports from the casino noted multiple chip cash outs on the same day, with some of these transactions being structured to avoid the AUD10,000 reporting threshold.

Further investigations noted that he would send large cash payments to various entities in Vietnam through a remittance dealer. The remittance dealer was a trusted associate of the person and had been non-compliant with his reporting obligations under the FTR Act.

Offence	Drug importation
Customer	Individual, foreign entity
Industry	Remittance services, gambling services
Channel	Agent / third party
Jurisdiction	International - Vietnam
Designated service	Designated remittance arrangement, gambling services
Indicators	Large cash amounts deposited with remittance dealer Multiple chip cash outs on the same day Structuring of chip cash outs Use of a remittance dealer to send large cash amounts overseas Use of third parties to purchase gaming chips Wire transfers to a country of interest



Case 22

The use of life insurance single premium policies

A bankrupt used the name of a family member to pay cash into an account and to draw a cheque to the value of the cash. He provided the cheque to a lawyer. The lawyer provided a cheque to the family member for part of the sum and then deposited the remainder of the funds into the person's premium life policy which was immediately surrendered. The surrender value was paid into the family member's account.[4]

Offence	Fraud
Customer	Individual
Industry	Insurance intermediaries
Channel	Agent / third party, physical (face-to-face)
Jurisdiction	International
Designated service	Accounts, accounts - chequebook facility, insurance and superannuation services
Indicators	Cheques issued to a family member Purchase of an insurance policy followed by immediate surrender Use of gatekeepers, e.g. accountant and lawyer to undertake transactions

[4] Financial Action Task Force (FATF) 'Money Laundering and Terrorist Financing Typologies 2004 – 2005', published 10 June 2005, *<http://www.fatf-gafi.org/dataoecd/16/8/35003256.pdf>.*

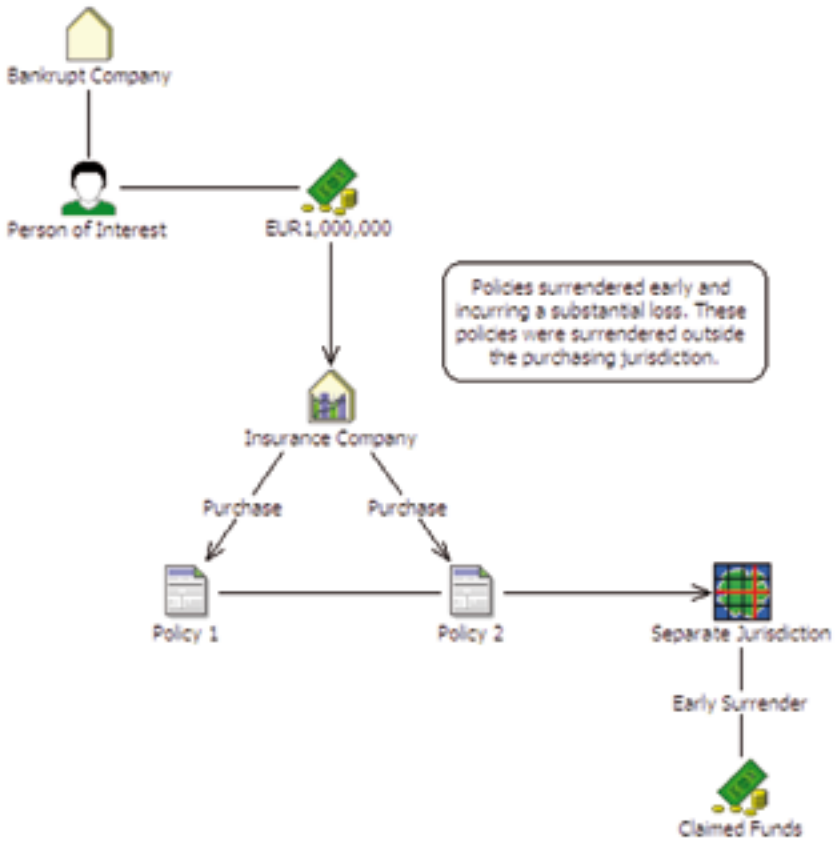
Case 23

Early surrender of life insurance policy to evade creditors

The subject deposited 1 million Euros in cash with a life insurance company in two single premium life policies which were surrendered early incurring a loss of 40 per cent of the investment. The investment was cashed outside the jurisdiction concerned in an effort to evade creditors seeking remuneration from the subject's fraudulently declared bankrupt company.

Source: Belgium[5]

Offence	Fraud
Customer	Individual
Industry	Insurance intermediaries
Channel	Physical (face-to-face)
Jurisdiction	International
Designated service	Insurance and superannuation services
Indicators	Early surrender of insurance policy incurring substantial loss Insurance policy cashed outside the jurisdiction of purchase Large amount of cash used to purchase insurance policy



[5] Financial Action Task Force (FATF) 'Money Laundering and Terrorist Financing Typologies 2004 – 2005', published 10 June 2005, Case Example 2, <*http://www.fatf-gafi.org/dataoecd/16/8/35003256.pdf*>.

Case 24

Life insurance as a cover for tax fraud

A husband and wife had taken out a life insurance policy each in their own names with annual premiums. In the event of the death of one of the spouses, the other spouse would become the beneficiary of the insurance. The holder of the account through which the premiums had been paid was found not to be the policy-holders' but a company abroad of which they were directors. However, this was a life insurance policy taken out privately by the couple and not by the company. Investigations revealed that the scenario set up had been intended to conceal the illicit origin of the funds which originated from serious and organized tax fraud.[6]

Source: Belgium

Offence	Tax fraud
Customer	Business, foreign entity, individual
Industry	Insurance intermediaries
Channel	Physical (face-to-face)
Jurisdiction	International
Designated service	Accounts, insurance and superannuation services
Indicators	Use of an offshore company to pay the premiums for an insurance policy taken out privately by individuals

[6] Financial Action Task Force (FATF) 'Money Laundering and Terrorist Financing Typologies 2004 – 2005', published 10 June 2005, *<http://www.fatf-gafi.org/dataoecd/16/8/35003256.pdf>.*

Case 25

Money launderers use the insurance industry to clean their funds

Clients in several countries used the services of an intermediary to purchase insurance policies. Identification was taken from the client by way of an identification card, but these details were unable to be clarified by the providing institution locally, which was reliant on the intermediary doing due diligence checks.

The policy was put in place and the relevant payments made by the intermediary to the local institution. Then, after a couple of months had elapsed, the institution would receive notification from the client stating that there was now a change in circumstances, and they would have to close the policy suffering the losses but coming away with a clean cheque from the local institution.

On other occasions the policy would be left to run for a couple of years before being closed with the request that the payment be made to a third party. This was often paid with the receiving institution, if local, not querying the payment as it had come from another reputable local institution.[7]

Offence	Money laundering
Customer	Individual
Industry	Insurance intermediaries
Channel	Agent / third party, physical (face-to-face)
Jurisdiction	International
Designated service	Insurance and superannuation services
Indicators	Early surrender of insurance policy incurring substantial loss Insurance policy being closed with request of the payment to be made to a third party Use of intermediary to make insurance policy payments

[7] Financial Action Task Force on Money Laundering (FATF), 'Report of Money Laundering Typologies 2003-2004', viewed 03/01/2007, <*http://www.fatf-gafi.org/dataoecd/19/11/33624379.PDF*>.

Case 26

Criminal funds laundered through payment of insurance premiums

A company director set up a money laundering scheme involving two companies, each one established under two different legal systems. Both of the entities were to provide financial services and providing financial guarantees for which he would act as director.

These companies wired the sum of USD1.1 million to the accounts of the company director in Country S. It is likely that the funds originated from some sort of criminal activity.

Funds were transferred from one account to another (several types of accounts were involved, including both current and savings accounts). Through one of these transfers, the funds were transferred to Country U from a current account in order to make payments on life insurance policies. The investment in these policies was the main mechanism in the scheme for laundering the funds. The premiums paid for the life insurance policies in Country U amounted to some USD1.2 million and represented the last step in the laundering operation.[8]

Offence	Money laundering
Customer	Individual, business
Industry	Insurance intermediaries, authorised deposit-taking institutions
Channel	Electronic
Jurisdiction	International
Designated service	Accounts, electronic funds transfer, insurance and superannuation services
Indicators	Elaborate movement of funds through different accounts Wire transfers used to purchase insurance policies

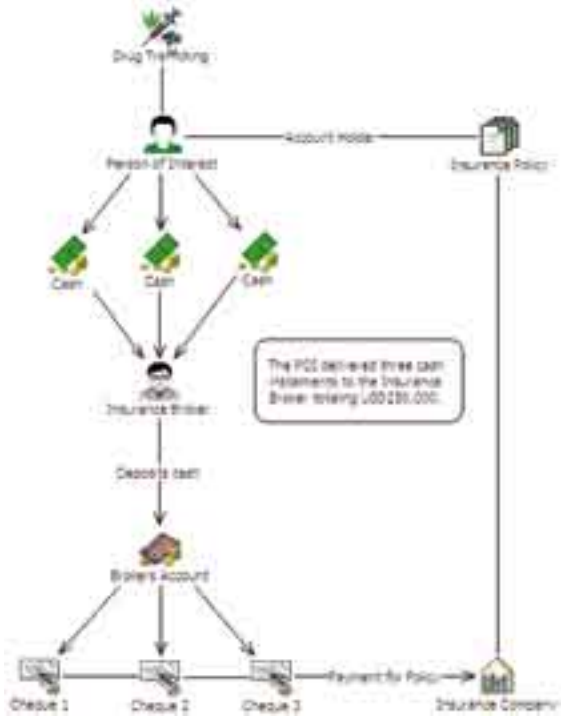
[8] Financial Action Task Force on Money Laundering (FATF), 'Report of Money Laundering Typologies 2002-2003', *<http://www.fatf-gafi.org/dataoecd/29/33/34037958.pdf>.*

Case 27

Drug trafficker launders funds through purchase of life insurance policy

A person (later arrested for drug trafficking) made a financial investment (life insurance) of USD250,000 by means of an insurance broker. The person contacted an insurance broker and delivered a total amount of USD250,000 in three cash instalments. The insurance broker did not report the delivery of that amount and deposited the three instalments in the bank. These actions raised no suspicion at the bank, since the insurance broker was known to them as being connected to the insurance branch. The insurance broker delivered, afterwards, to the insurance company responsible for making the financial investment, three cheques from a bank account under his name, totalling USD250,000, thus avoiding raising suspicions with the insurance company.[9]

Offence	Drug trafficking
Customer	Individual
Industry	Insurance intermediaries, authorised deposit-taking institutions
Channel	Agent / third party, physical (face-to-face)
Jurisdiction	International
Designated service	Accounts, accounts - chequebook facility, insurance and superannuation services
Indicators	Depositing multiple large amounts of cash and receiving multiple cheques drawn on that account Use of an intermediary to make large cash deposits



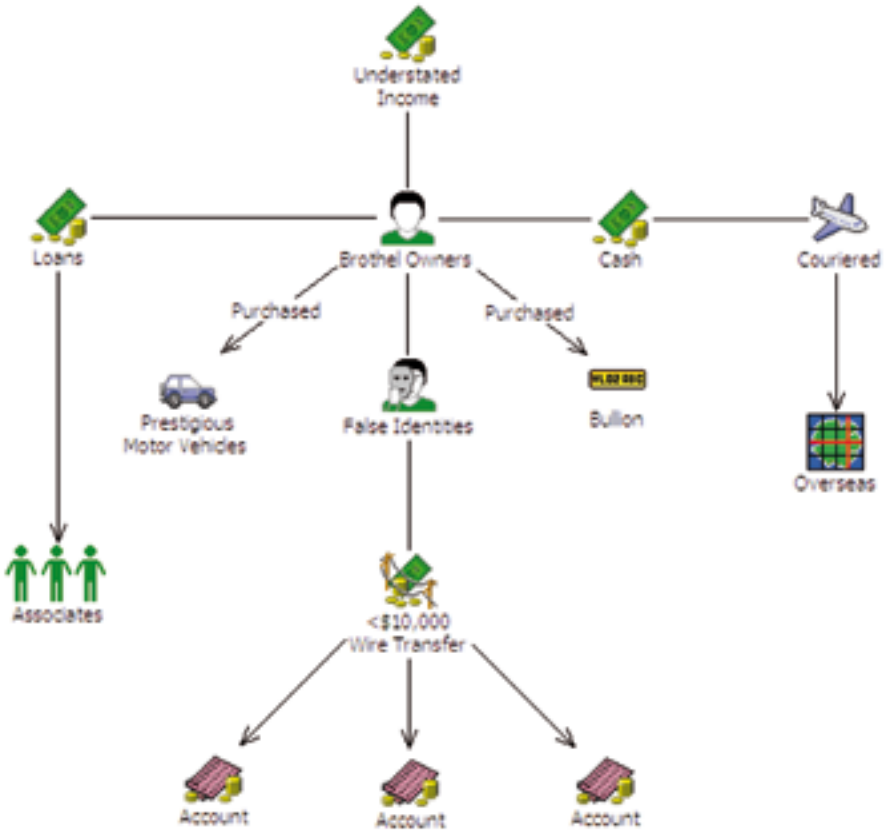
[9] Financial Action Task Force on Money Laundering (FATF), 'Report of Money Laundering Typologies 2002-2003', *<http://www.fatf-gafi.org/dataoecd/29/33/34037958.pdf>.*

Case 28

Understated income siphoned to overseas bank accounts

In an organised tax evasion scam, two brothel owners withheld cash takings, understated their income and siphoned funds to overseas bank accounts over a three-year period. The offenders obtained false identification documents and structured the transfers using false identities and names of associates. One of the offenders then changed his method of laundering the cash payments, possibly as a result of his growing awareness of the role and function of AUSTRAC. Methods included the physical carriage of cash out of Australia, the purchase of bullion, acquisition of prestigious motor vehicles, and loans to associates.

Offence	Tax evasion
Customer	Business
Industry	Authorised deposit-taking institutions, bullion services
Channel	Physical (face-to-face)
Jurisdiction	International
Designated service	Accounts, bullion trading, electronic funds transfer, cash carrying and payroll services
Indicators	Physical carriage of cash / bnis out of Australia Purchase of high value assets, e.g. prestige motor vehicles Structuring of wire transfers



Case 29

Smuggling of gold to evade tax

Paul was a well-known customer of a European bank. On a number of occasions he purchased gold bullion from the bank in ingots of 1 kilogram with the explanation that he was buying the gold to export directly to a foreign company. Paul transported the gold out of the bank by himself after each transaction. In a single year he purchased a total of more than 800 kilograms of gold with a value of more than USD7 million. The gold was paid for by funds drawn from his company account. The bank was also able to see that at regular intervals funds were transferred into the account from another company in a neighbouring country, as one would expect. However, Paul's actions in transporting the gold himself seemed unusual to the bank, and the bank officials decided to disclose their concerns to the national FIU. The FIU researched Paul and his company within various law enforcement intelligence databases, but no obvious link to criminality could be found. However, the scale of the gold purchases justified a formal investigation by the FIU, and further enquiries were undertaken.

These enquiries revealed that Paul was not in fact selling the gold to a foreign company as claimed. Before buying the gold, Paul always met with a foreign citizen named Daniel. Although they drove to the bank together in Paul's car, Daniel never entered the bank. After Paul purchased the gold, they drove to Daniel's car and hid the gold in the boot. Then Daniel drove back to his own country, crossing the border without declaring the bullion at Customs and therefore avoiding paying import duties. Once in his own country, Daniel handed the gold over to Andrew, who delivered it to another company for sale on the open market. A proportion of the profits from the sale of the gold was transferred back to Daniel's company, from which he drew the next tranche of funds to purchase more gold. The amount of additional profit generated by this simple tax evasion scheme was substantial.

At the time of writing, criminal proceedings for money laundering in conjunction with tax evasion were being raised against Paul, Daniel and Andrew. The smuggling operation was estimated to have caused tax losses to the government of some USD1 million. Because the proceeds from selling the smuggled gold were obtained illegally, the judicial authorities in the FIU's country have also begun criminal proceedings against the individuals involved.[10]

Offence	Tax evasion
Customer	Individual
Industry	Bullion services, authorised deposit-taking institutions
Channel	Physical (face-to-face)
Jurisdiction	International
Designated service	Accounts, bullion trading, electronic funds transfer
Indicators	Gold transported by the individual but purchased with funds drawn from a company account Large purchases of gold with the transportation of the gold conducted by the individual Sale of large amounts of gold from an individual Third party present for all transactions but does not participate in the actual transaction

[10] 'FIU's in Action' 100 Cases from the Egmont Group, Concealment within Business Structures (Chapter), *<http://www.egmontgroup.org/library_sanitized_cases.html>.*

Case 30

Retail gold purchases serves as direct method of laundering

A foreign national used the services of a bureau de change to buy 265 ingots of gold with a total value of about USD2 million paid in cash. These transactions took place over a period of 18 months. The buyer, who did not have a bank account, alternated temporary jobs with periods of unemployment, suggesting that he was acting on behalf of a third party, whether a natural or legal person, who was probably involved in drug trafficking. The facts were forwarded to the prosecutor, and an investigation is ongoing.[11]

Offence	Money laundering
Customer	Individual
Industry	Bullion services, money service businesses
Channel	Physical (face-to-face)
Jurisdiction	International
Designated service	Bullion trading, foreign exchange services
Indicators	Large amounts of cash to purchase to gold Unexplained wealth inconsistent with economic situation Use of a third party to purchase gold

[11] Financial Action Task Force on Money Laundering (FATF), 'Report of Money Laundering Typologies 2002-2003, Case 15, <*http://www.fatf-gafi.org/dataoecd/29/33/34037958.pdf*>.

Case 31

Purchasing and reselling of precious metals and jewellery for settling of illegal alternative remittance payments

Originator A in Japan, upon a remittance request from a client residing in Japan, directs him to transfer the amount of remittance and a commission to the bank account of A.

- Payer B who is in another country receives payment directions from A by the internet, the telephone and facsimile, and pays the specified amount of money to the designated recipient out of the stocked money.
- A carries out cross-border remittance of the money collected in Japan regularly to the bank account of accomplice C in the other country.
- C takes out the money from his bank account and purchases precious metals and jewellery in that country. C carries these precious metals and jewellery into another country by means of wearing them on his body, putting them into carry-on bags, etc., and hands them to B.
- B cashes the precious metals and jewellery.[12]

Offence	Illegal alternative remittance
Customer	Individual
Industry	Bullion services, remittance services, authorised deposit-taking institutions
Channel	Electronic (internet), fax / telephone
Jurisdiction	International
Designated service	Accounts, designated remittance arrangement, bullion trading
Indicators	Purchasing high value assets (precious metals and jewellery) using cash Regular sale of large amounts of precious metals and jewellery

[12] APG Typologies Working Group Asia/Pacific Working Group on Money Laundering (APG) 'Annual Typologies Report 2003-2004', Section 1: Summary of Regional Methods and Trends, p. 7, <*http://www.apgml.org/frameworks/docs/4/APG%20Typologies%20Yearly%20Report%202003-04%20_public_.pdf*>.

Case 32

Gold suppliers implicated in drug proceeds

In January 1999, the El Dorado Task Force (EDTF), under the auspices of the United States' Immigration and Customs Enforcement (Special Agent in Charge)/New York, initiated Operation Meltdown, an undercover investigation targeting gold suppliers in the New York area. The EDTF received information from a documented informant that numerous businesses in the New York area were laundering narcotics proceeds through the sale of gold and other precious metals. According to the information, a jeweller would receive narcotics proceeds (cash) and would either provide gold pellets (shots) or melt and mould the equivalent value of gold into various items.

The EDTF identified jewellers that moulded gold into the following items: bolts, nuts, cones and wrenches. In some cases the gold was secreted into jewellery machines which where then shipped to Colombia. Once the gold was received in Colombia, it was resold for cash, thus completing the laundering cycle.

During the course of the investigation, confidential sources of information and undercover agents delivered purported narcotics proceeds to several jewellery stores and received either gold shot or disguised gold in return. Undercover agents and confidential sources delivered more than USD1 million dollars in cash to different wholesale and retail businesses. In return for the cash, the undercover agents and cooperating witnesses received more than 100 kilograms of gold, which they told the suspects would be smuggled to Colombia.

Immigration and Customs Enforcement (Special Agent in Charge)/New York agents assigned to EDTF conducted a takedown that included the arrest of 11 suspects for money laundering violations and execution of eight search warrants. To date Operation Meltdown has seen 23 individuals arrested and six guilty pleas under Title 18 USC 1956 Violations have been entered. To date, 140 kilograms of gold (estimated value of USD1.4 million); approximately USD1 million in loose diamonds; USD2.8 million in currency; 118 kilograms of cocaine; three moulds in the shape of cones, wrenches and screws; six guns and two vehicles have been seized.[13]

Offence	Drug distribution, money laundering
Customer	Business, individual
Industry	Bullion services
Channel	Agent / third party, physical (face-to-face)
Jurisdiction	International - Colombia
Designated service	Bullion trading, cash carrying and payroll services
Indicators	Cash used to purchase large amounts of gold Regular sale of large amounts of gold with payment received in cash

[13] APG Typologies Working Group Asia/Pacific Working Group on Money Laundering (APG) 'Annual Typologies Report 2003-2004', Section 1: Summary of Regional Methods and Trends, p. 7, <*http://www.apgml.org/frameworks/docs/4/APG%20Typologies%20Yearly%20Report%202003-04%20_public_.pdf*>.

Case 33

Currency exchange business used to launder funds

A multi-million dollar money laundering syndicate was dismantled following the dissemination of information held by AUSTRAC to a joint task force. The investigation into the activities of a currency exchange business culminated in the arrest of four people who were charged with numerous money laundering and structuring offences.

At the initial phase of the investigation, the suspicious activities of the currency exchange business and associated persons were detected through FTR information. Financial investigators interrogated the AUSTRAC database throughout the course of the investigation with significant results. Searches of account numbers were able to assist in establishing relevant details of transactions and identifying associates. A number of SUSTRs relevant to the investigation highlighted transactions that were alleged to have been deliberately structured to fall below the cash transaction reporting threshold in an attempt to avoid reporting obligations.

A number of search warrants were executed simultaneously on the premises of the currency exchange business and the persons associated. A total of AUD47,500 was seized during the execution of the search warrants and approximately AUD247,000 in assets are the subject of Commonwealth restraining orders.

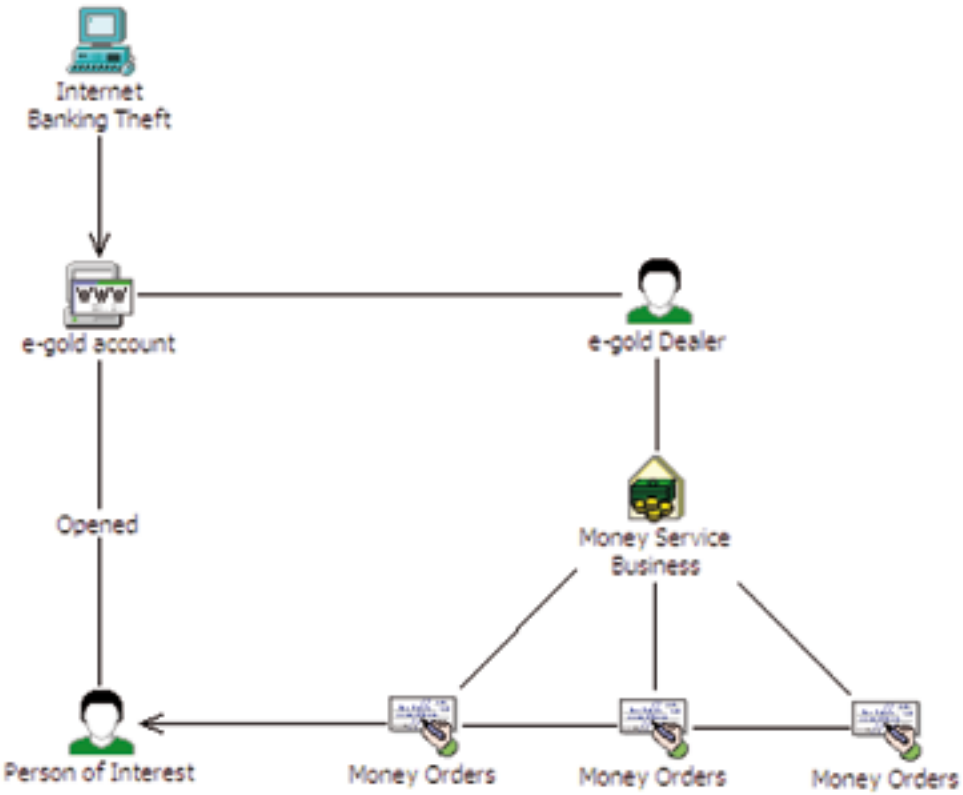
Offence	Structuring, money laundering
Customer	Business, individual
Industry	Money service businesses, authorised deposit-taking institutions
Channel	Physical (face-to-face)
Jurisdiction	Domestic
Designated service	Accounts, foreign exchange services
Indicators	Structuring of cash transactions

Case 34

E-gold account used to facilitate internet fraud

A young person opened an e-gold account to enable him to receive the proceeds of internet banking thefts from an offshore associate. He then attempted to redeem the value of the e-gold by requesting the e-gold dealer to provide him with postal orders. In an effort to conceal his identity he informed the cash dealer that he had lost his passport and requested that the dealer call a money service business and inform them that a person matching his description would present himself to collect the money orders at a particular time. It is believed that he was not going to send money offshore but would keep the proceeds for himself. He has been arrested and prosecuted.

Offence	Fraud
Customer	Individual
Industry	Money service businesses, authorised deposit-taking institutions
Channel	Electronic (internet)
Jurisdiction	Domestic
Designated service	Accounts, payment orders and stored value cards
Indicators	Purchase of multiple money orders

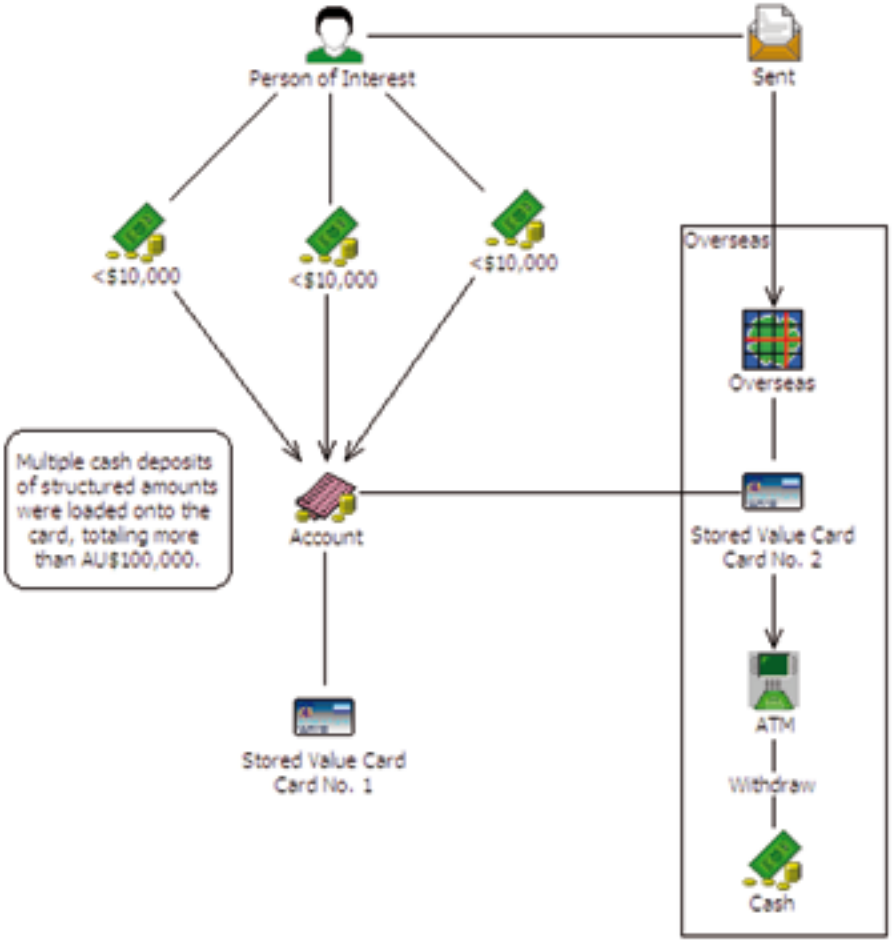


Case 35

Stored value cards sent offshore to withdraw crime proceeds

The holder of a stored value card was found to have regularly loaded value by paying cash just below the AUD10,000 reportable threshold. A second card linked to the same account was sent overseas where the funds were withdrawn through ATMs. The process was repeated, with more than AUD100,000 laundered through the scheme.

Offence	Money laundering
Customer	Individual
Industry	Money service businesses, authorised deposit-taking institutions
Channel	Mail, physical (face-to-face)
Jurisdiction	International
Designated service	Accounts, payment orders and stored value cards
Indicators	Cash deposited domestically with the funds subsequently withdrawn from ATMs offshore Regular use of stored value card to withdraw funds overseas Structuring of cash deposits



Case 36

Bank drafts purchased in third party names to evade tax

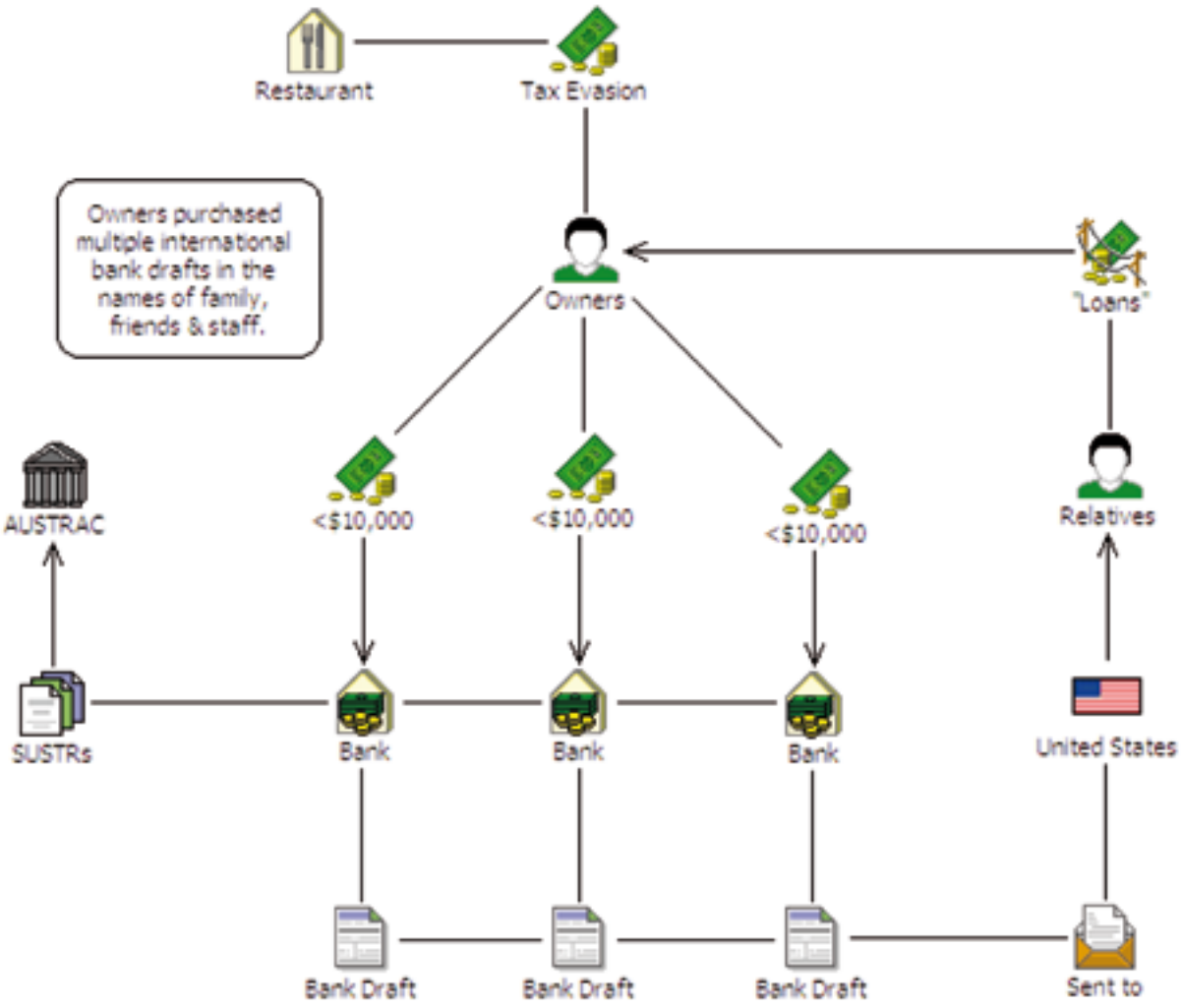
An investigation was initiated based on the receipt of anonymous information that indicated a restaurant was paying wages in cash and evading taxation requirements.

Auditors conducted AUSTRAC searches revealing SUSTRs which indicated that one of the owners of the restaurant was purchasing multiple international bank drafts with cash, in amounts just below the AUD10,000 reportable threshold. The drafts were purchased in the names of family, friends and staff members and signed with different signatures. Based on this information it was decided to audit the taxpayer and the business.

As the investigation progressed, examination of evidence confirmed that the restaurant owner was purchasing USD bank drafts with cash in false names and sending these offshore to relatives overseas.

Search warrants were executed and the information obtained, together with banking records and an extensive analysis of the business, clearly indicated that the owners had been systematically skimming profits from the restaurant and manipulating the cash registers to give incorrect sales readouts. The skimmed funds were then sent to relatives overseas. The money was returned to Australia as 'loans' and interest on these 'loans' was claimed as tax deductions. Amended assessments were issued on all the business owners resulting in approximately AUD8.4 million in tax and penalties.

Offence	Tax evasion
Customer	Business
Industry	Authorised deposit-taking institutions, remittance services
Channel	Mail, physical (face-to-face)
Jurisdiction	International
Designated service	Debt instruments, loan services, electronic funds transfer
Indicators	Structuring the purchase of international bank drafts Frequent loans sent from relatives Frequent remittance of bearer negotiable instruments, e.g. bank drafts offshore U-turn transactions occurring with funds being transferred out of Australia and then portions of those funds being returned


Restaurant
Tax Evasion
Owners purchased multiple international bank drafts in the names of family, friends & staff.
Owners
"Loans"
AUSTRAC
<$10,000
<$10,000
<$10,000
Relatives
SUSTRs
Bank
Bank
Bank
United States
Bank Draft
Bank Draft
Bank Draft
Sent to

Case 37

Syndicate travels to offload drug proceeds through money exchange

A syndicate was involved in a sophisticated MDMA importation network. The proceeds of the importation were collected in cash and various arrangements made for the funds to be delivered overseas.

One group travelled between Sydney and Brisbane stopping at various towns to visit different branches of banks. They purchased bank drafts for amounts under AUD10,000 and by the end of the trip had accumulated over AUD1 million in bank drafts. These drafts were then carried to Singapore and negotiated through a Singapore money exchange for Euros and US dollars.

Cash couriers were also used and would travel with amounts under the AUD10,000 reporting threshold to Singapore. On arrival in Singapore the funds were dispersed in a number of ways. This included the purchase of USD100 traveller's cheques which were given to the principals of the syndicate. Funds were also deposited directly into the principal's bank accounts in Hong Kong or into other accounts in Singapore that syndicate members had established in the names of companies controlled by the syndicate.

Offence	Drug trafficking
Customer	Individual
Industry	Money service businesses, authorised deposit-taking institutions
Channel	Physical (face-to-face)
Jurisdiction	International - Singapore
Designated service	Debt instruments, foreign exchange services, cash carrying and payroll services
Indicators	Bank drafts cashed in for foreign currency, e.g. Euros, USD Cash used to purchase multiple bank drafts Multiple transactions of a similiar nature conducted in different locations Numerous bank drafts purchased domestically and subsequently deposited internationally Structuring the purchase of international bank drafts Physical carriage of cash / BNIs out of Australia

Case 38

CEO assists in structuring of traveller's cheques

This case involved currency exchange and travellers' cheque fraud conducted by two persons being the main person of interest and the then Chief Executive Officer (CEO) and Director of a finance company. The person of interest attended the finance company several times to meet with the CEO which resulted in two transactions being conducted. The transaction involved the exchange of Australian currency in excess of AUD10,000 for American currency and travellers' cheques. When the person received travellers' cheques, he completed the required travellers' cheques sales documentation in false names and did not sign the travellers' cheques. The transactions had been recorded as separate amounts, all less than AUD10,000, even though a much larger amount had been initially provided by the target. Computer records from the finance company showed that the larger transaction of an amount over AUD10,000 was broken into smaller amounts under AUD10,000. Each amount under AUD10,000 was entered into the company computer system in different exchange rates in an attempt to conceal the true amount of the transaction and thus avoid the reporting requirements of the FTR Act.

Offence	Fraud
Customer	Business, individual
Industry	Money services businesses
Channel	Physical (face-to-face)
Jurisdiction	Domestic
Designated service	Foreign exchange services
Indicators	Large amounts of currency exchanged for traveller's cheques Structuring of cash to purchase traveller's cheques

Case 39

Financial adviser involved in drug distribution network

A registered financial adviser was involved in a drug distribution network. Documents seized when his property was raided showed that the financial adviser had been laundering the proceeds of his drug crime through his business and property dealings.

He bought properties and obtained falsely high valuations for them and then as soon as they settled he would sell them on to his associates. His company facilitated the loan application, including providing false documents and references. It is believed that he had contacts in the industry to assist with processing loan applications.

The associate signed a Deed of Agreement relinquishing all interest in the property to the target and on settlement date the two contracts would settle simultaneously. The excess money was used to pay off other real estate interests and drug business. This method of laundering money meant that the targets had effective control over numerous properties without ever appearing on any government documents as having an interest. It appears that this scheme had not been operating for long as most of the properties were significantly encumbered.

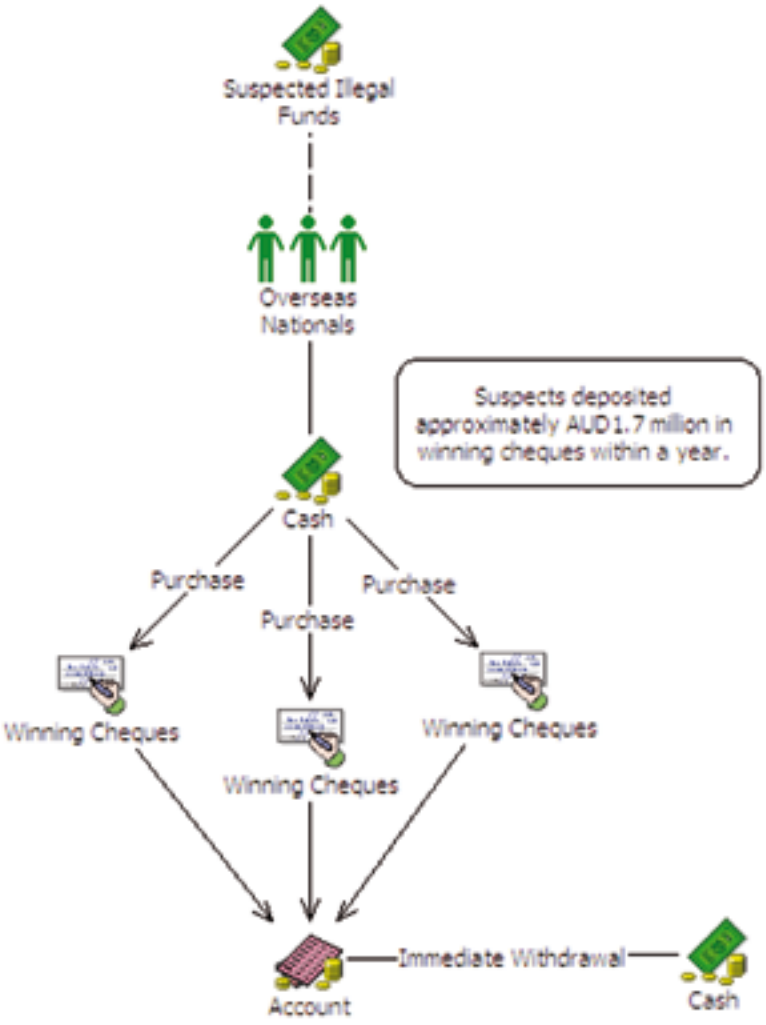
Offence	Drug distribution, money laundering
Customer	Individual and business
Industry	Financial advisors and planners, authorised deposit-taking institutions
Channel	Agent / third party
Jurisdiction	Domestic
Designated service	Loan services, Australian financial services license
Indicators	Frequent purchase and immediate sale of high value assets, e.g. property

Case 40

Overseas nationals purchase winning jackpots with illegal proceeds

AUSTRAC referred a matter relating to a group of overseas nationals buying winning jackpots from other persons at various clubs in Sydney. The suspects deposited approximately AUD1.7 million in winning cheques within a year, immediately withdrawing money in cash afterwards. The source of the funds used to buy winning jackpots was suspected to be from illegal means.

Offence	Money laundering
Customer	Business, individual
Industry	Gambling services, Authorised deposit taking institution
Channel	Physical (face-to-face)
Jurisdiction	Domestic
Designated service	Accounts - chequebook facility, money on deposit, gambling services
Indicators	Frequent deposits of winning gambling cheques followed by immediate withdrawal of funds in cash



Case 41

Casino used as preferred method to launder millions

AUSTRAC information identified a number of bank accounts and businesses used to launder proceeds derived from alleged criminal activities. It was also found that the alleged money launderers were using the casino as a preferred method of laundering millions of dollars accumulated from their activities. The methods used to launder the money included purchasing and cashing out chips without playing, putting funds through slot machines and claiming credits as a jackpot win and playing games with low returns but higher chances of winning.

Offence	Money laundering
Customer	Individual
Industry	Authorised deposit-taking institutions, gambling services
Channel	Physical (face-to-face)
Jurisdiction	Domestic
Designated service	Accounts, gambling services
Indicators	Frequently playing games with low returns but with higher chances of winning Inserting funds into slot machines and immediately claiming those funds as credits Purchasing and cashing out casino chips with no gaming activity

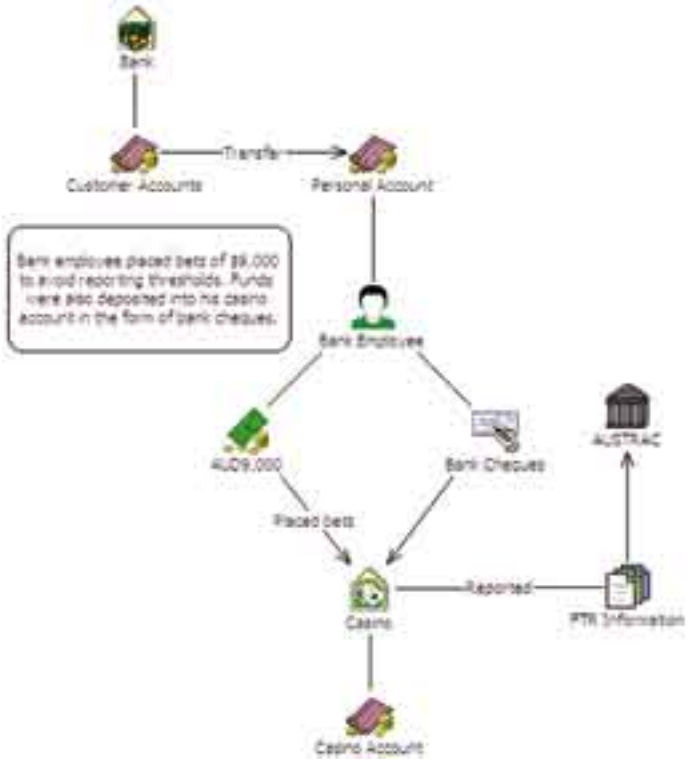
Case 42

Bank employee gambles millions from clients' accounts

An investigation into a bank employee who gambled millions of dollars from clients' accounts was initiated as a direct result of AUSTRAC information. The suspect used his knowledge of the bank's internal procedures to discreetly transfer funds from customers' accounts to his own personal account.

Over a period of time, these funds were deposited into his casino account in the form of bank cheques made out in his name. The casino reported the regular deposit of bank cheques to AUSTRAC. The same casino had also previously lodged reports when the suspect had placed bets of AUD9,000 to avoid the AUD10,000 reporting threshold. As a result of the investigation, the suspect was charged with three counts of money laundering and 37 counts of fraud.[14]

Offence	Fraud
Customer	Individual
Industry	Authorised deposit-taking institutions, gambling services
Channel	Physical (face-to-face)
Jurisdiction	Domestic
Designated service	Accounts, debt instruments
Indicators	Structuring the placement of betting transactions Unexplained wealth inconsistent with economic situation



[14] 'FIU's in Action' 100 Cases from the Egmont Group, Misuse of Legitimate Businesses (Chapter), <*http://www.egmontgroup.org/library_sanitized_cases.html*>.

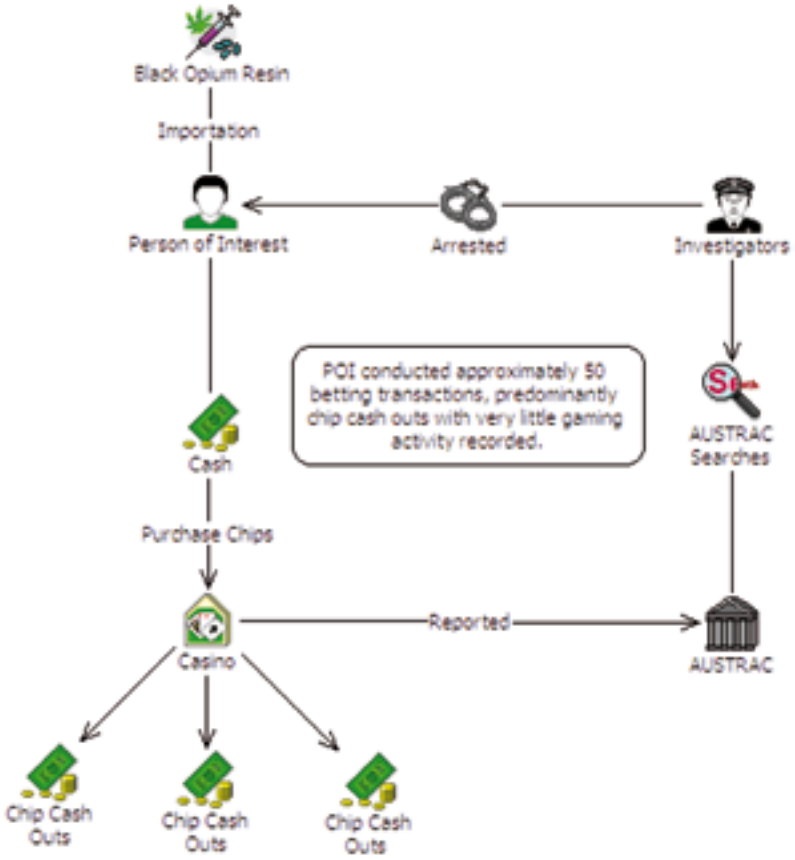
Case 43

Proceeds of drugs used to purchase chips and claim funds as winnings

A cargo consignment addressed to a person of interest contained approximately 3.4 kilograms of black opium resin, concealed within the contents. The person was arrested when attempting to collect the consignment. Search warrants were then conducted on the person's two premises where a further six sticks of opium were located.

Following the arrest, searches were conducted on the AUSTRAC database which found that the person was a regular patron of a casino, having conducted approximately 50 betting transactions, predominantly chip cash outs totalling AUD890,000. Very little casino gaming play was recorded for the person and it was assumed that he used the proceeds from previous importations to purchase chips and claim the funds as winnings.

Offence	Drug importation
Customer	Individual
Industry	Gambling services,
Channel	Physical (face-to-face)
Jurisdiction	Domestic
Designated service	Gambling services
Indicators	Large chip cash outs with little casino gaming play



Case 44

Criminal attempts to launder fraud proceeds through the diamond market

A known criminal who had benefited financially from a fraud that took place in another country attempted to send money to jewellers to purchase precious stones. The financial institution holding the account had been concerned about the individual for some time and had made several suspicious transaction reports to the FIU. The client attempted to send USD8.2 million to the jewellers. Before this took place the bank took the commercial decision to freeze the accounts. The law enforcement agency made initial investigations and was satisfied that the attempt to buy precious stones had been an attempt to launder the proceeds of the fraud.[15]

Offence	Fraud, money laundering
Customer	Individual
Industry	Bullion services, authorised deposit-taking institutions
Channel	Electronic
Jurisdiction	International
Designated service	Accounts, electronic funds transfer, bullion trading
Indicators	An unusually large transfer of money from a individual to a business

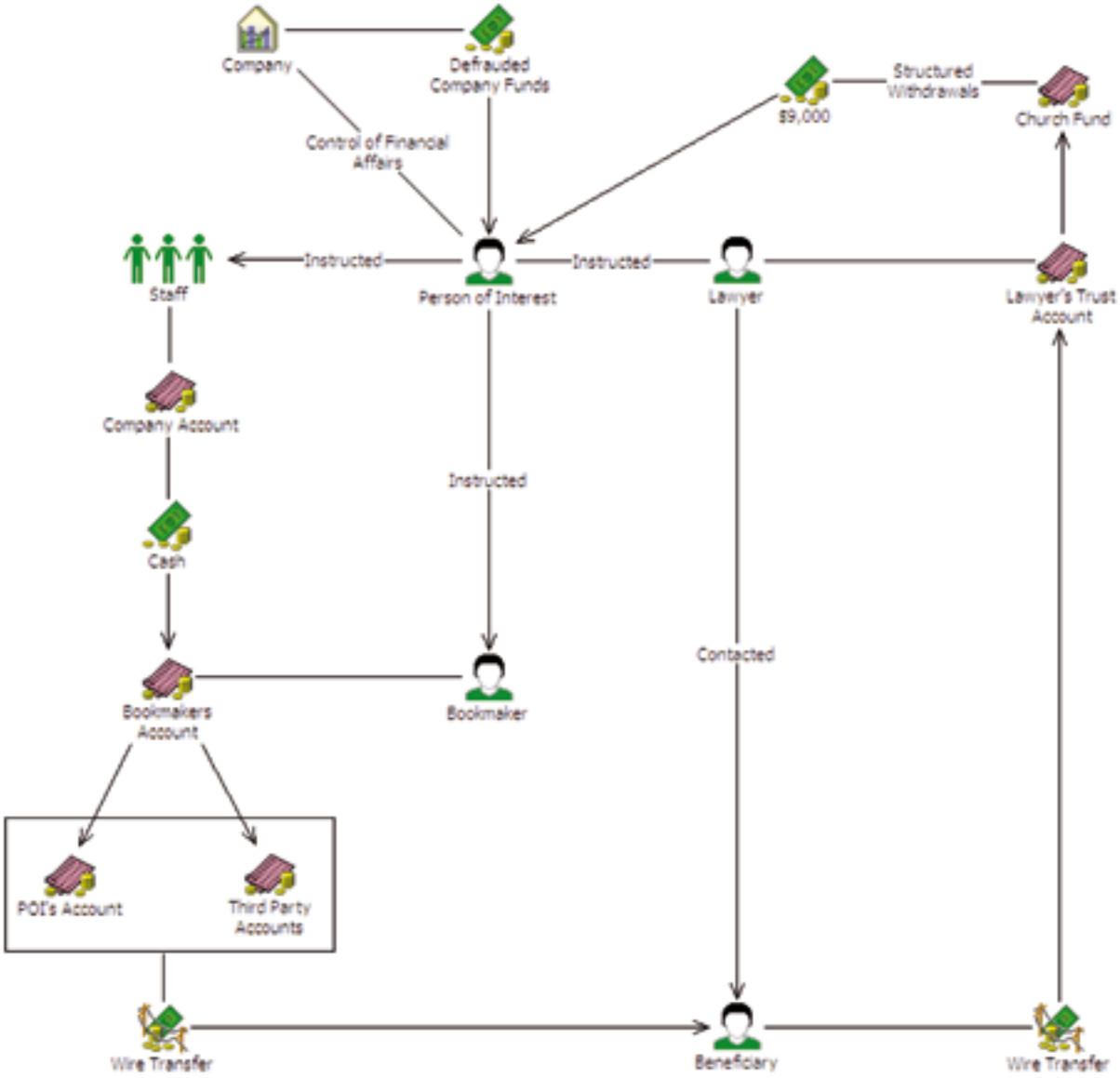
[15] Financial Action Task Force on Money Laundering (FATF), 'Report of Money Laundering Typologies 2002-2003', *<http://www.fatf-gafi.org/dataoecd/29/33/34037958.pdf>*.

Case 45

Financial controller launders funds through bookmaker

A person in control of a corporation's financial affairs abused this position of trust by defrauding the company. The person authorised and instructed staff to make electronic funds transfers from the company to his bookmakers' accounts. He then instructed the bookmakers to direct excess funds and winnings from their accounts to his account or third party accounts, and instructed bank officers to transfer funds from his accounts internationally. In order to layer and disguise the fraud, he instructed his lawyer to contact the beneficiary of the original international transfers to return the payments via wire transfers into the lawyer's trust account. Approximately AUD450,000 was returned in one international transfer to the lawyer's trust account. The lawyer then transferred AUD350,000 to a church fund in an attempt to further hide the assets and was preparing to transfer the funds to an overseas account. To access these funds the person made structured withdrawals of AUD9,000 each within a nine day period.

Offence	Fraud
Customer	Business, individual
Industry	Gambling services, professional services, authorised deposit-taking institutions
Channel	Agent / third party, electronic
Jurisdiction	International
Designated service	Accounts, gambling services, electronic funds transfer
Indicators	Elaborate movement of funds through different accounts Funds transferred to a charity fund Structuring of cash withdrawals Transfers from company accounts to private betting accounts Transferring funds into third party accounts Using third parties to undertake wire transfers U-turn transactions occurring with funds being transferred out of Australia and then portions of those funds being returned Use of gatekeepers, e.g. accountant and lawyers to undertake transactions


Company
Defrauded Company Funds
Control of Financial Affairs
$9,000
Structured Withdrawals
Church Fund
Staff
Instructed
Instructed
Person of Interest
Lawyer
Lawyer's Trust Account
Company Account
Instructed
Cash
Contacted
Bookmakers Account
Bookmaker
POI's Account
Third Party Accounts
Wire Transfer
Beneficiary
Wire Transfer

Case 46

Drug proceeds used to repay finance loans

A newly appointed credit manager at a car loan company was concerned about one of his customers. The customer had recently bought a luxury sports car worth about USD55,000. He obtained a five-year loan for USD40,000 through the credit company, and had paid the balance in cash.

The credit manager undertook some checks against historical records and discovered that the customer had several loans over the previous six years; all for the same amount of money and all with a large proportion of cash as a deposit. More significantly, in a number of the cases the loans had been repaid early in cash. The credit manager decided to report his concern to the senior management of the loan company. After assessing the facts, the management decided to disclose the case to the national FIU.

The FIU searched the disclosure against their databases, and very quickly linked the customer to a long established criminal organisation. The FIU forwarded the disclosure to an operational team in the police force, which was already targeting the organisation. The team obtained a court order to examine all relevant records at the loan company. It became clear that the customer was selling the newly bought cars on to private buyers and small garages, and obtaining cheques from these new owners. Further investigation revealed a single bank account into which all cheques gained from the sale of the car were paid.

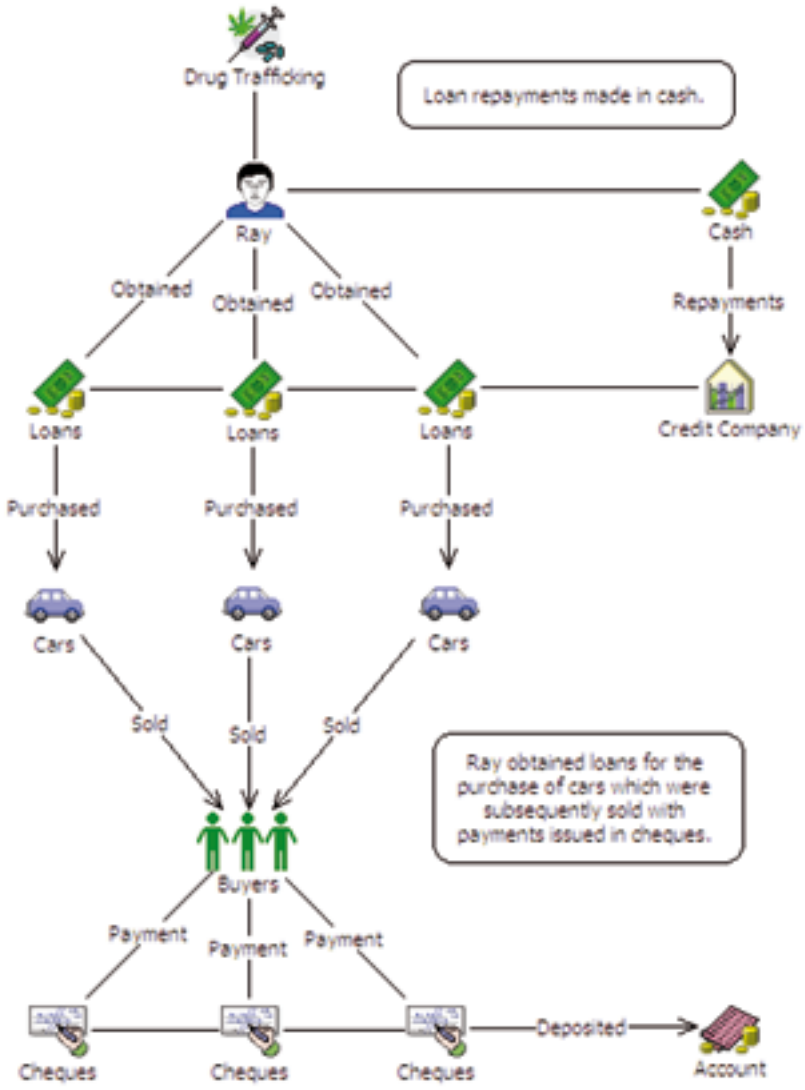
It appeared that the customer was working at the criminal organisation's laundering division. He was entering cash from the sale of drugs into the banking system by means of the initial cash deposit to the car loan firm, as well as clearing the loan with a second cash sum. The cheques from customers and small businesses, to whom he sold the cars, would appear to any bank employee examining the account to be legitimate sources of income. The loss made on both the loan and the drop in resale value the criminal organisation simply saw as a cost to be borne in exchange for cleaned funds that would attract no law enforcement attention.

Because of the identification of the bank account, an accurate assessment of the criminally laundered funds could be made. The financial information collected allowed the financial investigators on the operational team to produce a more accurate benefit of crime statement.

An additional USD300,000 was confiscated as a result of the information generated by the initial disclosure.[16]

[16] 'FIU's in Action' 100 Cases from the Egmont Group, *<http://www.egmontgroup.org/library_sanitized_cases.html>.*

Offence	Drug trafficking, money laundering
Customer	Individual
Industry	Authorised deposit-taking institutions, designated non financial businesses and professions
Channel	Physical (face-to-face)
Jurisdiction	International
Designated service	Accounts, accounts - chequebook facility, loan services
Indicators	Frequent early repayments of loans Large cash deposits into company accounts Multiple cheques cashed into the one bank account Multiple loans obtained over a short period of time with repayments made in cash Obtained loan and repaid balance in cash Purchasing high value assets (motor vehicles) followed by immediate resale with payment requested via cheque



Case 47

Solicitor coordinates u-turn transactions to legitimise funds

An Australian-based solicitor structured funds to an offshore account in Hong Kong. At times it is believed that he actually carried cash to Hong Kong. His colleague, a Hong Kong-based solicitor, arranged for the creation of offshore companies in the British Virgin Islands and bank accounts in Hong Kong to receive structured funds from Australia. These funds were then transferred to other countries by the Hong Kong-based solicitor to hide from authorities or returned to Australia in order to appear legitimate.

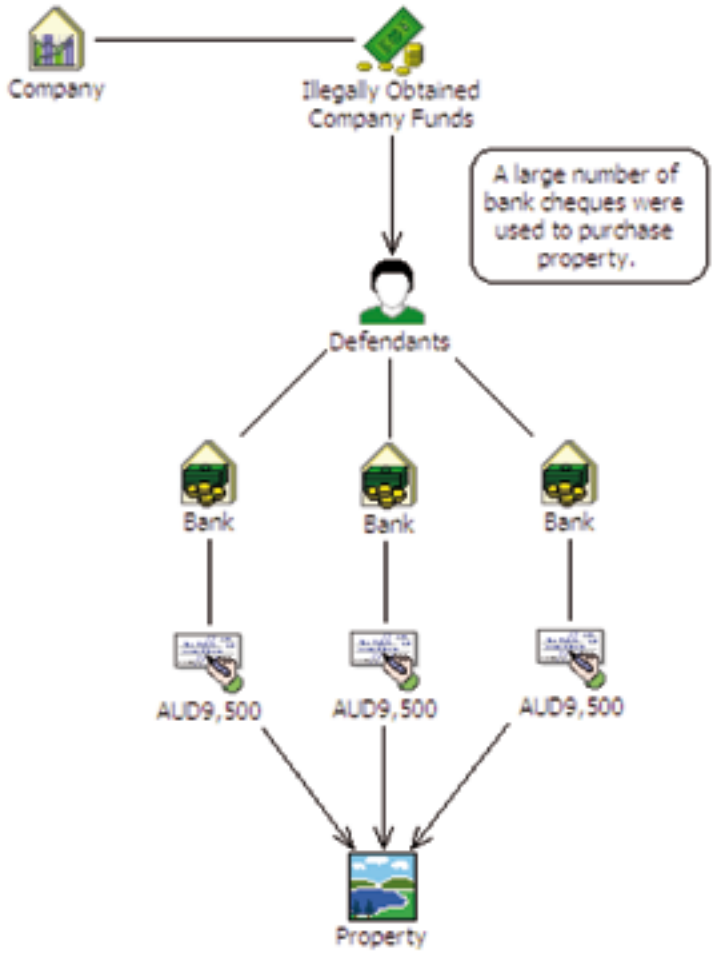
Offence	Money laundering
Customer	Business, foreign entity, individual
Industry	Professional services, authorised deposit-taking institutions
Channel	Agent / third party, electronic, physical
Jurisdiction	International – Hong Kong, British Virgin Islands
Designated service	Accounts, electronic funds transfer, cash carrying and payroll services
Indicators	Physical carriage of cash / BNIs out of Australia Structuring of wire transfers Use of gatekeepers (solicitor's) to conduct wire transfers U-turn transactions occurring with funds being transferred out of Australia and then portions of those funds being returned Wire transfers to tax haven countries

Case 48

Structured bank drafts to purchase property

AUSTRAC information assisted in identifying real estate which had been purchased with illegally obtained company funds. A large number of bank cheques in the amount of AUD9,500 were used by the defendants to purchase the property. These bank cheques were purchased over a period of days by the defendant from numerous banks in the suburbs of Perth.

Offence	Fraud
Customer	Business, individual
Industry	Professional services, authorised deposit-taking institutions
Channel	Physical (face-to-face)
Jurisdiction	Domestic
Designated service	Accounts – chequebook facility, debt instruments
Indicators	Multiple transactions of a similar nature at numerous branches within a short space of time Structuring the purchase of bills of exchange, e.g. bank cheques Structuring the purchase of a high value asset, e.g. property



Case 49

Gatekeepers used in web of criminal activity

This case involved the production of large quantities of amphetamines in several states of Australia. The suspects laundered most of the proceeds of the manufacture of the amphetamine with the assistance of Australian entities. The Australian-based entities deposited cash supplied to them by the wife of the main suspect (usually in structured amounts under the AUD10,000 reporting threshold) into their own accounts. The funds were drawn from the accounts using cheques payable to the suspect's wife or a company or business over which she and her husband had control. The Australian-based entities were also instructed to send some of the money to overseas accounts by international wire transfer. Money was often moved through different accounts, before being wire transferred offshore. The case involved approximately AUD5 million.

Over AUD1 million was also laundered by the group through an accountancy firm. The firm was initially approached on the basis that one of the suspects had substantial funds overseas, which he wished to repatriate to Australia. At the time, the person was a bankrupt and money could not be held in his own name. Advice was sought from the accountants to devise a structure to enable the repatriation of the funds and acquisition of real estate.

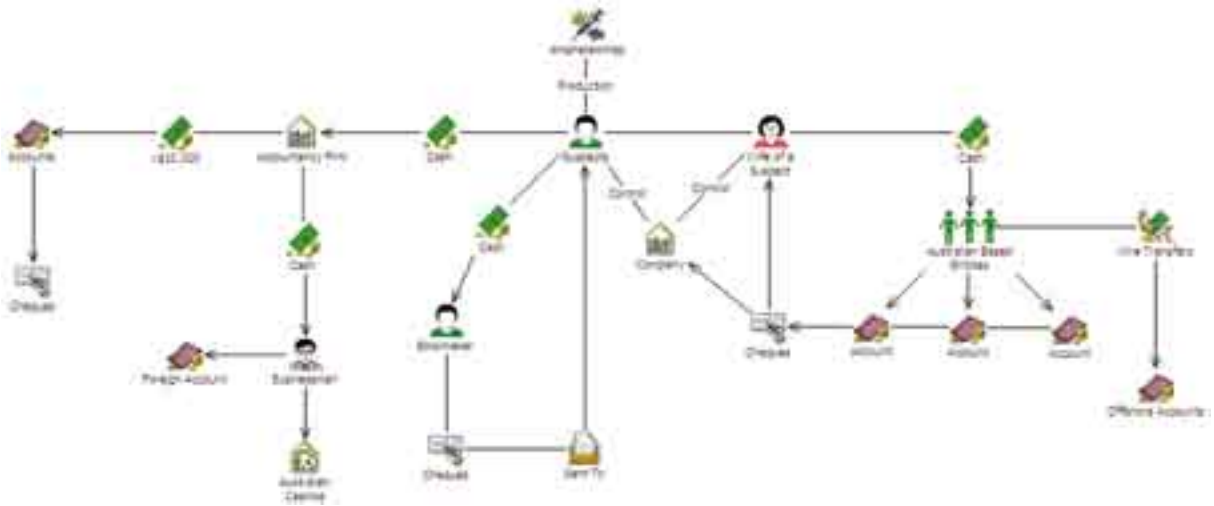
The accountants were given AUD20,000 to be used as a deposit on a real estate purchase. The accountants were aware of reporting thresholds and deposited the money into bank accounts in amounts less than the AUD10,000 reporting threshold. The accountants recommended a number of money laundering schemes to the principals of the drug ring. Their standard approach was to launder the money into a number of bank accounts in amounts less than the reporting threshold of AUD10,000 and to then draw cheques on those accounts.

The accountants used 15 different bank accounts to receive the cash. These included personal accounts, the bank accounts of others, unwitting family members, the accountants' business accounts (including trust accounts), and the bank accounts of corporate entities established for the purpose. Two other methods used to launder the funds were use of bookmakers and gamblers.

In the case of the bookmakers, the method was to attend race days with substantial amounts of cash. The person would seek out a bookmaker he knew, express his discomfort at carrying such a large amount in cash and ask them to hold his cash for him until he either used it for bets or collected it at the end of the day. He would then leave it with the bookmaker and deliberately not collect it at the end of the day. Early the following week he would contact the bookmaker and ask him to post him a cheque for the money.

The accountants had a business association with a wealthy businessman who was a frequent gambler at Australian casinos. The accountants approached the businessman and offered to provide cash at short notice to him or his associates for gambling at casinos. The accountants offered to accept 95 per cent of the value of the cash they provided on the basis that the gambler later repaid the money by depositing money into a foreign bank account which had been set up for the purpose.

Offence	Drug production
Customer	Business, individual
Industry	Professional services, authorised deposit-taking institutions, gambling services
Channel	Agent / third party, physical (face-to-face)
Jurisdiction	Domestic
Designated service	Accounts, electronic funds transfer, accounts - cheque book facility, gambling services
Indicators	Cash deposits given to gatekeepers (accountants) to place in the gatekeepers or associates accounts Cheques made out regularly to companies and individuals not linked to the account Deposit of gambling proceeds into a foreign bank account Leaving large amounts of cash with a bookmaker and requesting a cheque in return Purchase of high value assets, e.g. real estate Use of gatekeepers, e.g. accountant and lawyers to undertake transactions Use of a third party to gamble proceeds through casinos Use of third parties to deposit cash and conduct wire transfers



Case 50

Layering funds to evade tax

A person was involved in a multi million dollar tax fraud undertaken through lodging fraudulent Goods and Services Tax (GST) claims. To achieve the fraud, he used a number of stolen and false identities and forged documentation to open and operate bank accounts, obtain credit cards, register companies and open serviced and virtual offices.

The companies' bank accounts received the proceeds of the fraud and subsequently transferred the funds into other company accounts and various stolen identity accounts. These funds were moved constantly to have the appearance of being legitimate. The person also falsified trade documents to launder money between the companies controlled by him. The funds would be moved from one company to the other under the guise of legitimate business. He also employed international accounting firms using stolen identities and provided forged documentation to help undertake the fraud. The person used these gatekeepers to help distance himself from the underlying fraud. Once the proceeds had been layered, he then withdrew funds using ATMs, business cheques, credit cards, cash cheques, electronic debit system, direct transfers to other parties and cash withdrawals. The cash withdrawals were varied in amounts and were both structured and non-structured.

Offence	Tax fraud
Customer	Business, individual
Industry	Professional services, authorised deposit-taking institutions
Channel	Agent / third party, individual
Jurisdiction	Domestic
Designated service	Accounts, electronic funds transfer, accounts – chequebook facility
Indicators	Elaborate movement of funds through different accounts Structuring of cash withdrawals Use of companies to move funds under the guise of legitimate transactions Use of false and stolen identities to open and operate bank accounts Use of gatekeepers (accountant) to give appearance of legitimacy

Case 51

Phantom vessel insured to launder funds

A money launderer purchased marine property and casualty insurance for a phantom ocean-going vessel. He paid large premiums on the policy and bribed the intermediaries so that regular claims were made and paid. However, he was very careful to ensure that the claims were less than the premium payments, so that the insurer enjoyed a reasonable profit on the policy. In this way, the money launderer was able to receive claims cheques which could be used to launder funds.
The funds appeared to come from a reputable insurance company, and few questioned the source of the funds having seen the name of the company on the cheque or wire transfer.[17]

Offence	Money laundering
Customer	Individual
Industry	Insurance intermediaries
Channel	Physical (face-to-face)
Jurisdiction	Domestic
Designated service	Electronic funds transfer, insurance and superannuation services, accounts – chequebook facility
Indicators	Regular claims made less than the premium payments

[17] Financial Action Task Force on Money Laundering (FATF), 'Report of Money Laundering Typologies 2003-2004', *<http://www.fatf-gafi.org/dataoecd/19/11/33624379.PDF>.*

Appendix

FATF Typologies Work

The FATF holds its global typologies exercise each year, which includes active participation by the APG and other regional anti-money laundering bodies. Arising from its yearly typologies exercise, the FATF publishes a yearly typologies report to consider priority topics in detail.

Although the FATF has conducted typologies exercises since its beginning, reports of this work have only been made public since the 1995 exercise (released in June 1996). All reports include selected case studies.

FATF-XVI (June 2005) -
Major topics covered in the report include:

- alternative remittance systems
- money laundering vulnerabilities in the insurance sector
- proceeds from trafficking in human beings and illegal immigration.

FATF-XV (February 2004) -
Major topics covered in the report include:

- wire transfers and terrorist financing
- non-profit organisations and links to terrorist financing
- the vulnerabilities of the insurance sector to money laundering
- politically exposed persons (PEPs)
- the role of 'gatekeepers' or non financial professions in money laundering.

FATF-XIV (February 2003) -
Major topics covered in the report include:

- Terrorist financing
- Money Laundering through the securities sector
- The gold and diamond markets
- Insurance and money laundering
- Credit and debit cards and money laundering

FATF-XIII (February 2002) -
Major topics covered in the report include:

- terrorist financing
- correspondent banking
- corruption and private banking
- bearer securities and other negotiable instruments
- coordinated money laundering among organised crime groups
- introduction of Euro banknotes
- suspicious transaction reporting and money laundering cases.

FATF-XII (February 2001) -
Major topics covered in the report include:

- on-line banking and internet casinos
- trust, other non-corporate vehicles and money laundering
- lawyers/notaries, accountants and other professionals
- the role of cash vs other payment methods in money laundering schemes
- terrorist related money laundering.

FATF-XI (February 2000) -
Major topics covered in the report include:

- online banking: distinguishing legitimate banking from money laundering services offered through the internet
- alternate remittance systems: A worldwide view of their role in money laundering
- company formation agents and their services
- trade related activities and money laundering.

FATF-X (February 1999) -
Major topics covered in the report include:

- the single European currency and large denomination banknotes
- offshore financial centres of non-cooperative countries or territories
- the role of the 'foreign legal entity' in money laundering
- new payment technologies
- potential use of the gold market in money laundering operations.

FATF-IX (12 February 1998) -
Major topics covered in the report include:

- new payment technologies: present status and potential vulnerabilities to money laundering
- money remittance businesses and activities (both formal and informal)
- other observed trends (insurance, money exchange, cross-border movements, the gold market)
- money laundering and non-financial professions (lawyers, notaries, accountants, company formation agents, real estate, sellers of high-value items).

FATF-VIII (February 1997) -
Major topics covered in the report include:

- attempts to estimate the size of the money laundering problem
- principal sources of illegal proceeds laundered
- main money laundering methods detected in the banking, non-bank financial institution and non-financial business sectors
- electronic funds transfers and their vulnerability to money laundering
- new money laundering counter-measures (legislative, regulatory, etc.)
- key money laundering trends in non-FATF members.

FATF-VII (28 June 1996) -
Major topics covered in the report include:

- in addition to the primary topics mentioned above for FATF-VIII, the group of experts also examined money laundering trends involving the insurance and securities industries (http://www.apgml.org/frameworks/default.aspx?FrameworkID=5).