AUSTRAC

Typologies and Case Studies Report 2009

Australian Government

Australian Transaction Reports and Analysis Centre

Acknowledgement: The valuable contribution of reporting entities and AUSTRAC's designated agencies in producing this document is acknowledged.

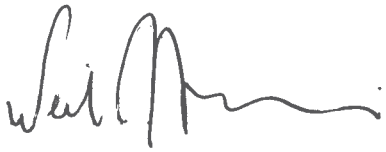
Foreword

As Australian and international businesses grapple with the impact of the global financial crisis, government and industry must remain vigilant against attempts to take advantage of the crisis to commit money laundering. With opportunities ever present to misuse our financial system, timely and accurate reporting of financial transactions and suspicious matters to AUSTRAC takes on extra importance.

The *AUSTRAC Typologies and Case Studies Report 2009* presents a range of case studies highlighting illicit activities that may have remained undetected if not for diligent reporting by entities. The cases illustrate how the reports submitted to AUSTRAC have assisted law enforcement agencies and other government authorities trace those involved in the importation and trafficking of illegal drugs, superannuation fraud and illegal investment schemes, tax evasion, credit card fraud, and other organised crime.

As with previous Typologies and Case Studies Reports, this publication combines case study information collected by AUSTRAC's law enforcement, national security and revenue partner agencies and AUSTRAC's own research into money laundering and terrorism financing methods. The report provides examples of how criminals have attempted to exploit the financial system and also includes red flag 'indicators' – examples of suspicious behaviour that may indicate the possibility of money laundering or terrorism financing activity.

The *AUSTRAC Typologies and Case Studies Report 2009* is a valuable educative resource for both reporting entities and AUSTRAC's partner agencies in their continued efforts to combat financial and other crime.



Neil J Jensen PSM
Chief Executive Officer, AUSTRAC

Contents

Introduction

The Australian Transaction Reports and Analysis Centre (AUSTRAC) continues to support law enforcement agencies in the global fight against organised crime and the financing of terrorism. In many cases, the information gained from the monitoring and analysis of financial activities has allowed authorities to take action against those misusing the legitimate financial system for illegal activities. In addition to the arrests of those involved, authorities have often undertaken proceedings to confiscate the money and other assets derived from criminal activities.

The vigilance of reporting entities, particularly in identifying suspicious matters, has greatly assisted AUSTRAC and law enforcement agencies in our endeavours. The close cooperation between reporting entities, law enforcement agencies and AUSTRAC has enabled the production of material such as the AUSTRAC Typologies and Case Studies Reports to assist all parties in understanding how criminals and the financiers of terrorism conduct their activities. As in the previous two reports, the case studies in this report identify various mechanisms and methodologies used to conceal, launder or move illicit funds.

Criminals continue to adapt the methods they use to undertake their illicit financial activities. As avenues are closed down or more closely monitored by authorities, criminals must find new means. This constant disruption to their activities contributes to the fight against global organised crime and the financing of terrorism. Similarly, the collaboration between reporting entities, law enforcement agencies and AUSTRAC in identifying new mechanisms and methodologies is also critical in keeping pace with the threat posed by organised crime.

Report methodology

The information contained in this report was generated from the following research material:

- sanitised cases from AUSTRAC's partner agencies
- existing AUSTRAC strategic and typology research
- publicly available open source information.

This report identifies some key methods that have been used in Australia to conceal the origins of illicit funds or, in the case of terrorism financing, conceal the purpose for which those funds were intended. These methods are illustrated through the use of case studies and diagrams.

Please note that the case studies presented in this report are limited to those cases that have been approved for external use.

Each case study within this report has been presented in a way that highlights the common elements involved in the money laundering or terrorism financing process. These are:

- Offence – the crime or civil proceeding involved (not the actual charges).
- Customer – the type of customer/s involved in perpetrating the offence (this can be an individual, business or foreign entity).
- Industry – the industry through which transactions were conducted – in some cases multiple industries were involved.
- Channel – the means by which the offenders completed or attempted to complete transactions (predominantly either in person, via electronic means or through an intermediary/third person).
- Jurisdiction – the location (domestic or international) in which the transactions were facilitated.
- Designated service – the category of 'designated service', or other financial product, used in the offence. AUSTRAC groups the designated services listed in section 6 of the *Anti-Money Laundering and Counter Terrorism Financing Act 2006* (AML/CTF Act) into categories containing similar activities (as per the designated services category table on page 6). The case studies within this report have been arranged according to the designated services used within each case.
- Indicators – the 'red flag' activity which would indicate the possibility of money laundering or terrorism financing. An extensive list of the indicators used in this report can be found in Appendix A.

Designated service category	AML/CTF Act section 6 – item number/s
Financial services (Table 1)	
Account and deposit-taking services	Items 1–5
AFSL holder arranging a designated service	Item 54
Cash carrying/payroll services	Items 51–53
Chequebook access facilities	Items 14–16
Currency exchange services	Item 50
Custodial/depository services	Items 46–47
Debit card access facilities	Items 18–20A
Debt instruments	Items 8–9, 17, 34, 36
Electronic funds transfers (EFT)	Items 29–30
Leasing/hire purchase services	Items 10–13
Life insurance services	Items 37–39
Loan services	Items 6–7, 48–49
Money/postal orders	Items 27–28
Pensions/annuity services	Items 40–41
Remittance services (money transfers)	Items 31–32
Retirement savings accounts (RSAs)	Items 44–45
Securities market/investment services	Items 33, 35
Stored value cards	Items 21–24
Superannuation and approved deposit funds	Items 42–43
Travellers cheque exchange services	Items 25–26
Bullion dealing (Table 2)	Items 1–2
Gambling services (Table 3)	Items 1–14

Financial crime and money laundering threats and methodologies

AUSTRAC's vision is to have an Australian community that is hostile to money laundering and the financing of terrorism. It is also important for the agency, its partner agencies and reporting entities to understand the evolving nature of financial crime, which is often the source of the illicit funds involved in money laundering.

Financial crimes can include a wide range of activities, from fraud against potential investors to active manipulation of the stock market. The modern globalised economy and new technologies have created additional opportunities for fraud. They have also presented criminals with new ways to commit existing crimes.

While the current global economic crisis has prompted a more cautious international financial market, there are always opportunities for criminals to exploit the financial sector. Authorities have also noted that the financial crisis has led to increased detection of money laundering and other financial crime, as companies and investors around the globe scrutinise their accounts more closely. Scams such as 'Advance fee frauds', commonly referred to as 'Nigerian scams', continue to be widespread. Approaches may vary, but most scams aim to deceive unsuspecting victims into forwarding payments or divulging financial information such as bank account details. Scams can attract victims with claims of lottery wins, unexpected inheritances or government windfalls.

Other emerging methods being used to exploit the mainstream economy include frauds to avoid import taxes, equities market manipulation by criminal networks, and the use of new, unregulated financial mechanisms – such as internet-based currency – to conceal international transactions and launder money.[1]

Card skimming

'Card skimming' is the illegal copying of information from the magnetic strip of a credit or debit card. It is a more direct version of a 'phishing' scam (in which fraudsters send an email purporting to be from a legitimate source requesting that the recipient provides personal information).

One method of card skimming involves attaching small, sophisticated skimming devices to automatic teller machines (ATMs). These devices are secretly placed over the ATM's card slot and designed to look like part of the ATM. The devices electronically record and store the details of the cards as they are inserted into the ATM. Because debit and credit cards require a personal identification number (PIN) to access the account, the criminals also mount a pinhole camera on the ATM to record the customer as they enter their PIN.

Once the criminals have skimmed the victim's card, they can create a fake or 'cloned' card with the victim's details on it. The scammer is then able to access the victim's account.

Recent media reports indicate that card skimming is increasing in Australia. In a recent case, a number of Romanian nationals were arrested in Australia for their involvement in an ATM skimming ring in which more than 50 ATMs across Australia were affected. While the offenders concentrated mostly on ATMs in Sydney, they also stole more than AUD1 million from victims in Melbourne.[2]

1 Australian Crime Commission, *Organised Crime in Australia 2009*, Australian Crime Commission, Canberra, 2009, viewed 11 May 2009, <www.crimecommission.gov.au/publications/oca/index.htm>

2 News.com.au, 14 April 2009, 'Police believe ATM skimmers belong to international ring', viewed 11 May 2009, <www.news.com.au/story/0,23599,25332654-29277,00.html?from=public_rss>

Early release super schemes

Early release superannuation schemes are scams that offer consumers early access to their superannuation funds, often through a self managed superannuation fund. The organisers of the schemes often charge high fees for the service.

Consumers cannot legally access the 'preserved' part of their superannuation until they reach the 'preservation' age (which ranges from 55 to 60 years of age) and retire, or turn 65. While there may be exceptions to this rule in the case of severe financial hardship or on compassionate grounds, in general schemes that offer early access to superannuation funds are illegal.

Past examples of early release schemes have involved a financial adviser, or someone posing as a financial adviser, promising consumers quick and easy access to their superannuation benefits. In many cases the scammers deceive the superannuation fund into paying out the benefits directly to the adviser in cash. They may also ask the client to confirm a false statement (claiming, for example, that the client is suffering financial hardship) to secure the early release of the funds. Once the scammer has the money, they may disappear and leave the victim with nothing, or subtract substantial fees or commissions before forwarding the remainder of the funds to the victim.[3]

The erosion of superannuation funds through these early release scams can lead to an increased burden on tax-payers resulting from increased social security payments. And for the individual victims of these scams, the loss of their superannuation threatens their future financial independence.

Ponzi schemes

'Ponzi' schemes have existed for many years. They are simple and effective scams in which the promoters attract investors to a scheme by promising a very high return on investment, while guaranteeing the security of the investment.

The scammers use some of the funds deposited by early investors to pay initial dividend cheques or interest – at this early stage the ponzi scheme only requires a few investors to operate successfully. The promoter continues paying the investors impressive dividends for a couple of months until the investors, encouraged by the early dividends, decide to invest more.

The investors may also encourage their friends and relatives to invest. Soon there is a steady flow of funds into the scheme and an ever-growing number of investors.

If the promoter is disciplined and retains sufficient funds in the scheme to continue to pay out 'dividends', a ponzi scheme can continue for many years. Theoretically, if the scheme continues to draw in new investors, it could go on indefinitely. In practice such schemes usually collapse because the promoter starts to spend the money too quickly, or the pool of investors starts to dry up.[4]

The recent Bernard Madoff case in the United States, which involves investor losses of at least USD50 billion, is a high-profile example of corporate fraud which operated on a massive scale over many years. It is also a dramatic example of the type of fraud schemes left exposed by the global financial crisis. Madoff has allegedly admitted that his investment advisory business at the centre of the fraud was 'basically, a giant Ponzi scheme.'[5]

3 SCAMwatch, 2008, Australian Competition & Consumer Commission, Canberra, viewed 11 May 2009, <www.scamwatch.gov.au/content/index.phtml/tag/SuperannuationScams>

4 FIDO website, 2009, Australian Securities & Investments Commission, Canberra, viewed 30 April 2009, <www.fido.gov.au/fido/fido.nsf/byheadline/Ponzi+schemes?openDocument>

5 U.S. Securities and Exchange Commission, 11 December 2008, *SEC Charges Bernard L. Madoff for Multi-Billion Dollar Ponzi Scheme*, press release, SEC, Washington, viewed 11 May 2009, <www.sec.gov/news/press/2008/2008-293.htm>

Boiler-room scams

Fake investment advice is a common avenue for fraud. In 'boiler-room' scams, the scammers telephone victims claiming they were given the victim's name by a friend who has previously profited from the scammer's 'insider' investment advice. The scammer will recommend buying shares in various companies, advising the victim that the shares are undervalued and on the verge of rising sharply in value.

The recommended shares are usually for small, unlisted companies, rather than blue-chip or established companies. The scammer uses the funds invested by victims of the scam to purchase low-value shares in the companies, forcing up the price of the shares. The scammers then contact the victims advising them that their investment has made an impressive short-term profit and urging them to buy more shares.

In many cases the victims are encouraged by the initial profit and agree to purchase even more shares. After artificially inflating the prices, the scammers then sell off the shares to the victims at a substantial profit. The price of the shares then plummets, leaving the investors with potentially very significant losses.[6]

Internet scams

Many internet-based scams take place without the victim even realising they have been targeted.

The growth of internet-based shopping in particular presents scammers with increased opportunities. Scammers use the anonymous nature of the internet to target unsuspecting shoppers. A common scam involves the perpetrators convincing victims to enter into deals outside legitimate online auction sites. The scammers may claim that the winner of an auction has pulled out and then offer the item to the victim. Once the victim pays for the item, the scammer disappears with the victim's money and the legitimate auction site is unable to help.

Another variation features scammers who pretend to be selling a product – often at heavily discounted prices – to obtain the victim's credit card or bank account details. When the transaction for the purchase is complete, the scammers take the victim's money and send the victim a faulty or worthless product, or nothing at all.[7] Case 26 in this report is an example of criminals using internet shopping to commit fraud.

Other scammers prey on the emotions and goodwill of victims through online dating scams. By promising relationships, companionship and romance, scammers can deceive their victims to such an extent that the victims continue to provide payments even after they begin to doubt the scammer's claims. Commonly the scams require the victim to transfer funds from accounts or through remittance services to foreign jurisdictions where no previous transfers have been undertaken by the victim.

Lottery and sweepstake scams

Lottery and sweepstake scams are most often promoted in Australia by direct mailing to potential victims, but they can also be carried out by phone or email. The scammers promote fake lotteries offering 'huge' prizes, including holidays, cars, and cash, with the victims being told that they have a 'guaranteed' chance of winning.

A common message from the promoters to victims is that 'you have been chosen to win one of these prizes' but in order to participate the victim must buy a 'trial sample.' This sample is usually a poor quality product such as a pen, vitamins or makeup, worth a small fraction of what the victim is asked to pay.

Another approach used by the scammers is to tell the victim that they must pay a 'processing fee' or 'handling fee' or customs duties or taxes and must send a cheque or money order to the promoter immediately, otherwise they will miss out on this 'fabulous opportunity'.[8]

---

6 Australian Taxation Office, 11 March 2009, Australian Taxation Office, Canberra, viewed 11 May 2009, <www.ato.gov.au/superfunds/content.asp?doc=/Content/00183101.htm&page=21&H21>

7 SCAMwatch, 2008, Australian Competition & Consumer Commission, Canberra, viewed 11 May 2009, <www.scamwatch.gov.au/content/index.phtml/tag/OnlineAuctionShoppingScams>

8 SCAMwatch, 2008, Australian Competition & Consumer Commission, Canberra, viewed 11 May 2009, <www.scamwatch.gov.au/content/index.phtml/tag/LotterySweepstakeScams>

Reporting suspicious matters

Reports of suspicious matters have been the catalyst for many significant investigations conducted by AUSTRAC's national security, law enforcement, revenue collection and social justice partner agencies. The prompt reporting of suspicious customer activity by reporting entities has enabled AUSTRAC to immediately refer the information to relevant agencies, leading to successful law enforcement outcomes. A number of the investigations included in this *Typologies and Case Studies Report* were initiated as a result of high-quality, timely and relevant reports of suspicious matters.

The grounds for suspicion have often provided valuable leads to investigators to assist in the identification of illegal activity. Some of the more common themes or indicators reported include:

- customers who avoid, or attempt to avoid, transaction reporting obligations
- customers who use multiple reporting entities and/or branches to avoid arousing suspicion and detection
- customers who undertake transactions that appear inconsistent with their profile
- customers who conduct multiple transactions within a short time frame
- customers who exhibit irregular behaviour or patterns of transactions
- use of currency that is in an unusual condition (for example, dirty, wet, smelly)
- frequent exchanges of currency denominations (for example, exchanging $20 notes for $100 notes) or currency types (for example, exchanging Australian dollars for euros) where such exchanges are inconsistent with the customer's profile
- regular transfers of funds between a customer's personal account and a business or commercial account
- international funds transfers to high-risk countries, where such transactions are inconsistent with the customer's profile. High-risk countries include:
  - countries commonly associated with the production or transport of drugs
  - countries known to be tax havens*
  - countries associated with phishing scams and card skimming
- customers who regularly use stored value cards and frequently add value to the card below the card's threshold limits, particularly when the card is used domestically.

Accurate and timely reporting of suspicious matters is underpinned by effective 'know your customer' information collection and verification processes, a customer due diligence program and the vigilance of reporting entities. Staff training and awareness together with intuitive transaction monitoring systems are critical to the detection of suspicious activities and their subsequent reporting to AUSTRAC and law enforcement agencies.

* The Australian Taxation Office maintains a list of jurisdictions it considers to be tax havens. This list is available on the Tax Office website at <www.ato.gov.au> and continues to be reviewed and updated as circumstances change.

Law enforcement agency quotes on the value of reports of suspicious matters

'This report will assist in a matter in which the suspected offences are money laundering, welfare fraud and tax evasion.'

'Based on the suspect transaction report (SUSTR), the subject of the investigation appears to have a lengthy history of fraudulent activity.'

'I have found this SUSTR very useful – the person is well known to us and this change in financial pattern is of great interest to us.'

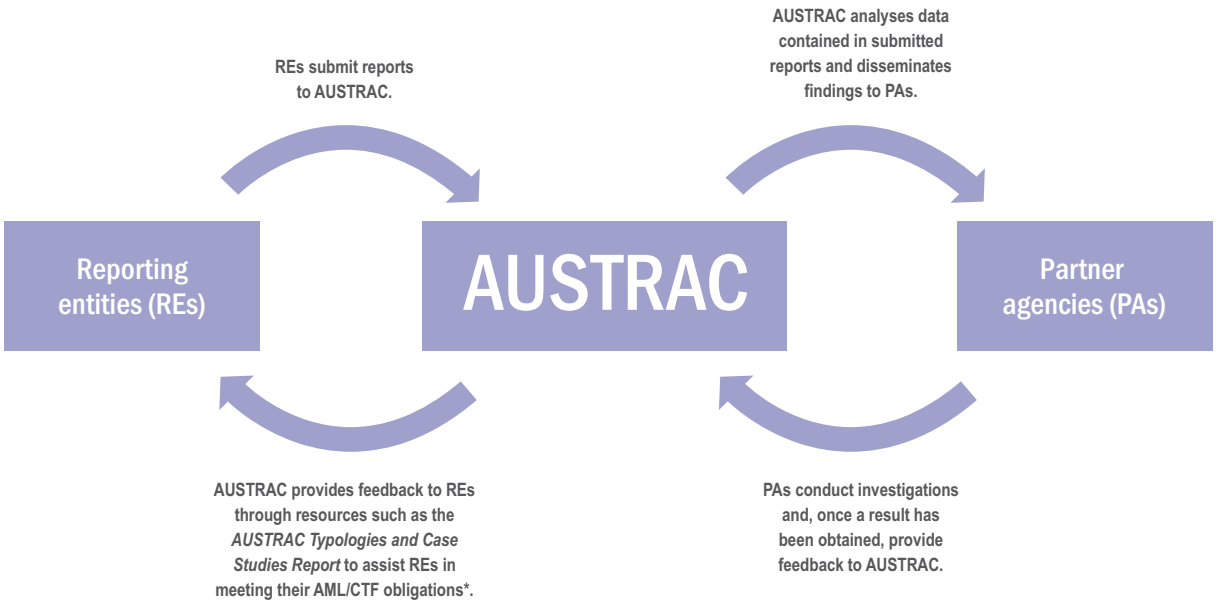
'This SUSTR…was an excellent referral which helped us recognise a suspect transaction pattern.'

AUSTRAC feedback process

In carrying out its AML/CTF regulatory functions, AUSTRAC collects reports from reporting entities in the financial, bullion and gambling sectors that provide designated services under the *Financial Transaction Reports Act 1988* (FTR Act) and the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act).

As part of its financial intelligence unit functions, AUSTRAC then analyses data contained within these reports to uncover activities and patterns that may indicate money laundering, terrorism financing or other criminal activities. This information is then disseminated to national security, law enforcement, revenue collection or social justice agencies, as well as certain international bodies.

The AUSTRAC feedback process is an important collaborative process between government and industry to combat money laundering and terrorism financing in Australia.



* Obligations under the AML/CTF Act include implementing an AML/CTF program, conducting risk assessments, identifying and verifying customers, conducting ongoing customer due diligence and submitting AML/CTF Act reports to AUSTRAC. Obligations under the FTR Act include submitting transaction reports to AUSTRAC.

Case studies

Case 1 – Illegal investment scheme cost investors $75 million

Offence	Fraud
	Money laundering
Customer	Individual
Industry	Banking (ADIs)
	Gambling services
Channel	Electronic
Jurisdiction	International – Vanuatu, Switzerland, New Zealand, Indonesia, United Kingdom
Designated service	Account and deposit-taking services
	Gambling services
	Loan services
	Securities market/investment services
Indicators	Funds transfers to numerous offshore jurisdictions with no business rationale
	Large number of accounts held by customer with the same institution
	Numerous large deposits via ATMs
	Value of funds transfers inconsistent with customer profile

The managing director of two public companies listed on the Australian Securities Exchange allegedly operated a managed investment scheme in breach of the *Corporations Act 2001*.

The suspect entered into loan agreements directly with investors to raise funds for the managed investment scheme. Meanwhile an unrelated company also used investors' funds to invest in the suspect's illegal scheme.

When authorities began investigating one of the two public companies, they found that the company owed approximately AUD18 million to about 50 investors. Meanwhile, the suspect owed a total of about AUD75.8 million to investors, most of them from South Australia. It is also alleged that a former member of an outlaw motorcycle gang had invested in the fund, and attempted to claim security of AUD17 million over the suspect's assets after the scheme collapsed.

It is alleged that over three years the scheme received loans totalling AUD215 million from investors, who were offered interest rates of between three per cent and six per cent per month. Further investigations revealed that some funds from the scheme had been re-invested in a number of companies associated with the suspect. The Federal Court of Australia found that ten such companies were parties to the scheme and ordered that they be wound up.

AUSTRAC information was used to monitor the activities of the suspect throughout the investigation. AUSTRAC intelligence reports and suspect transaction reports (SUSTRs) indicated that he had made a number of large deposits via ATMs and undertaken international funds transfers to a sports bookmaker in the United Kingdom, an investment company in Vanuatu, and accounts in Switzerland, New Zealand and Indonesia.

Case 2 – Money launderer used false name to launder millions

Offence	Fraud Money laundering
Customer	Individual Business
Industry	Banking (ADIs)
Channel	Electronic Physical
Jurisdiction	International – United States, Asia
Designated service	Account and deposit-taking services Gambling services
Indicators	Business activity inconsistent with profile Large funds transfers after gambling activity Large international funds transfers Use of false identification documentation (to conduct transactions, etc.)

A law enforcement agency began investigating an individual for allegedly laundering large amounts of money. In all, authorities suspect the individual's fraudulent activities involved more than AUD58 million.

Law enforcement enquiries identified that the suspect was a director of an offshore company, operating accounts in Australia under both his own name and business names. Investigators identified that the suspect had transferred more than AUD12 million into various Australian accounts from overseas accounts, with approximately AUD3 million coming from accounts in the United States. The suspect had also transferred approximately AUD19 million out of Australia to accounts in Asia and the United States, and had conducted these particular transactions using a false name.

In addition, AUSTRAC had received a suspect transaction report (SUSTR) detailing the suspect's suspicious activities at casinos. These casino visits were often followed by large international funds transfers to an Asian account.

Law enforcement officers identified that the suspect had opened a bank account using a false name, an offence under section 24 of the *Financial Transaction Reports Act 1988*. Officers also enacted restraining orders under section 18 of the *Proceeds of Crime Act 2002* to restrain AUD6.7 million of funds in related company accounts.

An agreement was reached between the offender and the Commonwealth, with the offender forfeiting a sum of approximately AUD3.37 million.

Case 3 – Company director hid gambling profits

Offence	Tax evasion
Customer	Individual Business
Industry	Banking (ADIs) Gambling Real estate
Channel	Electronic
Jurisdiction	International
Designated service	Account and deposit-taking services Gambling services
Indicators	Business activity inconsistent with profile Large cash deposits Structuring of transactions

AUSTRAC received a number of suspect transaction reports (SUSTRs) from reporting entities indicating that a company director was deliberately structuring transactions and carrying out large cash transactions. Despite this, the director claimed his company was returning only low profits.

An audit was conducted into the company's activities, and the director provided bank statements for some, though not all, of the accounts identified in the audit. The statements included deposits that were the result of betting and gambling activities.

AUSTRAC information also identified international funds transfers which helped uncover previously unknown overseas bank accounts and property assets belonging to the company director.

Action was taken against the director and approximately AUD2 million in tax and penalties was raised.

Case 4 – Director used company funds to cover personal gambling debts

Offence	Fraud
Customer	Individual Business
Industry	Gambling Banking (ADIs)
Channel	Electronic (internet)
Jurisdiction	Domestic
Designated service	Account and deposit-taking services Gambling services
Indicators	Betting accounts with large deposits but with minimal betting activity Cash withdrawals from betting accounts in cheques and vouchers Structuring of gambling purchases, payouts and withdrawals Unusual pattern of phone betting transactions Use of company accounts for personal use Use of false documentation

A company director allegedly used more than AUD1 million of company funds for his personal gambling and entered into an agreement rendering the company liable for his gambling debts.

Reporting entities submitted 24 suspicious transaction reports (SUSTRs) to AUSTRAC detailing a variety of suspicious activities undertaken by the director, including:

- structuring gaming chip purchases and cash outs at casinos in amounts less than AUD10,000 to avoid the transaction reporting threshold
- making large deposits into phone betting accounts and, after minimal gambling, withdrawing similar amounts from the account using cheques and vouchers. On one occasion the director deposited AUD1 million into a phone account and, within 30 minutes, had withdrawn AUD950,000 from the account in cheques, vouchers and cash
- when redeeming vouchers, requesting cash in structured amounts less than AUD10,000 to avoid the transaction reporting threshold, and requesting that the remainder of the funds be deposited into his account.

As a result of his actions, the director was charged with nine counts of dishonestly using his position as a director of the company and a further 16 charges of falsifying an account or record made or required for accounting purposes.

Case 5 – Funds from illegal investment schemes laundered in New Zealand

Offence	Money laundering
Customer	Individual
Industry	Gambling Real estate Banking (ADIs)
Channel	Electronic
Jurisdiction	International – New Zealand
Designated service	Account and deposit-taking services Gambling services
Indicators	Purchase of high-value assets (vehicles, real estate) Outgoing transfer with corresponding incoming funds transfer – appears to be a 'u-turn' transaction

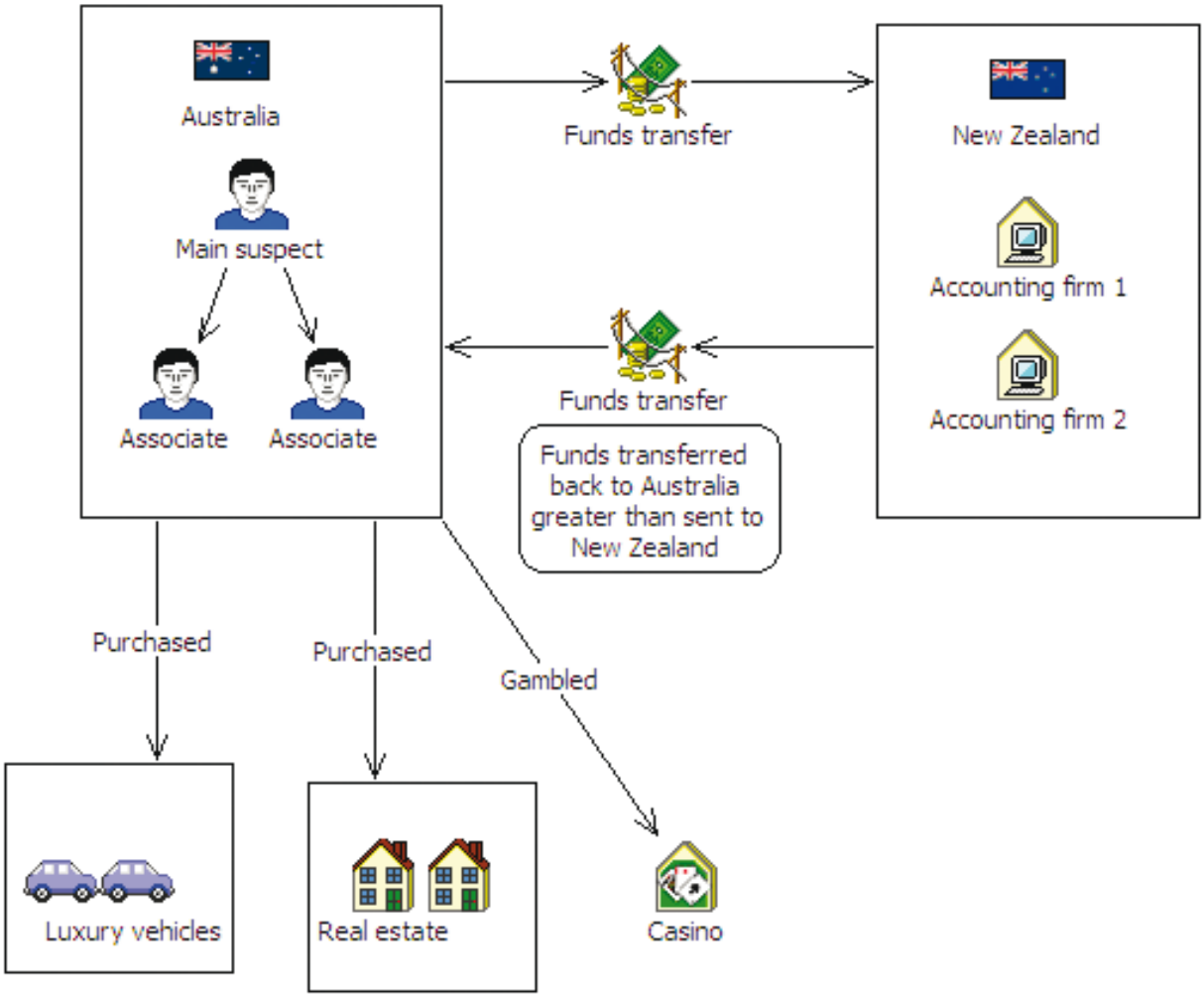
Authorities began investigating a suspect allegedly involved in illegally raising investment funds and operating an unregistered managed investment scheme.

AUSTRAC began monitoring the financial activities of the suspect and his associates, and analysis of the information gathered indicated that the suspect was sending funds from Australia to two accounting firms in New Zealand. The funds were then transferred back to Australia, where they were used to purchase luxury vehicles and real estate, and for gambling.

A suspect transaction report (SUSTR) detailing the main suspect's activities was also submitted to AUSTRAC.

AUSTRAC information showed that the amount of funds returning to Australia was greater than the amount originally sent to New Zealand. Authorities concluded that the suspects were raising money from the public in Australia and New Zealand to fund the managed investment scheme, and that the funds were being transferred to New Zealand and then back to Australia to disguise their origins.

Further investigations followed, and both suspects were charged with operating an unregistered managed investment scheme and sentenced to two years imprisonment.


Australia
Main suspect
Associate
Associate
Funds transfer
New Zealand
Accounting firm 1
Accounting firm 2
Funds transfer
Funds transferred back to Australia greater than sent to New Zealand
Purchased
Purchased
Gambled
Luxury vehicles
Real estate
Casino

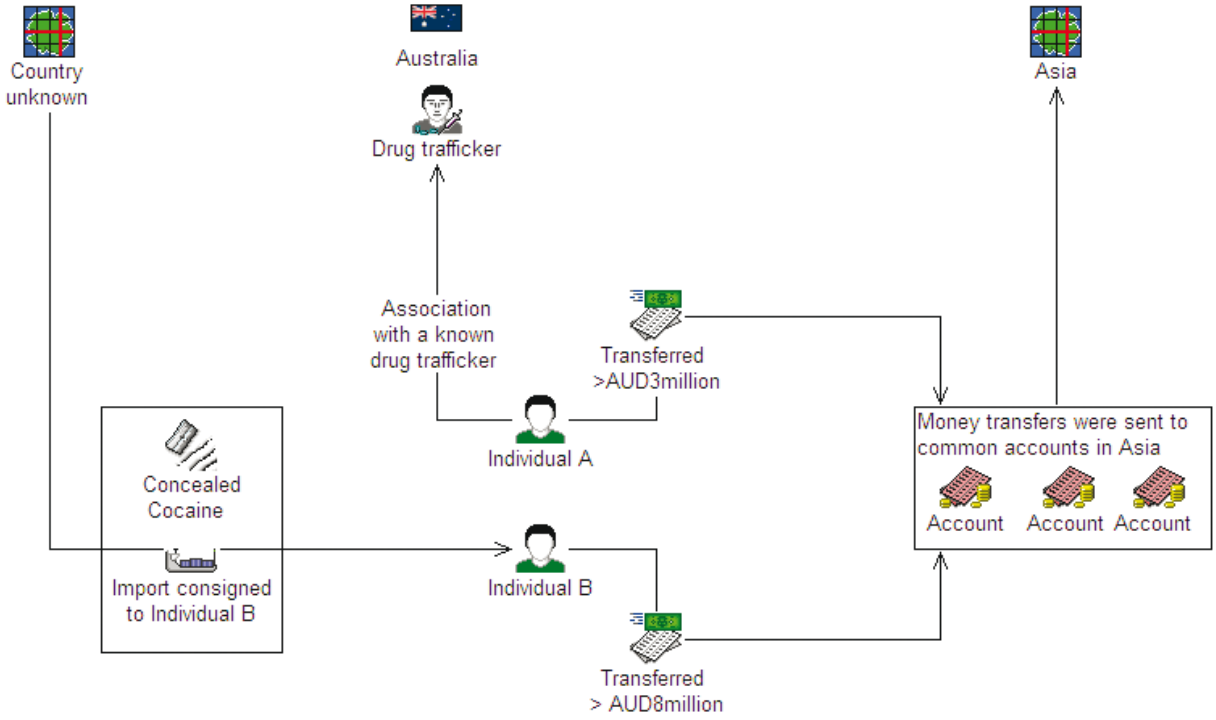
Case 6 – Significant cocaine shipment intercepted

Offence	Drug importation
Customer	Individual Business
Industry	Banking (ADIs)
Channel	Agent/third party Electronic
Jurisdiction	International – Asia
Designated service	Account and deposit-taking services
Indicators	Business activity inconsistent with business profile Large cash deposits Multiple deposits made to same overseas account by different people Use of third parties to conduct transactions

AUSTRAC alerted law enforcement partner agencies about unusually large amounts of money being transferred from Australia to Asia. The individual transferring the funds was known to police due to his association with a known drug trafficker. Over a two-month period the suspect transferred more than AUD3 million to various accounts in Asia. The details of the transactions indicated that the large cash deposits made by the suspect were derived from business activities; however, investigating officers found it suspicious that more than AUD8 million had been transferred overseas mostly within an 18-month period, when the company had been operating for several years without undertaking any prior international funds transfers.

Further investigations identified a second suspect who was also transferring money from Australia to the same accounts in Asia. Investigating officers monitoring the premises of this second suspect intercepted a third person leaving these premises – this third person was carrying AUD1.5 million in cash at the time, further adding to the officers' suspicions.

The second suspect continued to send money to accounts in Asia through an intermediary acting on his instructions. Investigations identified a shipping container from overseas due to be delivered to the second suspect in Australia. When the container arrived in Australia, it was found to contain a large, commercial quantity of cocaine. Law enforcement officers arrested several suspects as a result of the investigation.


Country unknown
Australia
Drug trafficker
Asia
Association with a known drug trafficker
Transferred >AUD3million
Individual A
Money transfers were sent to common accounts in Asia
Account
Account
Account
Concealed Cocaine
Import consigned to Individual B
Individual B
Transferred > AUD8million

Case 7 – Trusted priest defrauded nursing home resident of $50,000

Offence	Fraud
Customer	Individual
Industry	Banking (ADIs)
Channel	Electronic
Jurisdiction	International – Thailand
Designated service	Account and deposit-taking services
Indicators	Funds transferred to overseas account but then withdrawn in Australia Use of international credit card

A priest who held powers of attorney and guardianship for an elderly nursing home resident fraudulently withdrew approximately AUD50,000 from the victim's account. The withdrawal prompted a suspect transaction report (SUSTR) to be submitted to AUSTRAC, which formed the basis for law enforcement enquiries into the matter.

These investigations were further aided by the information contained within an international funds transfer instruction (IFTI) report submitted to AUSTRAC. The IFTI report indicated that the priest had transferred a further AUD30,000 to an account in Thailand and enabled law enforcement officers to establish that this international transfer had been debited from an internationally issued credit card.

A civil settlement was negotiated and the stolen money was repaid to the victim.

Case 8 – International fraudster arrested and extradited

Offence	Money laundering
Customer	Business
Industry	Banking (ADIs)
Channel	Electronic
Jurisdiction	International – The Netherlands
Designated service	Account and deposit-taking services
Indicators	Purchase of high-value assets Use of company accounts for personal use

A law enforcement agency commenced an investigation into money laundering following allegations of a fraud committed against a European bank. The fraud was worth AUD17 million and it is alleged that some of the proceeds of the fraud were laundered in Australia.

The stolen funds were deposited into Australian bank accounts in the name of two registered companies, via a Dutch corporate bank account. The main suspect in Australia was a listed director of both these companies. The suspect purchased a number of assets in Australia, which were suspected to have been bought with the proceeds of the fraud.

AUSTRAC information assisted law enforcement officers in tracking approximately AUD1.3 million of the proceeds of the fraud, and the main suspect was arrested and extradited overseas.

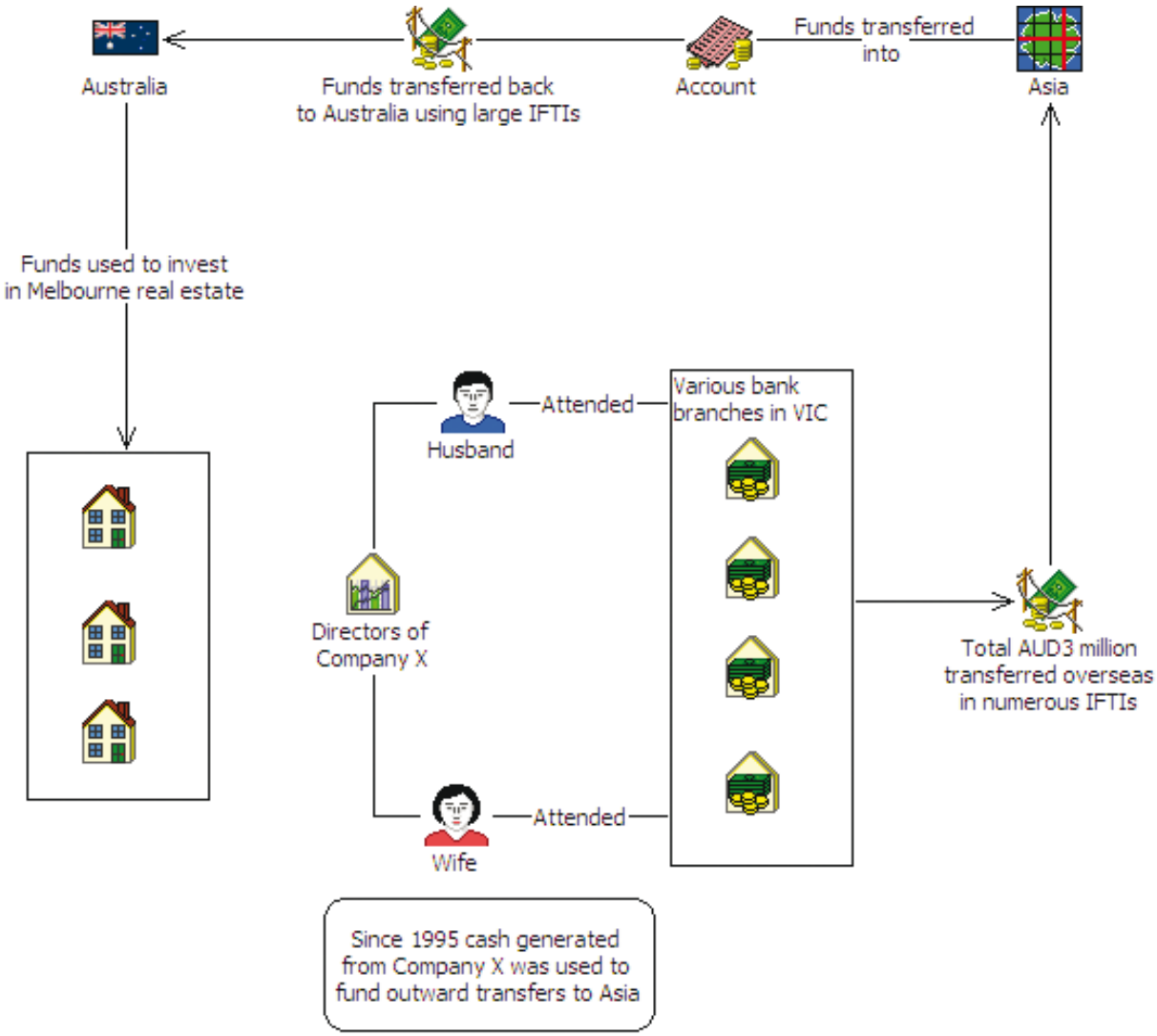
Case 9 – Couple attempted to dodge millions in tax through money laundering

Offence	Money laundering Tax evasion
Customer	Individual Business
Industry	Banking (ADIs) Real estate
Channel	Physical (face-to-face) Electronic
Jurisdiction	International – Asia
Designated service	Account and deposit-taking services
Indicators	Multiple funds transfers to common beneficiaries Outgoing transfer with corresponding incoming funds transfer – appears to be a 'u-turn' transaction Purchase of high-value assets (real estate)

Analysis of AUSTRAC information revealed that a husband and wife were regularly undertaking structured international funds transfers to Asia. Over a number of years the couple, who were joint directors of a company registered in their names, had regularly sent international funds transfers to Asia via various bank branches in Victoria using cash generated from their company. They had sent more than AUD3 million overseas in this manner.

Further investigations revealed that approximately AUD4.8 million in taxable income for the couple was unaccounted for. It was alleged that the transfers represented undeclared income generated from the couple's business. It was suspected that the remitted funds were transferred to a second overseas account and then sent back to Australia via large international funds transfers.

It was believed that after the couple received the funds back in Australia, the funds were invested in real estate in Melbourne. Thus, the funds from the tax evasion were successfully laundered and integrated back into the Australian economy. A proceeds of crime investigation into the couple's assets was successful in restraining AUD16 million of real estate.


Australia
Funds transferred back to Australia using large IFTIs
Account
Funds transferred into
Asia
Funds used to invest in Melbourne real estate
Husband
Attended
Various bank branches in VIC
Directors of Company X
Total AUD3 million transferred overseas in numerous IFTIs
Wife
Attended
Since 1995 cash generated from Company X was used to fund outward transfers to Asia

Case 10 – Imported furniture hid 28 kilos of heroin

Offence	Drug importation
Customer	Individual Business
Industry	Banking (ADIs)
Channel	Electronic
Jurisdiction	International – Indonesia, Hong Kong, China, Canada, the Netherlands
Designated service	Account and deposit-taking services
Indicators	Business activity inconsistent with profile Co-mingling of funds Large international funds transfers

A suspect transaction report (SUSTR) submitted to AUSTRAC prompted further analysis of the financial activities of a suspected international drug trafficking syndicate. The syndicate comprised an Australian individual and businesses with links to an Indonesian furniture business.

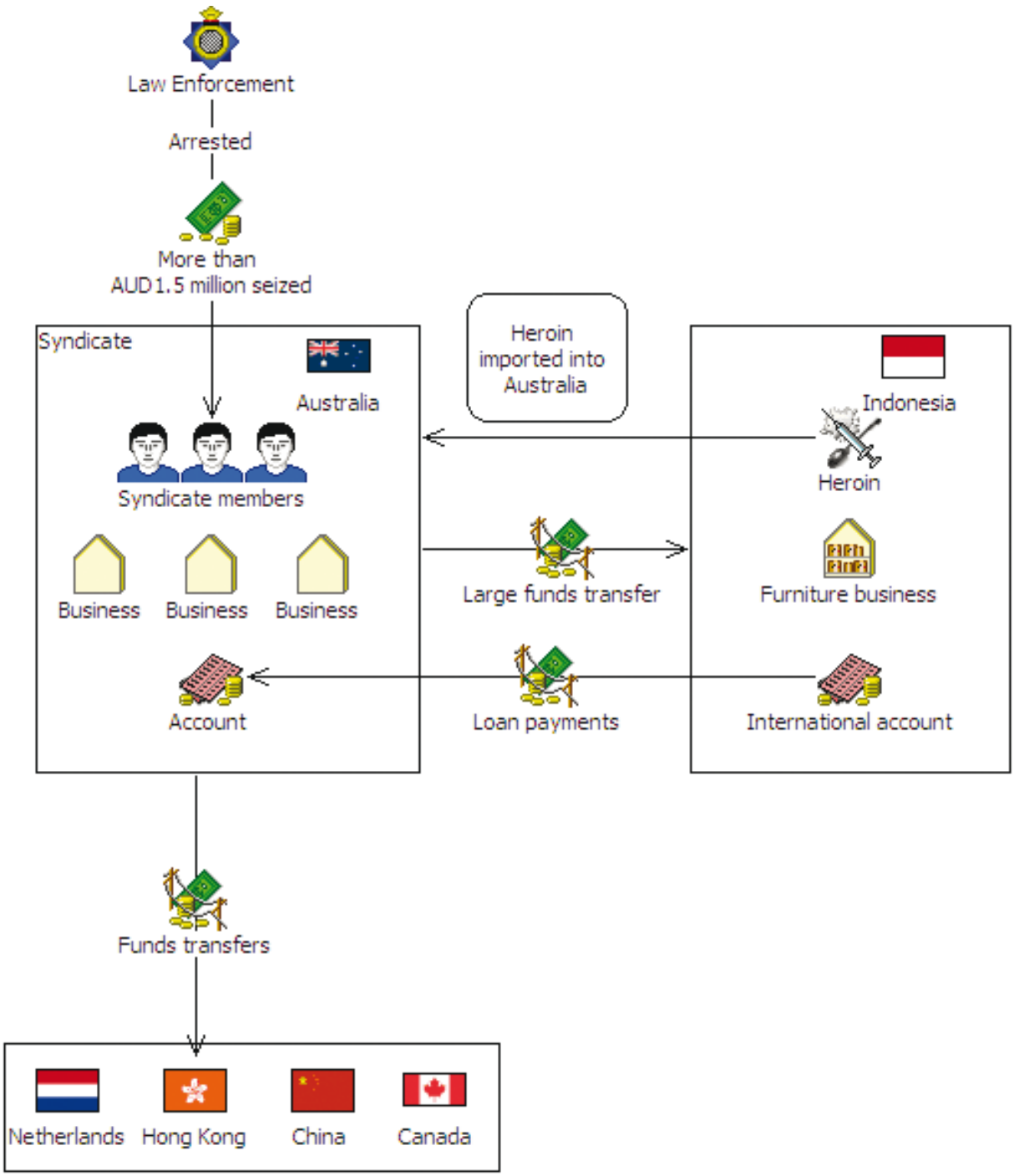
The SUSTR highlighted how members of the syndicate had conducted unusual, large international funds transfers to Indonesia. Further analysis of AUSTRAC information identified other outward funds transfers to Hong Kong, China, Canada and the Netherlands. The Indonesian furniture business was the main beneficiary of the international transfers, receiving a total of AUD480,000 sent by the syndicate and other unknown entities in Australia.

The Australian syndicate members were also the recipients of funds transfers from Australia to Indonesia. These outgoing payments were deposited into an international account associated with the furniture business. The syndicate members also received international funds transfers into their accounts in Australia – the transfer reports for these transactions described the transfers as loan repayments.

Law enforcement investigations identified that the furniture business was being used to import commercial quantities of heroin into Australia. The syndicate also used the furniture business to co-mingle illicit cash with legitimate funds to conceal the movement of funds offshore via international fund transfers.

Law enforcement officers arrested the syndicate members and seized more than AUD1.5 million in cash. Investigations identified that the syndicate was involved in an attempt to import 28 kilograms of heroin into Australia. Law enforcement officers intercepted 69 packages of heroin hidden inside three chests of drawers, part of a consignment of wooden furniture sent from Indonesia.

The law enforcement operation prevented a large amount of heroin from reaching Australian streets and disrupted an organised drug importation syndicate. Members of the syndicate were charged with importing and attempting to possess a commercial quantity of heroin.


Law Enforcement
Arrested
More than
AUD 1.5 million seized
Syndicate
Australia
Syndicate members
Business
Business
Business
Account
Heroin
imported into
Australia
Indonesia
Heroin
Large funds transfer
Furniture business
Loan payments
International account
Funds transfers
Netherlands
Hong Kong
China
Canada

Case 11 – Accountant laundered proceeds of $10 million tax evasion scheme

Offence	Tax evasion Money laundering
Customer	Individual Business
Industry	Professional services
Channel	Electronic
Jurisdiction	International – Vanuatu
Designated service	Account and deposit-taking services
Indicators	Funds transfers involving a tax haven * Use of false invoicing

* The Australian Taxation Office maintains a list of jurisdictions it considers to be tax havens. This list is available on the Tax Office website at <www.ato.gov.au>, and continues to be reviewed and updated as circumstances change.

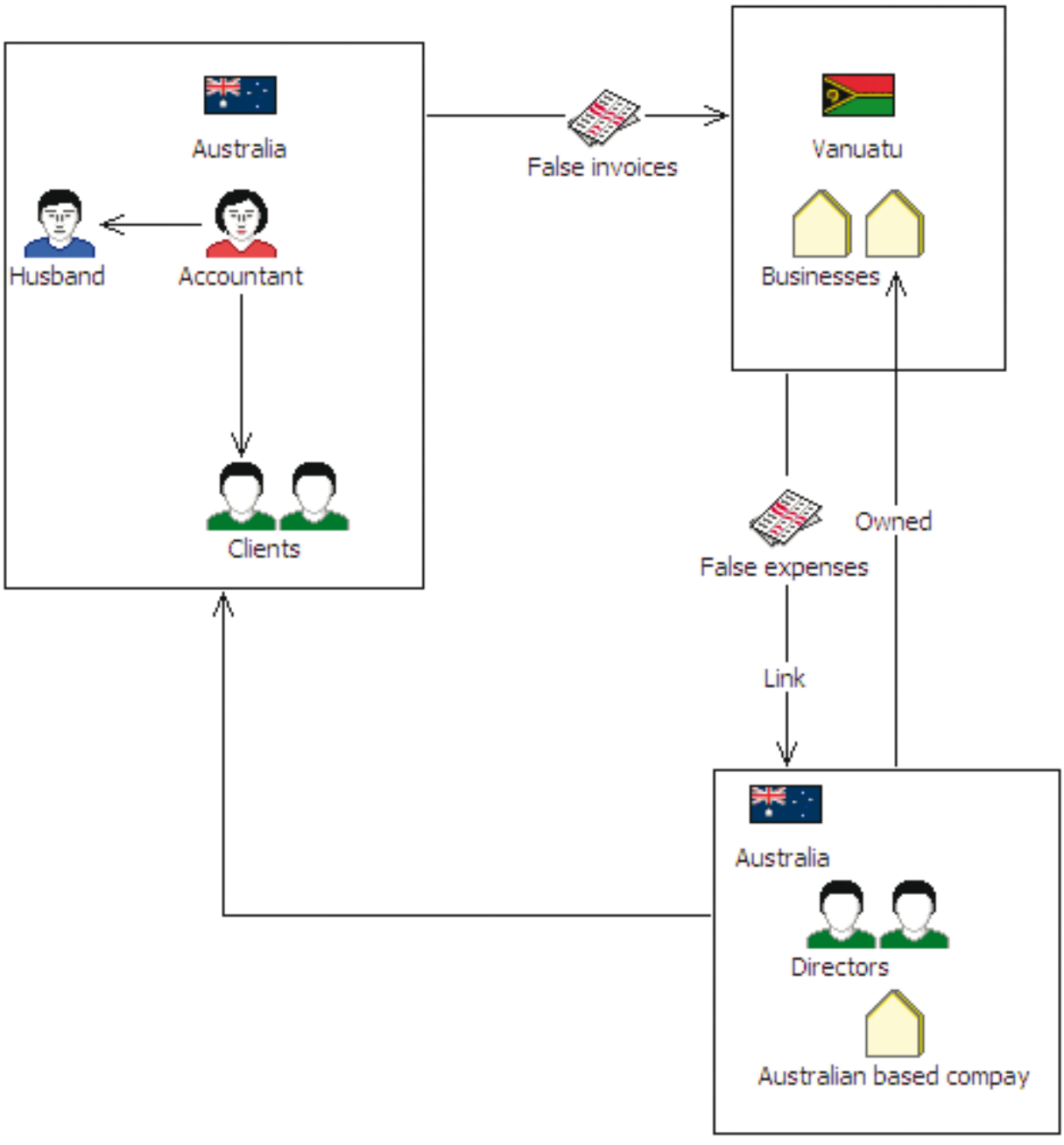
A Sydney accountant has been charged with 34 offences after she allegedly incorporated businesses in Vanuatu to help clients evade tax by laundering funds through a AUD10 million offshore tax evasion scheme.

Authorities allege that the accountant promoted and implemented the scheme on behalf of her Australian-based clients, and have investigated businesses in Vanuatu as part of their ongoing probe.

The accountant, her husband and ten of her clients have been charged with a total of 153 offences, including defrauding the Commonwealth, obtaining financial advantage by deception and using money as an instrument of crime.

The scheme allegedly involved the use of companies in Vanuatu, which were owned by the directors of Australian-based companies, to issue false invoices to the companies for services that were never actually provided. The companies then claimed tax deductions for the false expenses, while the funds held offshore were laundered back to the individuals in Australia to avoid being disclosed as income in tax returns.

To date, the investigation has traced AUD5.2 million allegedly laundered through the tax evasion scheme; however, authorities suspect that the matter could involve as much as AUD10 million in laundered funds.


Australia
Husband
Accountant
Clients
False invoices
Vanuatu
Businesses
False expenses
Owned
Link
Australia
Directors
Australian based compay

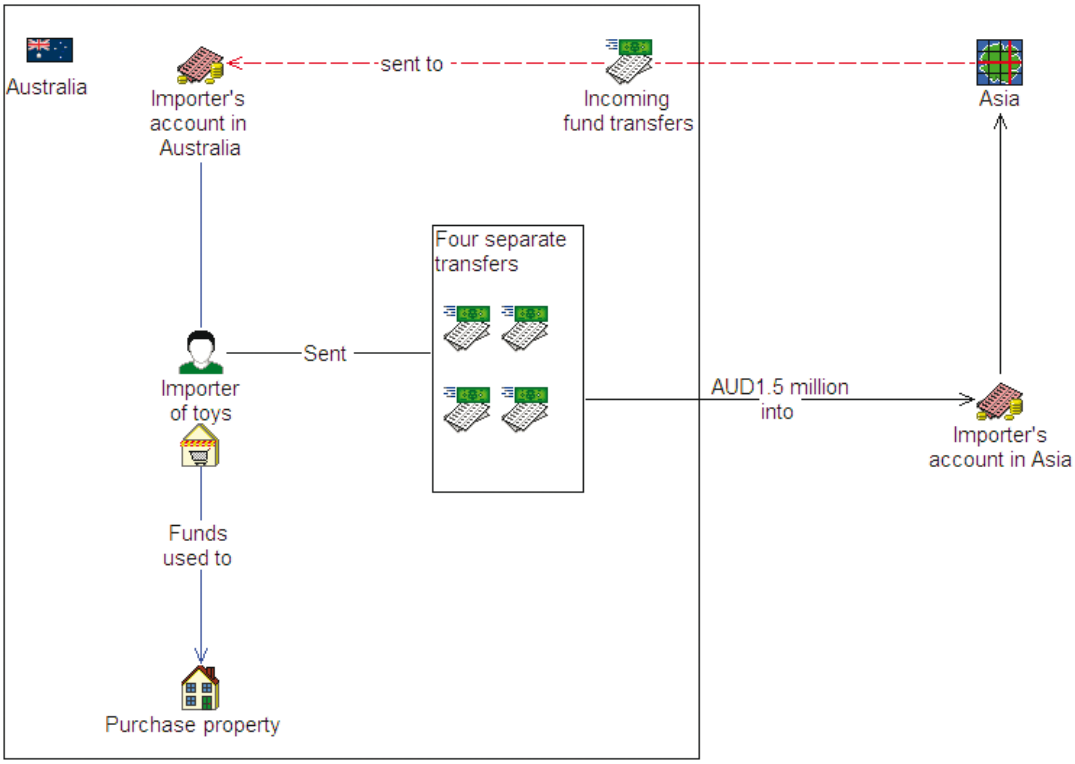
Case 12 – Toy importer avoided substantial tax obligations

Offence	Tax evasion
Customer	Business
Industry	Banking (ADIs) Real estate
Channel	Electronic
Jurisdiction	International – Asia
Designated service	Account and deposit-taking services
Indicators	Large international funds transfers Purchase of high-value assets (real estate)

An importer of toys and other items from Asia was suspected of attempting to avoid his tax obligations after failing to lodge tax returns, and an audit was conducted into his activities.

Investigations established that the importer had transferred more than AUD1.5 million into an account he held in Asia in four separate transfers. In addition, investigators noted incoming international funds transfers into the importer's Australian account; he was also found to have purchased an expensive residential property in Australia. The importer was unable to substantiate the source of the funds he had originally transferred to his overseas bank account.

Authorities took action against the importer and approximately AUD1 million in tax and penalties was raised.



Case 13 – Company profited from fraudulent tax deductions

Offence	Tax fraud
Customer	Business
Industry	Banking (ADIs)
Channel	Electronic
Jurisdiction	International – Europe
Designated service	Account and deposit-taking services
Indicators	Business activity inconsistent with profile

An Australian company was audited after information from an international counterpart government agency revealed that the company was fraudulently claiming tax deductions for research and development activities supposedly undertaken on behalf of a European company.

Financial transaction information indicated that the Australian company and one of the company directors had been the main beneficiaries of more than AUD1 million transferred to Australia from Europe. However, auditors discovered that the company had not included any relevant income in its taxation returns for the relevant years to explain the overseas transfers.

After repeated requests from the auditors to the company and its directors for clarification, the directors eventually claimed that the transfers represented loan repayments but were unable to provide satisfactory evidence to substantiate this. As a result, action was taken against the company and its directors and approximately AUD2.1 million in tax and penalties was raised.

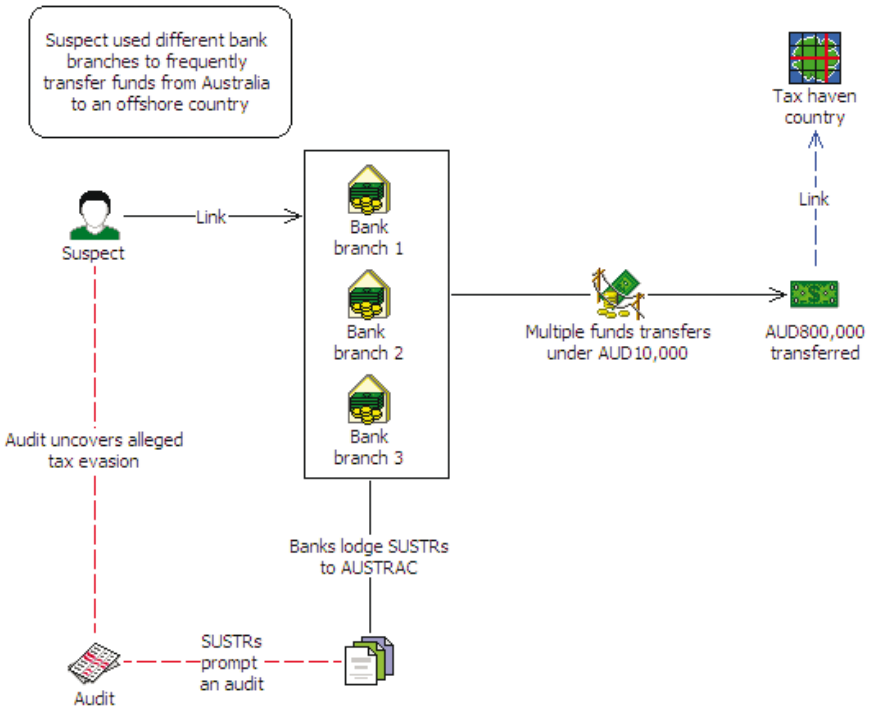
Case 14 – Suspect hid $800,000 in tax haven

Offence	Tax evasion
Customer	Individual
Industry	Banking (ADIs)
Channel	Electronic
Jurisdiction	International
Designated service	Account and deposit-taking services
Indicators	Funds transfers involving a tax haven* Multiple funds transfers below AUD10,000 Multiple transactions occurring on the same day from different geographical locations

* The Australian Taxation Office maintains a list of jurisdictions it currently considers to be tax havens. This list is available on the Tax Office website at <www.ato.gov.au>, and continues to be reviewed and updated as circumstances change.

Three different banks lodged suspect transaction reports (SUSTRs) with AUSTRAC describing the suspicious activities of a bank customer. These reports prompted an audit of the suspect's affairs and it was discovered that the suspect was attempting to evade taxation obligations.

The SUSTRs showed that the suspect was making numerous international funds transfers to a tax haven destination* in amounts just less than AUD10,000. The suspect often sent three or more transfers on the same day from different bank branches. AUSTRAC information indicated that the suspect had sent more than AUD800,000 offshore over a two-and-a-half-year period in an attempt to avoid paying tax.



Case 15 – Illegal tobacco smugglers caught

Offence	Illegal tobacco importation
Customer	Individual Business
Industry	Banking (ADIs)
Channel	Electronic
Jurisdiction	International – New Zealand, Middle East
Designated service	Account and deposit-taking services
Indicators	Co-mingling of funds†

† While this customer behaviour may not be directly observable by reporting entities, it is an activity commonly used to facilitate or hide money laundering and other offences.

A law enforcement agency discovered a shipping container in New Zealand, destined for Australia, which allegedly contained illicit tobacco products. The container originated in the Middle East and, following its arrival in New Zealand, the shipping agents received instructions to forward the container on to Australia.

'Transhipment', in which international cargo passes through a third country on the way to its final destination, is one method used by criminal groups attempting to prevent illegally imported goods being detected. However, in this case, the container was held at the New Zealand shipping agent for some time and the intended recipient in Australia was required to pay storage fees before the shipping agent would release the container.

AUSTRAC information identified an international funds transfer from Australia to pay the New Zealand shipping agent, enabling law enforcement officers to identify the intended recipient of the illicit tobacco products in Australia.

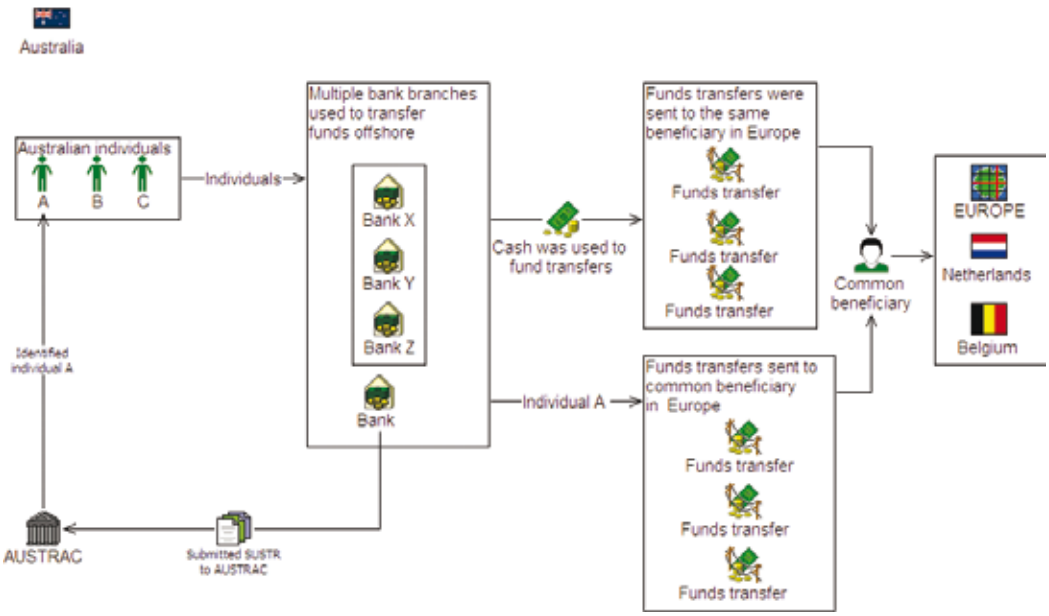
Due to the low cost of illicit tobacco products in the Middle East the importers attempted to disguise payment for the tobacco within their normal business activities. The importers' legitimate business activity included regular international transactions, providing a veil of legitimacy under which to import products illegally.

Case 16 – Overseas funds transfers helped identify European drug merchants

Offence	Drug importation
Customer	Individual
Industry	Banking (ADIs)
Channel	Physical (face-to-face) Electronic Agent/third party
Jurisdiction	International – Belgium, the Netherlands
Designated service	Account and deposit-taking services
Indicators	Cash payments for funds transfers Multiple geographical locations used to conduct transfers Multiple low-value funds transfers Use of third parties to conduct international funds transfers

In prior years, law enforcement investigations have uncovered criminal associates making international funds transfers from Australia to common beneficiary customers in Belgium and the Netherlands to import drugs. The subsequent law enforcement actions resulted in multiple drugs seizures.

In this case, a suspect transaction report (SUSTR) submitted to AUSTRAC assisted law enforcement officers investigating a suspected Eastern European crime network involved in the importation of drugs. The SUSTR detailed the activities of an individual using banks to send low-value international funds transfers to a beneficiary who held accounts in Belgium and the Netherlands. Investigators also identified two more individuals in Australia using multiple bank branches to transfer funds in amounts less than AUD10,000 to this same European beneficiary. These individuals all paid for the funds transfers with cash.



Case 17 – International money launderer imprisoned

Offence	Money laundering
Customer	Individual
Industry	Banking (ADIs)
Channel	Physical (face-to-face)
Jurisdiction	International – Middle East, Indonesia
Designated service	Account and deposit-taking services
Indicators	Large cash transactions conducted over a short period of time Large international funds transfers Multiple funds transfers conducted from the same location Use of false identification documentation (to conduct transactions, etc.)

AUSTRAC disseminated a number of suspect transaction reports (SUSTRs) to a partner law enforcement agency, triggering an investigation that led to the arrest of a large-scale money launderer.

AUSTRAC information identified a number of international funds transfers to Indonesia and the Middle East via various companies. The overseas transfers included a total of approximately AUD225,000 sent to accounts in Indonesia. The overseas beneficiary customers had previously come to the attention of law enforcement agencies during a related investigation.

The suspect in the case used a bank branch to transfer approximately AUD150,000 to a recipient in the Middle East using a company account. A week later, the suspect used the same bank branch to make two more transfers, for AUD50,000 each, also to the Middle East. The following day the suspect once again attended the same branch and attempted to transfer approximately AUD290,000 from a company account to an account in the Middle East using a false identity. Bank staff became suspicious about the authenticity of the identification provided by the suspect, and the transaction was declined.

The suspect's attempt to use false identification sparked the investigation and he was later arrested by police while in possession of two drivers licences showing different identities.

It was discovered that, in all, the suspect had transferred, or had attempted to transfer, approximately AUD911,000 from Australia to accounts in the Middle East and Indonesia. Law enforcement officers were able to restrain approximately AUD290,000 in funds prior to them being transferred. The suspect was charged under section 29(4)(b) of the *Financial Transaction Reports Act 1988* with making a false statement and causing a cash dealer to make a false report, and sentenced to three years imprisonment. The offender was also charged with dealing with the proceeds of crime under section 400.4 of the *Criminal Code Act 1995* and sentenced to a further nine months imprisonment.

Case 18 – Significant amphetamines importation seized

Offence	Drug importation
Customer	Individual
Industry	Banking (ADIs)
Channel	Physical (face-to-face)
Jurisdiction	International – Asia
Designated service	Account and deposit-taking services
Indicators	Departure from Australia shortly after making funds transfers[†] Structured transactions Withdrawing all, or nearly all, funds from an account within a short period of time

[†] While this customer behaviour may not be directly observable by reporting entities, it is an activity commonly used to facilitate or hide money laundering and other offences.

An investigation into a suspected drug importation operation resulted in a significant drug seizure by law enforcement officers in Australia. The main Australian suspect in the operation was involved in the transfer of approximately AUD127,000 to Australia prior to the importation, allegedly to cover the operation's administrative expenses. The suspect also used account details of other associates to transfer structured amounts of cash into Australia.

In addition, just prior to the importation of the drugs, the main suspect withdrew all of the funds from a co-conspirator's account via a series of withdrawals structured to fall below the AUD10,000 transaction reporting threshold. These funds were then transferred to a single account in Asia. The main suspect left Australia for a destination in Asia within days of completing these transactions.

The law enforcement investigations resulted in the seizure of 412 kilograms of amphetamines which had been imported into Australia, and the arrest of two individuals who were each sentenced to 14 years imprisonment. The main suspect was also arrested four years later and sentenced to 14 years imprisonment for his involvement in the operation.

Case 19 – Secret cash payment used to avoid stamp duty and launder money

Offence	Fraud Money laundering
Customer	Individual
Industry	Real estate Banking (ADIs)
Channel	Physical (face-to-face)
Jurisdiction	Domestic
Designated service	Account and deposit-taking services
Indicators	Client purchases or sells real estate above or below the market value while apparently unconcerned about the economic disadvantages of the transaction Large cash deposit

A vendor and purchaser colluded to transfer a property at an agreed price but then record the formal transaction price as significantly lower than the agreed price. The purchaser paid the difference between the two prices to the vendor in cash, which was not recorded on any of the formal conveyancing documents.

The vendor deposited the cash into his bank account on a date close to the date on which the contracts for the sale of the property were exchanged, indicating to law enforcement officers that the cash actually formed part of the total sale price.

Understating the official sale price of the property was an act of fraud allowing the offenders to avoid paying the required amount of stamp duty on the property. It is also suspected that the cash involved in the transaction was the proceeds of other criminal activities, and that the transaction was an attempt to launder the illicit cash through the real estate sector.

Law enforcement action was taken against the offenders and the property in question was seized under the *Proceeds of Crime Act 2002*.

Case 20 – Foreign students used to launder funds

Offence	Structuring
Customer	Individual
Industry	Banking (ADIs)
Channel	Agent/third party Electronic Physical (face-to-face)
Jurisdiction	Domestic
Designated service	Account and deposit-taking services
Indicators	Purchase of bank cheques Structured transactions Third parties used to open bank accounts Use of multiple accounts for deposits Use of student accounts after their departure from Australia Use of third parties to conduct transactions

Suspect transaction reports (SUSTRs) submitted to AUSTRAC by bank officers assisted an investigation into two individuals suspected of structuring deposits into multiple bank accounts to avoid the AUD10,000 transaction reporting threshold of the *Financial Transaction Reports Act 1988* (FTR Act).

One of the suspects involved in the offence was a bank employee who assisted the main suspect to avoid AUSTRAC reporting requirements by depositing AUD16,000 in two AUD8,000 amounts into the main suspect's bank accounts. The main suspect also purchased numerous bank cheques valued under AUD10,000 which were deposited into a high-interest bank account.

The main suspect also employed five students to make deposits into her account. She signed the forms and provided the cash for the deposits. The bank employee and the main suspect then opened accounts for the five students, with the main suspect as signatory to the accounts. The main suspect then deposited large volumes of funds into these accounts through structured transfers, even after some of the students had left the country. The main suspect then transferred these funds from the students' accounts to her personal account.

As a result of the investigation, the bank employee was charged with structuring transactions under section 31 of the FTR Act. The main suspect was also charged with structuring transactions under section 31 of the FTR Act and was found guilty on 12 counts.

Case 21 – Kidnapped daughter safely returned from Thailand

Offence	Kidnapping Structuring
Customer	Individual
Industry	Banking (ADIs)
Channel	Physical (face-to-face) Electronic
Jurisdiction	International – United Kingdom, Indonesia, Greece, Thailand
Designated service	Account and deposit-taking services
Indicators	Frequent cash deposits made over a short period of time Large cash deposit Similar transactions conducted over a short period of time Structuring of transactions Unusual customer behaviour

Law enforcement officers investigating a man they suspected of kidnapping his daughter requested information from AUSTRAC about any accounts linked to the man, or to members of his family, in Australia and the United Kingdom.

AUSTRAC information included several suspect transaction reports (SUSTRs) lodged by two different banks detailing how the suspect had made structured cash deposits into his accounts. One SUSTR described how the suspect had entered the bank with a bag of AUD100 notes and asked for assistance to count them. The cash totalled AUD30,000 and the suspect deposited AUD10,000, keeping the rest. He re-entered the same branch shortly after to deposit a further AUD5,000. Additional SUSTRs submitted by the banks described cash deposits made by the suspect in amounts just under the AUD10,000 transaction reporting threshold.

Further analysis of AUSTRAC information uncovered additional addresses and bank accounts linked to the suspect. The information revealed a series of international funds transfers sent from the United Kingdom and Indonesia to the suspect's accounts in Australia. The information also indicated that the suspect had been sending international transfers to Greece.

The suspect was arrested in Thailand and charged with detaining a person with intent to hold for ransom, demanding money with menaces, and kidnapping. The daughter was safely returned to her mother.

Case 22 – International drug syndicate uncovered

Offence	Drug importation
Customer	Individual
Industry	Banking (ADIs) Real estate
Channel	Electronic
Jurisdiction	International – Peru, United Kingdom
Designated service	Account and deposit-taking services
Indicators	Co-mingling of funds† Purchase of high-value assets (real estate)

† While this customer behaviour may not be directly observable by reporting entities, it is an activity commonly used to facilitate or hide money laundering and other offences.

An organised crime group became the focus of a law enforcement investigation after it was suspected that they were importing cocaine from Peru and supplying it to nightclubs in Australia.

AUSTRAC information allowed investigating officers to identify the main suspect in the group and then further reveal that he held three separate bank accounts with different banks. AUSTRAC information also revealed six financial transactions of interest to law enforcement authorities, including a significant cash transaction report (SCTR) and an international funds transfer to the United Kingdom. Several of the transactions were in excess of AUD10,000.

The reports allowed authorities to serve warrants on the three banks to obtain the complete transactional history of the suspect's accounts. A search warrant executed on the suspect's apartment revealed a small amount of amphetamines and AUD6,000 in cash. Authorities believe that the main suspect had been using his cash-based business to launder funds from criminal activities. The suspect also owned an apartment worth more than AUD1 million which is believed to have been purchased with the proceeds of his illegal activities.

Case 23 – Suspicious behaviour linked to large-scale identity fraud

Offence	Fraud
Customer	Individual
Industry	Banking (ADIs)
Channel	Physical (face-to-face) Electronic
Jurisdiction	International – Jordan, United Arab Emirates, Peru
Designated service	Account and deposit-taking services
Indicators	Account operated by someone other than the owner Large cash withdrawals with a bank cheque Large international funds transfers Transactions inconsistent with customer profile Unusual customer behaviour Use of third party accounts Withdrawing nearly all funds from an account in a short period of time

A bank teller submitted a suspect transaction report (SUSTR) to AUSTRAC detailing suspicious banking transactions. This report assisted authorities investigating a syndicate allegedly involved in large-scale identity fraud.

The report described over-the-counter bank transactions in which two people were involved – the account owner and the main suspect. The suspect was not connected to the account by any documentation, but controlled the transactions and would not allow the account owner to speak.

The pair transferred approximately AUD541,000 from a bank account in Jordan to an Australian account. They then withdrew approximately AUD394,000 from the Australian account using a bank cheque. When the teller requested the account owner undertake this withdrawal, the suspect became agitated and aggressive. The pair also transferred approximately AUD147,000 from the Australian account to a third party account. These transactions left the account owner with an account balance of just AUD1,000.

AUSTRAC information allowed authorities to link the suspect in this matter with the movement of funds to Jordan, the United Arab Emirates and Peru. Authorities continued their investigations and ultimately commenced proceeds of crime action against the suspect and members of the syndicate, and restrained approximately AUD1.6 million in assets, including real estate and cash.

Case 24 – Student received suspicious $100,000 cash deposit

Offence	Money laundering
Customer	Individual
Industry	Banking (ADIs)
Channel	Physical (face-to-face) Agent/third party
Jurisdiction	Domestic
Designated service	Account and deposit-taking services
Indicators	Account activity inconsistent with customer profile Multiple transactions on the same day Large cash deposit Use of inactive account Use of third party to conduct transactions

Authorities began investigating the activities of a student after a bank lodged a suspect transaction report (SUSTR) with AUSTRAC describing a large cash deposit made into the student's account.

The SUSTR described a deposit of AUD100,000 cash made into the account by a third party claiming to be a relative of the student. The bank also indicated that a deposit of AUD26,000 had previously been made into the same account at the same branch. Prior to these deposits there had been little activity in the student's account. The large deposits were inconsistent with the student's profile and past account activity and authorities continued investigating the student's apparent unexplained wealth.

Further enquiries revealed that the funds had then been withdrawn from the account with a bank cheque and that the cheque had been made out to a company. Law enforcement officers suspected the funds were the result of illicit activities and took action to restrain them.

Case 25 – Director illegally used company funds to buy real estate

Offence	Fraud Structuring
Customer	Individual
Industry	Banking (ADIs) Real estate
Channel	Physical (face-to-face)
Jurisdiction	Domestic
Designated service	Account and deposit-taking services
Indicators	Company account used for personal use Purchase of high-value assets (real estate) Structured transactions

A director of a company under liquidation dishonestly used company funds to purchase real estate. A suspect transaction report (SUSTR) lodged by the company's liquidator established that company funds had been withdrawn from the organisation's account during the liquidation period. The SUSTR sparked an investigation which revealed that the director had purchased real estate with company funds, using cheques in the amount of AUD9,500 to avoid the AUD10,000 transaction reporting threshold.

The director was charged and subsequently pleaded guilty to two counts of dishonestly using his position as a director to gain a personal advantage in breach of the *Corporations Act 2001*, and one charge of structuring transactions to avoid reporting under the *Financial Transaction Reports Act 1988*. The director received a three-year suspended prison sentence for the offences.

Case 26 – Internet bargains too good to be true

Offence	Fraud
Customer	Individual
Industry	Banking (ADIs)
Channel	Electronic (internet)
Jurisdiction	Domestic
Designated service	Account and deposit-taking services
Indicators	Use of false documentation Use of internet shopping sites

A law enforcement investigation into suspicious offers on internet shopping sites led to a criminal syndicate being dismantled and the arrest of two men for selling AUD4.5 million worth of goods bought with fake credit cards. It is alleged the syndicate amassed AUD1.3 million after selling 6,000 items on one site alone.

The investigation began after officers were tipped off about major retailers' gift cards being offered at discount rates on internet shopping sites.

Investigating officers searched a number of properties, including a post office where some items were allegedly stored while waiting to be posted. The searches revealed a large number of items, including computers, high-pressure steam cleaners and dozens of bottles of Penfolds Grange wine worth AUD700 each. It is believed that the items were purchased with fake credit cards bearing account details stolen from legitimate cardholders. A large number of fraudulent credit cards and drivers licenses were also seized.

One suspect was arrested and charged with four counts of knowingly dealing with the proceeds of crime, while the other suspect was charged with two counts.

Case 27 – South-East Asian 'textiles' company at centre of drugs syndicate

Offence	Drug trafficking
Customer	Individual
	Business
Industry	Banking (ADIs)
Channel	Physical (face-to-face)
	Electronic
	Agent/third party
Jurisdiction	International – South-East Asia
Designated service	Account and deposit-taking services
Indicators	Multiple funds transfers below AUD10,000
	Multiple funds transfers to common beneficiaries
	Use of third parties to conduct transactions

By analysing a series of international funds transfers to South-East Asia, AUSTRAC identified a suspect involved in drug trafficking. The suspect transferred approximately AUD220,000 offshore, mostly to beneficiaries in South-East Asia and generally in amounts of around AUD9,000. In one month alone the individual transferred almost AUD150,000 overseas. Importantly, bank staff lodged a suspect transaction report (SUSTR) informing AUSTRAC that the individual was using non-residents to conduct international transfers on his behalf.

An analysis of the transfers revealed that one of the primary beneficiaries in South-East Asia was a company purportedly involved in textiles and chemicals. Investigators identified additional Australian-based individuals also conducting multiple funds transfers to the overseas company and to various other beneficiaries in the same country. In total, approximately AUD250,000 was sent to the company. This pattern strongly suggested to authorities that a network of individuals in Australia was using these international funds transfers for a common purpose.

Law enforcement officers investigated the matter and uncovered a multinational drug trafficking syndicate.

Case 28 – Front company helped suspect profit from major conflict of interest

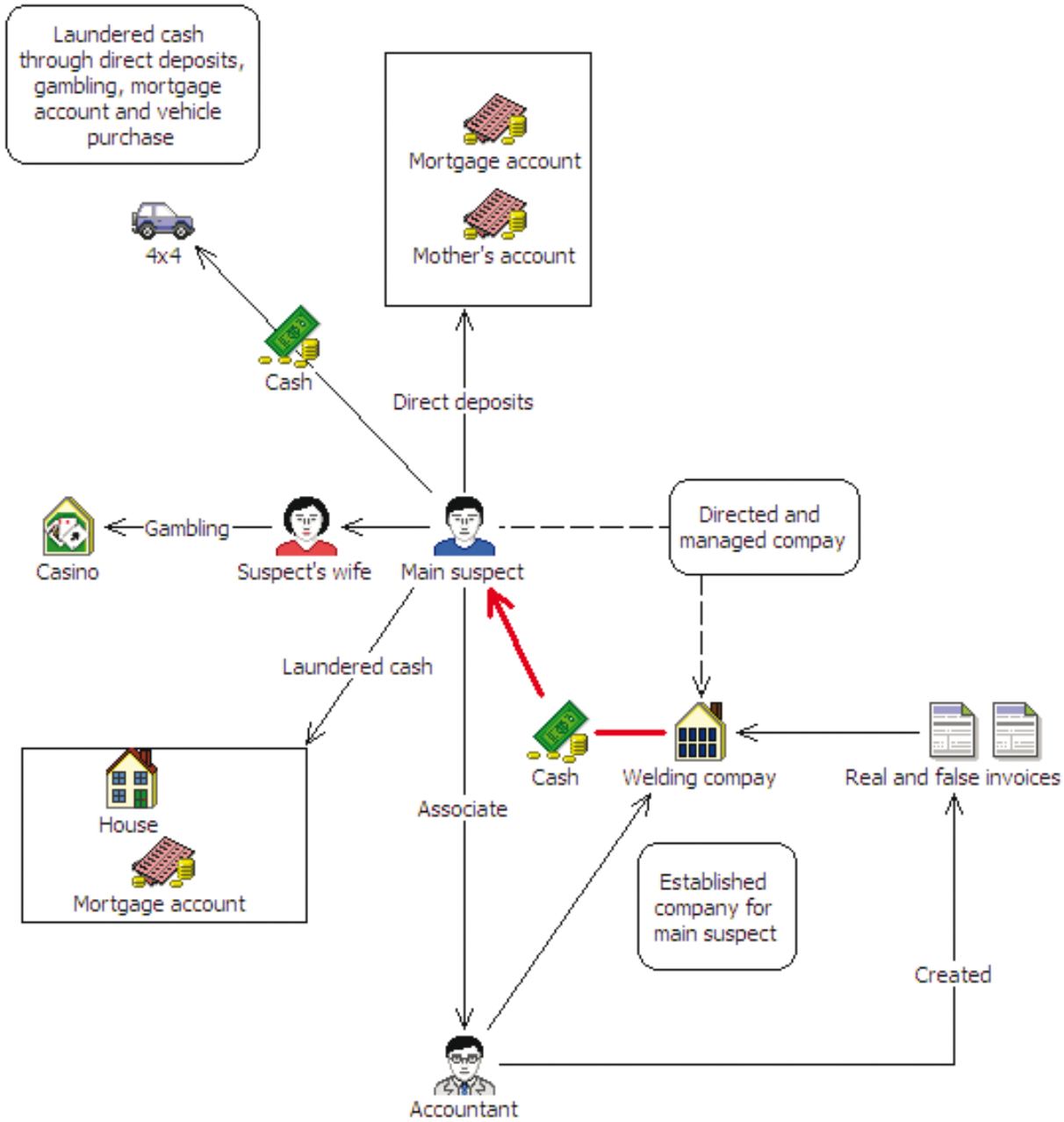
Offence	Fraud Money laundering
Customer	Individual
Industry	Banking (ADIs) Professional services Financial advisors/planners Real estate Gambling
Channel	Physical (face-to-face)
Jurisdiction	Domestic
Designated service	Account and deposit-taking services AFSL holder arranging a designated service Gambling services
Indicators	Purchase of high-value assets (real estate, vehicles) Low-value property purchased with improvements paid for in cash before re-selling Use of false documentation Use of false invoices Use of family member accounts Use of gatekeepers (accountant)

The main suspect in this case wanted to establish a profitable welding company but did not want to be legally associated with the company due to a professional conflict of interest. An associate of the main suspect, a certified accountant with no criminal history, became the legal and apparent senior staff member of the welding company, while the main suspect actually directed and managed the company, albeit without any legal standing to do so.

The accountant administered both real and false invoices to create the illusion that funds moving through the welding company were from legitimate commercial activity. He also drew up cash cheques and cashed these on a weekly or fortnightly basis. Frequently, these cash withdrawals from company accounts were for amounts greater than the AUD10,000 transaction reporting threshold. Bank staff did not become suspicious of these regular withdrawals due to the apparently legitimate nature of the transactions. The accountant then gave this cash to the main suspect, allowing the main suspect to receive profits while remaining at arm's length from the official business of the company.

The main suspect attempted to launder the cash proceeds through direct deposits into a mortgage account, deposits into his mother's credit union account, and the private cash purchase of a four-wheel drive vehicle. He also attempted to launder cash through accounts and through a mortgage for real estate which was in his father-in-law's name, but which was in fact operated by him. The property subject to the mortgage was established in a trust, although legal advice indicates that this was not a legitimate trust. The main suspect paid for improvements to this property with cash. Both the main suspect and his wife also gambled significant sums of money.

The welding company later became the focus of a corruption investigation which uncovered the illicit activities of the main suspect. The investigation further revealed that the company accountant was also a registered tax agent, a financial planner and a finance broker. In addition to the false invoicing and cash withdrawals he undertook for the welding company, he also supplied false documentation to clients wishing to misrepresent their financial status. These false documents included documents understating the income of clients who were attempting to avoid paying child support and documents overstating the incomes of clients applying for loans.


Laundered cash through direct deposits, gambling, mortgage account and vehicle purchase
Mortgage account
Mother's account
4x4
Cash
Direct deposits
Casino
Gambling
Suspect's wife
Main suspect
Directed and managed compay
Laundered cash
House
Mortgage account
Cash
Welding compay
Real and false invoices
Associate
Established company for main suspect
Created
Accountant

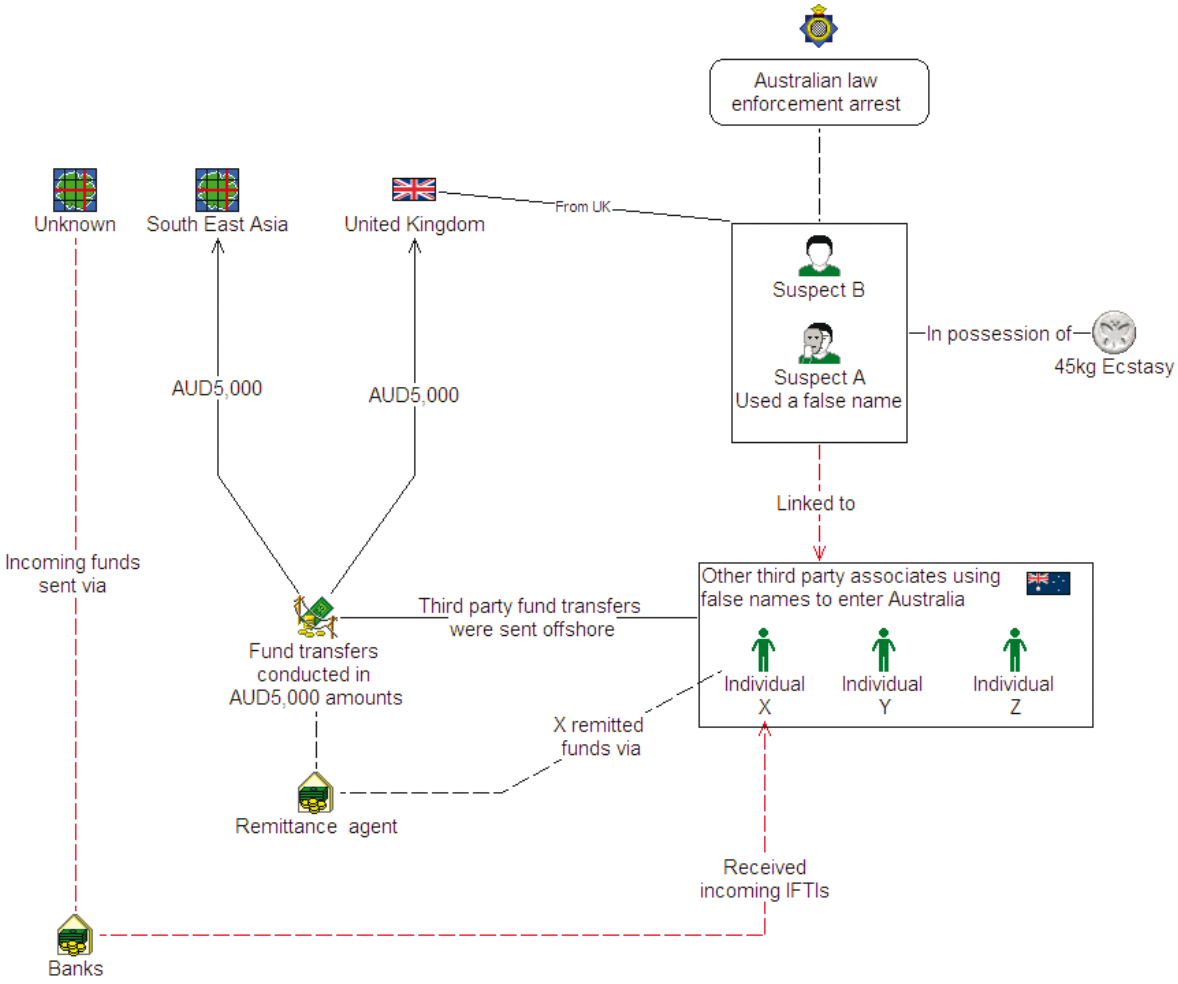
Case 29 – False identification central to ecstasy importation ring

Offence	Drug importation
Customer	Individual
Industry	Authorised deposit-taking institutions Currency exchange Remittance services
Channel	Electronic
Jurisdiction	International – United Kingdom, South-East Asia
Designated service	Account and deposit-taking services Currency exchange services Remittance services (money transfers)
Indicators	Multiple funds transfers below AUD10,000 Use of false identification documentation (to conduct transactions, etc.)

A law enforcement investigation led to the arrests of two suspects and the discovery of a large quantity of drugs. The suspects, who were originally from the United Kingdom (UK), were arrested in Australia in possession of 45 kilograms of ecstasy. Searches of AUSTRAC data revealed that one of the suspects was using a false identity, a fact confirmed by investigators.

AUSTRAC information also revealed that a number of associates of the two suspects were remitting funds from Australia to South-East Asia and the UK. Some of these associates were also operating under false names, after entering Australia from the UK using false identification documents.

The associates usually transferred funds overseas in amounts of less than AUD10,000, typically around AUD5,000. The main suspect in this group conducted the overseas transfers via remittance agents while also receiving incoming international funds transfer instructions (IFTIs) through a bank. Other associates in this group transferred money out of Australia using banks, money remitters and foreign exchange services.


Australian law enforcement arrest
Unknown
South East Asia
United Kingdom
From UK
Suspect B
Suspect A
Used a false name
In possession of
45kg Ecstasy
AUD5,000
AUD5,000
Linked to
Incoming funds sent via
Third party fund transfers were sent offshore
Other third party associates using false names to enter Australia
Individual X
Individual Y
Individual Z
Fund transfers conducted in AUD5,000 amounts
X remitted funds via
Remittance agent
Received incoming IFTIs
Banks

Case 30 – Super funds robbed of $1.5 million

Offence	Superannuation fraud
Customer	Individual
Industry	Banking (ADIs) Professional services
Channel	Physical (face-to-face) Electronic
Jurisdiction	International – Lithuania, other Eastern European country
Designated service	Account and deposit-taking services Debit card access facilities
Indicators	Frequent cheque deposits Funds withdrawn from overseas account through ATMs in Australia Similar transactions conducted over a short period of time Use of false company Use of false documentation

Law enforcement officers launched a major investigation into a sophisticated superannuation fraud valued at AUD1.5 million.

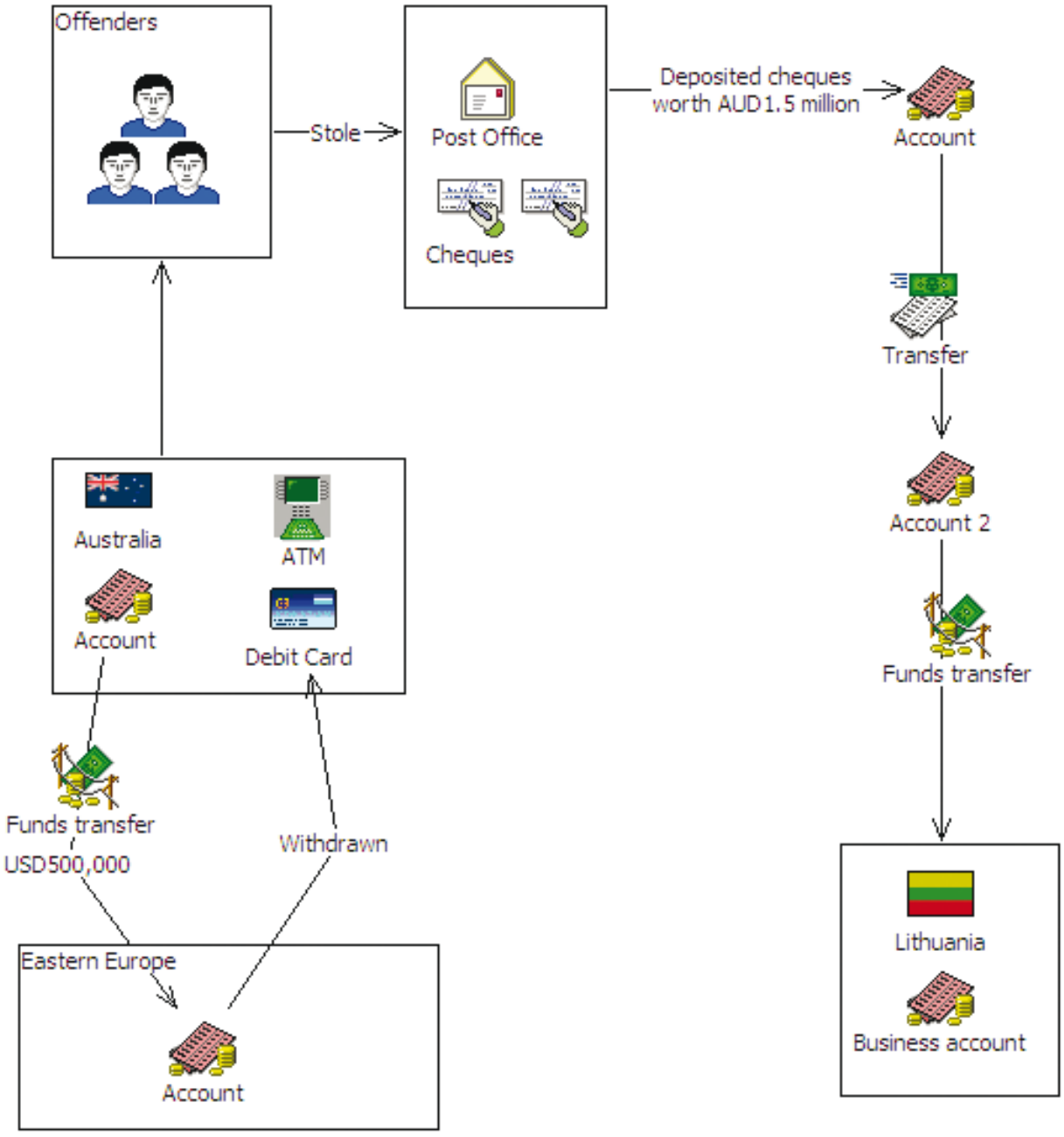
The offenders stole superannuation rollover cheques belonging to a legitimate industry superannuation fund from a post office. The cheques had been posted and delivered to the post office, where they were stolen from the superannuation fund's locked post office box.

The offenders registered a bogus business name similar to that used by the legitimate superannuation fund and opened two bank accounts using the registration papers of the new business. The first account was used to clear the cheques and deposit the stolen funds, from which they were transferred across to the second account. From the second account the funds were transferred to a Lithuanian business account. In total, 91 stolen cheques worth AUD1.5 million were deposited into the two accounts.

A bank submitted a suspect transaction report (SUSTR) to AUSTRAC after a suspect involved in the network deposited cheques that the bank believed were stolen.

AUSTRAC also received a report from a financial intelligence unit (FIU) in another Eastern European country about a business bank account opened in that country. Over a short period of time approximately USD500,000 had been transferred into the account from Australia. Most of the funds in this overseas account were then withdrawn through ATMs in Australia using debit cards linked to the account. Information from the Eastern European FIU assisted Australian authorities to identify the offenders and their accounts in Australia. Authorities subsequently froze the two Australian accounts; however, by this time a balance of only USD70,000 remained in the accounts.

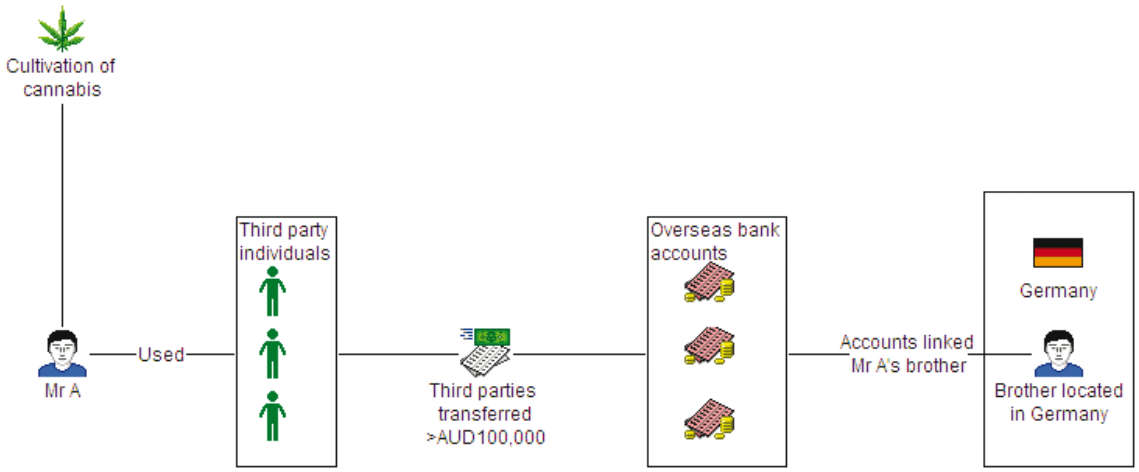
In total, the fraud is estimated to have cost the bank more than AUD700,000. The main offender was arrested and pleaded guilty to dealing with proceeds of crime (in excess of AUD1 million), stealing mail articles and breaking, entering and stealing. He was sentenced to nine years imprisonment with a six year non-parole period.


Offenders
Stole
Post Office
Cheques
Deposited cheques worth AUD1.5 million
Account
Transfer
Account 2
Funds transfer
Lithuania
Business account
Australia
ATM
Account
Debit Card
Funds transfer
USD500,000
Withdrawn
Eastern Europe
Account

Case 31 – Third parties used to sneak drug money overseas

Offence	Drug cultivation
Customer	Individual
Industry	Banking (ADIs)
Channel	Agent/third party Electronic Physical (face-to-face)
Jurisdiction	International – Germany
Designated service	Account and deposit-taking services Remittance services (money transfers)
Indicators	Multiple low-value transfers Use of third parties to conduct transactions

Law enforcement officers investigating the illegal cultivation of cannabis suspected that an individual involved in the activity was transferring illicit funds overseas. Investigators suspected that the individual was using third parties to transfer the funds to bank accounts in Germany held in his brother's name. Analysis of AUSTRAC information confirmed the investigators' suspicions and revealed that more than AUD100,000 had been transferred to the overseas accounts. The third parties transferred the funds in small amounts, always under AUD4,000, using both banks and money remitters for the transfers.



Case 32 – Online dating service used in attempted scam

Offence	Fraud
Customer	Individual
Industry	Banking (ADIs) Remittance services
Channel	Electronic (internet)
Jurisdiction	International – Nigeria, Spain, United States, United Kingdom
Designated service	Account and deposit-taking services Remittance services (money transfers)
Indicators	Activity inconsistent with customer profile Multiple funds transfers below AUD10,000 Multiple transactions occurring on the same day to the same beneficiary Use of multiple remitters in the same geographical location Use of variations when spelling names/addresses

Law enforcement officers began investigating a woman who was using a web-based email address to contact men through an online dating service. The woman said she was the 32-year-old daughter of an oil tycoon, on holiday in Asia with her father. The woman claimed to have conducted a business deal without her father's knowledge and wanted to send the AUD650,000 in proceeds to Australia to keep the deal secret from him. In return for accepting the funds, the woman offered the recipient of the email a commission of 29 per cent of the total transfer amount.

AUSTRAC also received a series of suspect transaction reports (SUSTRs) about the activities of the woman and a second individual, triggering AUSTRAC's automated monitoring system. AUSTRAC data suggested that the woman and the second individual were probably related, and were possibly mother and son.

AUSTRAC analysis showed specific patterns in the suspects' suspicious activities:

- Funds were sent to common recipients in Nigeria, Spain, the United States and the United Kingdom. Over a six-month period the two suspects transferred a total of AUD139,000 – activity out of character with their usual financial activity as they had no previous transactions recorded within AUSTRAC's database.
- Most of the transactions were outgoing international funds transfers instructions (IFTIs) sent through a money remitter service, and on one occasion by a bank. Some transfers were sent to the same recipients on the same day, whereas other transfers were made on alternate days, often to common recipients. The transactions were conducted at multiple remitters in the same region, and on two occasions via a remitter's internet facilities.
- One remittance provider noted that in several instances the pair had used variations when spelling names, addresses and other transaction details, and appeared to have undertaken transactions in amounts less than AUD10,000 in an attempt to avoid the perceived threshold reporting requirement.

Further analysis of AUSTRAC data revealed connections between the recipients in Spain and Nigeria and a number of other individuals in Australia, who had previously been the subject of SUSTRs.

Case 33 – Fake documents used for shares fraud

Offence	Fraud
Customer	Individual
Industry	Banking (ADIs) Real estate Securities and derivatives
Channel	Electronic
Jurisdiction	International – United States
Designated service	Account and deposit-taking services Securities market/investment services
Indicators	Purchase of high-value assets (real estate) Use of false documentation

The suspect, an owner and operator of a debt recovery business operating in Australia, established a number of accounts with an Australian bank. The suspect then opened a new account with a financial services company. She telephoned the company and informed them that in the course of managing her debt recovery business she was entitled to sell a portfolio of shares belonging to a third party based overseas. The suspect also faxed the company a letter allegedly from the owner of the shares authorising her to sell them. Despite this documentation and the phone call, the financial services company refused to execute the sale, stating that the instruction to sell the shares must come directly from the owner of the shares, or that the shares must first be registered in the suspect's name.

The shares were held by a share registry business which then received written notice, allegedly from the owner of the shares, stating that the shares should be sold and the proceeds paid to the suspect.

The suspect again contacted the financial services company, informing them that the shares had been transferred to her name and providing the required reference numbers. The company checked these reference numbers against those held by the share registry business and concluded that the shares had been legitimately transferred to the suspect. Acting on instructions from the suspect, the financial services company sold the shares and transferred the proceeds to her Australian bank account.

Shortly afterwards, the original owner of the shares contacted the financial services company claiming that authority had not been given for the shares to be sold. Law enforcement officers acted on this claim and arrested the suspect and her husband for the suspected fraudulent sale of the shares.

Investigations showed that the funds from this fraud had been transferred from the suspect's account into various term deposits, used for property purchases or transferred to a beneficiary in the United States.

Case 34 – AUSTRAC information helped shut down early release super scam

Offence	Superannuation fraud
Customer	Individual
Industry	Professional services
Channel	Electronic
Jurisdiction	Domestic
Designated service	Account and deposit-taking services Stored value cards
Indicators	Multiple funds transfers below AUD10,000 Transactions inconsistent with customer profile Use of stored value cards

AUSTRAC information assisted authorities investigating a man allegedly operating an illegal early release superannuation scheme. AUSTRAC received a number of suspect transactions reports (SUSTRs) suggesting that the individual was operating such a scheme, and disseminated these reports to authorities. AUSTRAC information showed that the operator of the scheme had transferred the funds generated by the scheme overseas in amounts of less than AUD10,000. He had also used cash to add more than AUD98,000 onto a stored value card.

The operator of the scheme was charged under the *Superannuation Industry (Supervision) Act 1993*, restricted from leaving Australia and prevented from providing any further financial services or disposing of any assets.

Case 35 – Part-time 'farmer' transferred $600,000 to Brazil

Offence	Drug trafficking Money laundering
Customer	Individual
Industry	Remittance services Currency exchange
Channel	Physical (face-to-face) Electronic
Jurisdiction	International – Brazil
Designated service	Currency exchange services Remittance services (money transfers) Travellers cheque exchange services
Indicators	Income inconsistent with customer profile Multiple funds transfers involving a high-risk drug country Purchase of travellers cheques with cash Structured transactions

AUSTRAC began monitoring the financial activities of a suspect after reporting entities submitted a series of suspect transaction reports (SUSTRs) which detailed his activities and triggered AUSTRAC's automated monitoring system. AUSTRAC prepared a report detailing the suspect's suspicious activities and passed it on to a law enforcement partner agency. Prior to receiving the information from AUSTRAC, law enforcement officers had already suspected the man of being a possible drug trafficker or money launderer based on his unexplained wealth and frequent travel and funds transfers to Brazil.

Over four years the suspect transferred AUD611,000 from Australia to Brazil through international remittances, the purchase of travellers cheques and foreign currency exchange. Of that total, 98 per cent (AUD601,000) was transferred within a two-year period. Reports detailing the suspect's activities reported his preference for transactions in amounts less than the AUD10,000 transaction reporting threshold and his preference for using cash or travellers cheques when transferring money to Brazil.

The individual informed reporting entities that he lived in Rio de Janeiro for six months of the year, where he owned a motel. His occupation was listed as farmer and small business operator, which were unlikely sources of income for the large amounts of funds the individual was transferring to Brazil. The recipient of all the international remittances appeared to be a relative, probably the man's son.

Case 36 – Casino 'high roller' defrauded banks of millions

Offence	Fraud
Customer	Individual
Industry	Gambling Banking (ADIs)
Channel	Physical (face-to-face)
Jurisdiction	Domestic
Designated service	Gambling services Loan services
Indicators	Client is a known frequent gambler and/or high roller at a casino Numerous loan applications for less than AUD25,000 Same or similar methods used to acquire more than one bank loan Use of false identification documentation (to conduct transactions, etc.)

A casino high roller defrauded banks out of millions of dollars by obtaining several hundred loans using false documents. The offender created the documents on his computer in a garage and submitted the completed loan applications from internet cafes. The offender committed the frauds to fund his gambling habit and to pay off casino gambling debts he owed to loan sharks.

The vast majority of the loan applications were for less than AUD25,000 as there were fewer customer verification requirements for people applying for loans of this size than for those applying for larger loans. Many of the loans were arranged to repeatedly purchase the same motor vehicle from the same seller.

The offender gambled most of the money at the casino and other venues around the state. In just three months the offender gambled more than AUD6.6 million at a casino.

Authorities tracked the offender's frauds for two years. They found that over eight months he had obtained 131 loans, worth more than AUD2 million, through various retail branches of a particular bank.

Additionally, the offender and his associates were also known within their ethnic communities as organisers of fraudulent personal loans. The offender arranged the fraudulent loans for fellow gamblers facing large gambling debts, and charged large commissions for the service. It is suspected that the offender operated the fraudulent loan operation from the casino he frequented.

Law enforcement officers linked the main offender to as many as 900 loans obtained using false documents. One Australian bank was forced to write off around AUD1.5 million in loan defaults to the offender and one of his associates.

The offender pleaded guilty in court to 13 charges of fraud involving 36 loans worth AUD781,282. He faced a further two charges for attempting to use a AUD65,000 bank cheque which was not his property. His associate pleaded guilty to 11 charges of fraud involving 37 loans worth AUD760,782. He also pleaded guilty to using a false Australian citizenship certificate to obtain a drivers licence.

Case 37 – Suspicious overseas transfer exposed Eastern European crime syndicate

Offence	Drug importation Money laundering
Customer	Individual
Industry	Remittance services
Channel	Agent/third party Electronic Mail Physical (face-to-face)
Jurisdiction	International – Eastern Europe
Designated service	Remittance services (money transfers)
Indicators	Purchase of bank drafts by third parties Use of third parties to conduct transactions Use of third-party accounts

An investigation into the operations of an international crime syndicate commenced after AUSTRAC referred a suspicious international funds transfer instruction (IFTI) to a law enforcement partner agency. Further investigation by the law enforcement agency revealed that the funds were the proceeds of a large Eastern European organised crime syndicate. The investigation led to the discovery of an Australian drug lab and the seizure of more than 100,000 ecstasy pills.

The investigation found that money launderers had originally used contacts in Eastern Europe to provide an underground money remittance service for Eastern European residents in Australia wishing to send funds back to their families. At the time alternative remittance arrangements were the only option available to remit money to the region. None of these overseas remittances were reported to AUSTRAC. After official banking channels were established to the region, the underground remittance activity continued, albeit primarily for criminal associates of the money launderers.

The money laundering operation was based on the activities of one family, which used a variety of methods to disguise their money laundering. They arranged secret meetings to exchange and collect funds, and used third parties and third-party accounts to remit funds to distance the remitters and the beneficiaries from the transactions. The money launderers also employed third parties to send funds overseas by purchasing and either mailing or couriering bank drafts.

Case 38 – Suspicious transactions led to ecstasy seizure

Offence	Drug importation
Customer	Individual
Industry	Remittance services
Channel	Electronic Agent/third party
Jurisdiction	International – United Kingdom
Designated service	Remittance services (money transfers)
Indicators	Multiple deposits made to same overseas account by different people Multiple low-value funds transfers Use of third parties to conduct transactions

A routine search of AUSTRAC information by a law enforcement partner agency identified a number of related transactions that appeared suspicious. The transactions were international funds transfers undertaken by both overseas visitors and Australian residents, and the nature and extent of the transactions suggested to authorities that they may have involved criminal activity.

The suspects sent multiple funds transfers from Australia to common beneficiaries in the United Kingdom. The group conducted 34 outgoing transfers, totalling AUD123,000, mostly through money remitters. A suspect transaction report (SUSTR) was also lodged with AUSTRAC, identifying additional associates linked to the group of suspects.

This AUSTRAC information contributed to a law enforcement investigation which ultimately foiled an attempt to import drugs and led to the interception of 2.5 kilograms of ecstasy and a small quantity of cocaine.

Case 39 – Large overseas transfers exposed illegal workers

Offence	Illegal immigration
Customer	Individual
Industry	Remittance services
Channel	Electronic
Jurisdiction	International – China, Philippines, Malaysia, Russia
Designated service	Remittance services (money transfers)
Indicators	Multiple funds transfers below AUD10,000 Same home address provided for funds transfers by different people

AUSTRAC information was used to help uncover a number of non-Australian citizens, mainly from China, working illegally in Western Australia. The illegal workers were employed in the construction industry – namely plastering – and were transferring funds to their families overseas, usually through a money transfer agency.

Utilising AUSTRAC data, investigating officers were able to identify as many as six workers who provided the same home address when undertaking international funds transfers over a 12-month period.

The workers linked to this address transferred a total of AUD284,077 overseas, mostly to China but also to the Philippines, Malaysia and Russia. The workers ensured all of these outgoing international funds transfers were for amounts of less than AUD10,000.

Authorities established that workers did not hold current visas and charged and detained them under the *Migration Act 1958*. They were removed from Australia to their home countries, each incurring a three-year exclusion period from returning to Australia and a debt to the Commonwealth for their detention and removal costs.

Case 40 – Illegal immigration operation uncovered

Offence	Fraud Illegal immigration
Customer	Individual
Industry	Remittance services
Channel	Electronic
Jurisdiction	International – China
Designated service	Remittance services (money transfers)
Indicators	Multiple low-value funds transfers Same address given for funds transfers by different people Use of false identification documentation (to conduct transactions, etc.)

An investigation by authorities identified an overseas national suspected of operating a bank account under a false name and possessing a false passport. The investigation also linked this main suspect with four more non-Australian residents who were either on bridging visas or awaiting the outcome of visa applications.

AUSTRAC information indicated that this group of five women, all non-Australian residents, had conducted a total of 30 international transfers through a money transfer agency, the transfers totalling AUD327,290. In the process of conducting the transfers all had given a home address which authorities suspected to be that of a brothel.

Further investigations into the main suspect's travel movements showed that she had initially entered Australia with an escort who subsequently departed Australia the next day. Authorities have noted this same travel arrangement being used by other individuals entering Australia on false passports via Perth International Airport.

As in this case, many groups facilitating illegal entries into Australia are highly organised: the group provided the suspect with a doctored Malaysian passport which incorporated an actual photograph of the suspect, allowing her to pass through Australian immigration and then establish identities under her own name as well as her false name.

This case is also consistent with some past instances of Chinese nationals using doctored Malaysian photo identification to enter Australia and then lodge claims for Protection visas. In many cases, the applicants were not legitimately seeking Protection visas, but instead using the claim to prolong their stay in Australia while they worked.

The main suspect in this case was convicted with possessing a false passport and operating a bank account in a false name under the *Foreign Passports (Law Enforcement and Security) Act 2005*.

Case 41 – Remittance dealer laundered $93 million for organised crime

Offence	Money laundering Drug trafficking
Customer	Individual
Industry	Remittance services
Channel	Electronic Physical
Jurisdiction	International – Vietnam, Cambodia, Hong Kong, other South-East Asian countries
Designated service	Remittance services (money transfers)
Indicators	Structuring of funds transfers Use of cash couriers Use of multiple remittance service providers to transfer funds to common overseas beneficiaries

A law enforcement investigation revealed that a number of organised crime syndicates were using a network of money remittance dealers in Sydney and Melbourne to launder the proceeds of drug importation and distribution operations.

The network of money remitters was controlled by a husband and wife and the wife's mother in Vietnam. The money remitters operated out of several shops, which were used by suspects from major Asian crime syndicates based in Victoria and New South Wales. The suspects transferred money to syndicates in Cambodia, Hong Kong and other South-East Asian nations.

The money remitters used various methods to prevent authorities from detecting their money laundering activities. These methods included:

- failing to report transactions to AUSTRAC
- concealing the identity of their clients and the overseas recipients
- using other remitters to reduce the size of the international transfers and conceal the frequency of the international transfers
- paying airline pilots to physically carry large amounts of cash overseas.

Employees of major banks were also investigated for their failure to report large-volume deposits and transfers made through the remittance dealers' bank accounts.

Investigators charged the proprietors of the money remittance providers and associated businesses with laundering in excess of AUD93 million. One of the airline pilots pleaded guilty to money laundering under the *Criminal Code Act 1995* and was sentenced to four-and-a-half years imprisonment.

Case 42 – Superannuation 'early release' scam foiled

Offence	Superannuation fraud
Customer	Individual
Industry	Superannuation
Channel	Electronic
Jurisdiction	International – Philippines, Pacific Island nations
Designated service	Superannuation and approved deposit funds
Indicators	Common bank accounts identify and link superannuants, facilitators and organisers Multiple low-value international funds transfers Significant cash withdrawals from superannuation accounts Unusual bank account activity into and out of superannuation account/s

A network of individuals established an unlicensed financial services business offering clients early access to their superannuation funds. This business acted as trustee for a self managed superannuation fund (SMSF).

It is alleged that the preserved superannuation benefits of 121 clients, worth more than AUD3.5 million, were deposited into the SMSF's bank accounts. These funds were rolled over from 11 legitimate superannuation funds. The SMSF managers then allegedly obtained early access to these benefits and withdrew and distributed the funds to the clients. As part of this process the fund managers retained commissions totalling more than AUD685,000 from the clients' funds.

The fund managers were aware that they had a legal obligation to preserve the benefits until their clients had satisfied a condition of release such as retiring or reaching 65 years of age; however, it appears the managers had no intention of complying with this obligation.

AUSTRAC received a suspect transaction report (SUSTR) about this early release scheme and identified one of the suspects operating the scheme.

The suspects transferred the commissions from the scam out of Australia through a regular series of low-value international funds transfers to the Philippines and Pacific Island nations.

Appendix A

Indicators of potential money laundering/terrorism financing activity

There are numerous indicators which may act as 'red flags' for reporting entities to identify potential money laundering or terrorism financing activity.

Although a single indicator does not necessarily indicate illicit activity, the existence of a 'red flag' indicator should encourage further monitoring and examination. In most cases it is the existence of multiple indicators that raises a reporting entity's suspicion of potential criminal activity, and influences their response to the situation.

Anti-money laundering and counter-terrorism financing (AML/CTF) officers should include these money laundering/terrorism financing indicators in staff training, and encourage their staff to use these indicators when describing suspicious behaviours for inclusion in suspect transaction or suspicious matter reports.

Money launderers and terrorism financiers will continuously look for new techniques to obscure the origins of illicit funds to give the appearance of legitimacy to their activities. AML/CTF officers should continually review their products, services and individual customers to ensure their internal AML/CTF systems and training remain effective.

The list below features indicators which appear within the case studies of this report, and should be treated as a non-exhaustive guide.

- account activity inconsistent with customer profile
- account operated by someone other than the owner
- betting accounts with large deposits but with minimal betting activity
- business activity inconsistent with business profile
- cash payments for funds transfers
- cash withdrawals from betting accounts in cheques and vouchers
- client is a known frequent gambler and/or high roller at a casino
- client purchases or sells real estate above or below the market value while apparently unconcerned about the economic disadvantages of the transaction
- co-mingling of illicit funds with legitimate sources of income
- common bank accounts identify and link superannuants, facilitators and organisers
- company account used for personal use
- departure from Australia shortly after making funds transfers
- frequent cash deposits made over a short period of time
- frequent cheque deposits
- funds transferred to overseas account but then withdrawn in Australia
- funds transfers involving a tax haven*
- funds transfers to numerous offshore jurisdictions with no business rationale
- funds withdrawn from overseas account through ATMs in Australia
- income inconsistent with customer profile
- large cash deposit
- large cash transactions conducted over a short period of time
- large cash withdrawals with a bank cheque
- large funds transfers after gambling activity
- large international funds transfers
- large number of accounts held by customer with the same institution
- low-value property purchased with improvements paid for in cash before re-selling
- multiple deposits made to same overseas account by different people
- multiple funds transfers below AUD10,000

* The Australian Taxation Office maintains a list of jurisdictions it considers to be tax havens. This list is available on the Tax Office website at <www.ato.gov.au>, and continues to be reviewed and updated as circumstances change.

- multiple funds transfers conducted from the same location
- multiple funds transfers involving a high-risk drug country
- multiple funds transfers to common beneficiaries
- multiple geographical locations used to conduct transfers
- multiple low-value funds transfers
- multiple transactions occurring on the same day from different geographical locations
- multiple transactions occurring on the same day to the same beneficiary
- multiple transactions on the same day
- numerous large deposits via ATMs
- numerous loan applications for less than AUD25,000
- outgoing transfer with corresponding incoming funds transfer – appears to be a 'u-turn' transaction
- purchase of bank cheques
- purchase of bank drafts by third parties
- purchase of high-value assets (e.g. real estate, luxury vehicles)
- purchase of travellers cheques with cash
- same-day transactions at different geographical locations
- same home address provided for funds transfers by different people
- same or similar methods used to acquire more than one bank loan
- significant cash withdrawals from superannuation accounts
- similar transactions conducted over a short period of time
- structuring of funds transfers or transactions
- structuring of gambling purchases, payouts and withdrawals
- third parties used to open bank accounts
- transactions inconsistent with customer profile
- unusual bank account activity into and out of superannuation account/s
- unusual customer behaviour
- unusual pattern of phone betting transactions
- use of cash couriers
- use of company accounts for personal use
- use of false company
- use of false identification documentation (to conduct transactions, etc.)
- use of false invoices
- use of family member accounts
- use of gatekeepers (e.g. accountant)
- use of inactive account
- use of international credit card
- use of internet shopping sites
- use of multiple accounts for deposits
- use of multiple remittance service providers to transfer funds to common overseas beneficiaries
- use of multiple remitters in the same geographical location
- use of stored value cards
- use of student accounts after their departure from Australia
- use of third parties to conduct international funds transfers
- use of third parties to conduct transactions
- use of third party accounts
- use of variations when spelling names/addresses
- value of funds transfers inconsistent with customer profile
- withdrawing all, or nearly all, funds from an account within a short period of time.

Appendix B

Further information on money laundering/ terrorism financing typologies

International AML/CTF organisations

Financial Action Task Force (FATF)
www.fatf-gafi.org

Asia/Pacific Group on Money Laundering (APG)
www.apgml.org

Egmont Group of Financial Intelligence Units
www.egmontgroup.org

AUSTRAC links

AUSTRAC
www.austrac.gov.au

AUSTRAC educational resources
www.austrac.gov.au/typologies.html
www.austrac.gov.au/education.html

FATF typologies work

Each year the FATF holds its global typologies exercise, which includes active participation by the APG and other regional anti-money laundering bodies. From this exercise the FATF publishes reports on industry sectors and money laundering and terrorism financing topics of global interest. The FATF website (listed above) features new FATF typologies reports as they are finalised and released.

FATF typology reports – 2008

Major topics include:

- money laundering and terrorist financing vulnerabilities of commercial websites and internet payment systems
- money laundering and terrorist financing risk assessment strategies
- FATF terrorist financing typologies report.

FATF typology reports – 2007

Major topics include:

- money laundering and terrorist financing through the real estate sector
- laundering the proceeds of Value Added Tax carousel fraud report.

FATF typology reports – 2006

Major topics include:

- trade based money laundering
- report on new payment methods
- the misuse of corporate vehicles including trust and company service providers.

FATF typology reports – 2005

Major topics include:

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

FATF typology reports – 2004

Major topics 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
- the role of 'gatekeepers' or non-financial professions in money laundering.

FATF typology reports – 2003

Major topics 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 typology reports – 2002

Major topics 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.

Index

Glossary and abbreviations

Glossary of terms

alternative remittance systems	Sometimes referred to as 'underground banking', these systems exist and operate outside traditional banking and financial channels. They typically involve little or no regulation and minimal documentation, and operate through networks of funds transfer agents who accept funds from remitters and deliver funds to recipients. In many cases these systems bypass the standard inter-bank funds transfer and settlement system.
beneficiary (or beneficiary customer)	This is the person (or organisation) who is the ultimate recipient of funds being transferred.
co-mingling	The process of combining the profits of illicit activities with the profits of a legitimate business to disguise the illicit funds and make them appear legitimate.
condition of release	Regulatory conditions that must be met before a superannuation benefit can be paid (e.g. reaching age 65, etc.)
restraint (of funds etc.)	A court order directing that the money, property, etc. suspected to be involved in a crime can only be disposed of or dealt with as directed by the court.
structuring	Also known as 'smurfing', this is a money laundering technique which involves the distribution of a large amount of cash into a number of smaller deposits to evade threshold reporting requirements. It could also involve the layering of funds for international funds transfers in an effort to avoid scrutiny of the transfers.
u-turn transactions	An international transaction where money transferred out of a country is immediately followed by an incoming transfer back into the country, without any obvious business rationale or logical explanation.

Abbreviations

ADIs – authorised deposit-taking institutions

AML/CTF Act – *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*

APG – Asia/Pacific Group on Money Laundering

ATM – automatic teller machine

AUD – Australian dollars

AUSTRAC – Australian Transaction Reports and Analysis Centre

EFT – electronic funds transfer

FATF – the Financial Action Task Force

FTR Act – *Financial Transaction Reports Act 1988*

GST – Goods and Services Tax

IFTI – international funds transfer instruction

ML/TF – money laundering/terrorism financing

OMSF – organised missing supplier fraud

PIN – personal identification number

RSAs – retirement savings accounts

SCTR – significant cash transaction report [1]

SMR – suspicious matter report

SUSTR – suspect transaction report [2]

UK – United Kingdom

USD – United States dollars

1 significant cash transaction reports are submitted to AUSTRAC under the FTR Act, in respect of a currency transaction involving AUD10,000 or more. As of 12 December 2008, the AML/CTF Act equivalent is the **threshold transaction report** (TTR),

2 suspect transaction reports are submitted to AUSTRAC under the FTR Act when a cash dealer has reasonable grounds to suspect that a transaction may be relevant to investigation of an offence against an Australian law. As of 12 December 2008, the AML/CTF Act equivalent is the **suspicious matter report** (SMR).

AUSTRAC Typologies and Case Studies Report 2009 feedback form

Your feedback is important and will assist us in planning future Typologies and Case Studies Reports and other resources. Please take the time to complete this form.

1. Please identify your type of organisation.

2. Please indicate how useful you found each section of this Typologies and Case Studies Report.

(1 = Not Useful, 5 = Very Useful)

	1	2	3	4	5
Report methodology (p5)					
Financial crime and money laundering threats and methodologies (p7)					
Reporting suspicious matters (p10)					
Case studies (pp12–61)					
Case study narratives					
'Red flag' indicators listed for each case					
Link diagrams for cases studies (where applicable)					
Appendix A – Consolidated list of indicators (p62)					
Appendix B – Further ML/TF information (p64)					
Index (p65)					

3. What section or case study in this report did you find the most helpful or interesting? Please explain why:

4. What information did you find least helpful or interesting? Please explain why:

5. What new issues, trends, or patterns in money laundering/terrorism financing would you like to see addressed in future Typologies and Case Studies Reports (or in other AUSTRAC resources)?

Please be specific (for example, you may be interested in more information about specific money laundering methods or typologies, new technologies, industries or designated services, or types of transactions):

Please return this completed feedback form to:

By post

Typologies and Feedback Unit
Australian Transaction Reports and Analysis Centre (AUSTRAC)
PO Box 5516
West Chatswood NSW 1515

By fax 02 9950 0820

By email TYPOLOGIES_&_FEEDBACK@austrac.gov.au

How can I contact AUSTRAC?

You can contact the AUSTRAC Help Desk
on 1300 021 037 between 8:30am to 5:00pm
[Eastern Standard Time] on weekdays
or email help_desk@austrac.gov.au

For more information visit:

www.austrac.gov.au

Australian Government

Australian Transaction Reports and Analysis Centre