Australian Government

Australian Transaction Reports and Analysis Centre

AUSTRAC

typologies and case studies report 2013

Contents

Introduction

The Australian Transaction Reports and Analysis Centre (AUSTRAC) is Australia's anti-money laundering and counter-terrorism financing (AML/CTF) regulator and specialist financial intelligence unit (FIU).

AUSTRAC's purpose is to protect the integrity of Australia's financial system and contribute to the administration of justice through its expertise in countering money laundering and the financing of terrorism.

AUSTRAC's role

As Australia's AML/CTF regulator, AUSTRAC oversees industry's compliance with the requirements of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) and the *Financial Transaction Reports Act 1988* (FTR Act). Where AUSTRAC detects cases of serious non-compliance with the AML/CTF Act or FTR Act, it may take appropriate and measured enforcement action to secure a regulated entity's compliance.

Entities subject to the AML/CTF Act include financial services providers, bullion dealers, designated remittance service providers, the gambling industry and other reporting entities which provide 'designated services' as outlined in section 6 of the AML/CTF Act. AUSTRAC also regulates 'cash dealers', as defined in the FTR Act.

As Australia's FIU, AUSTRAC analyses the financial transaction reports submitted by industry and disseminates the financial intelligence obtained from these reports to its partner agencies to assist them in their investigations.

AUSTRAC's partner agencies include Australian Government law enforcement, national and border security, revenue, regulatory and human services agencies, as well as state and territory law enforcement and revenue agencies. AUSTRAC also works closely with its international counterparts to contribute to global AML/CTF efforts.

Typologies and case studies report

AUSTRAC offers a range of education and guidance to assist industry in complying with its AML/CTF obligations. The *AUSTRAC typologies and case studies report 2013* is one example of such guidance. The case studies within this report highlight the value of industry's reporting of financial transactions and suspicious matters to AUSTRAC.

The case studies demonstrate how following the money trail is an effective way of detecting the activities of organised crime networks. The cases also highlight the value of a whole-of-government approach to combating organised crime. They detail successes achieved through AUSTRAC and revenue, regulatory and law enforcement agencies working together and sharing information about criminal activities.

Report types

In carrying out its AML/CTF regulatory functions, AUSTRAC receives financial transaction reports and reports of suspicious matters from regulated entities.

These reports are submitted by entities in the financial, cash carrying, bullion and gambling sectors that provide designated services under the AML/CTF Act. AUSTRAC also receives a small number of reports from 'cash dealers' regulated under the FTR Act.

AUSTRAC also receives certain cross-border movement reports from the general public.

The following details the five report types which AUSTRAC receives:

International funds transfer instruction (IFTI) reports – Under the AML/CTF Act, if a reporting entity sends or receives an instruction to or from a foreign country, to transfer money or property, that entity must submit an IFTI report.

Suspicious matter reports (SMRs) – Under the AML/CTF Act, a reporting entity must submit an SMR if, at any time while dealing with a customer, the entity forms a reasonable suspicion that the matter may be related to an offence, tax evasion, or the proceeds of crime. Entities must submit SMRs to AUSTRAC within three days of forming the suspicion (or within 24 hours for matters related to the suspected financing of terrorism). The equivalent report type for entities regulated under the FTR Act is the suspect transaction report (SUSTR).

Threshold transaction reports (TTRs) – Under the AML/CTF Act, if a reporting entity provides a designated service to a customer involving the transfer of currency (coin or paper money) or e-currency of AUD10,000 or more (or the foreign equivalent), then the reporting entity must submit a TTR. The equivalent report type for entities regulated under the FTR Act is the significant cash transaction report (SCTR).

Cross-border movement of physical currency (CBM-PC) reports – Under the AML/CTF Act, CBM-PC reports are submitted when physical currency of AUD10,000 or more (or the foreign equivalent) is carried, mailed or shipped into or out of Australia. When a person carries the currency, a CBM-PC report must be completed at the first Customs and Border Protection examination area upon entry into Australia or before leaving Australia. When a person mails or ships the currency into or out of Australia, a CBM-PC report must be submitted within five business days of the currency being received in Australia, or at any time before the currency is sent out of Australia.

Cross-border movement of bearer negotiable instrument (CBM-BNI) reports – Under the AML/CTF Act, CBM-BNI reports must be completed by persons entering or leaving Australia who are carrying bearer negotiable instruments (such as travellers cheques, cheques or money orders) of any amount, if asked by a Customs and Border Protection or police officer to complete such a report.

Industry's contribution to combating money laundering and terrorism financing

AUSTRAC engages with industry in order to develop a more complete and detailed picture of the money laundering environment in Australia, including vulnerabilities and emerging threats.

AUSTRAC analyses the reports it receives from reporting entities to uncover patterns of criminal activity. AUSTRAC disseminates this financial intelligence to its partner agencies for use in their criminal investigations and other operations.

AUSTRAC assists reporting entities to detect and deter money laundering by increasing their understanding of the money laundering and terrorism financing (ML/TF) vulnerabilities for their industry and the designated services they provide. By strengthening their internal AML/CTF controls and programs, reporting entities can better undertake enhanced and ongoing customer due diligence, and develop policies and measures to protect their services from criminal misuse.

This report contains case studies detailing investigations and operations by AUSTRAC's partner agencies. Most of the case studies have been assisted by reporting entities submitting transaction and suspicious matter reports to AUSTRAC. This reporting provides key intelligence to support law enforcement investigation requirements, including identifying relationships between individuals and networks, movement of funds and patterns of financial activity.

AUSTRAC publishes this report to inform industry, and the wider community, about the various methods criminals use to conceal, launder or move illicit funds and to commit financial or other crimes. This assists industry to strengthen measures to detect money laundering activity and to protect both businesses and customers from criminal activity.

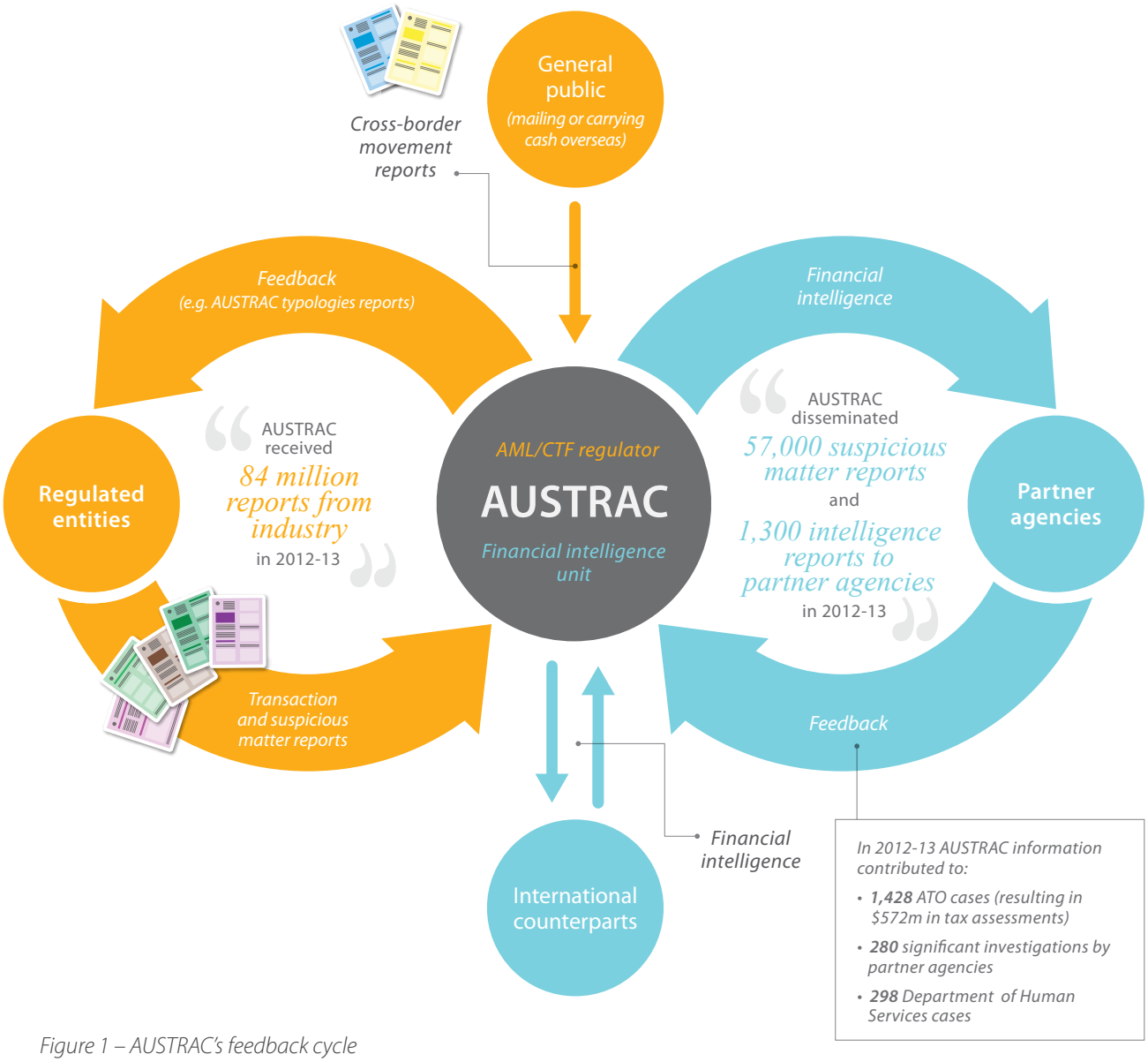


Figure 1 – AUSTRAC's feedback cycle

International cooperation

Cooperation between financial intelligence units (FIUs) is vital in the global fight against money laundering and terrorism financing. This cooperation not only benefits the operational work of the FIUs, but also law enforcement agencies tracking the international movements of the proceeds of crime.

AUSTRAC has an extensive network of international partners with which it shares its financial transaction information and intelligence. In return AUSTRAC receives valuable financial intelligence which assists its own detection and analysis of illicit transactions. AUSTRAC's international intelligence exchanges are undertaken in accordance with the terms of exchange instruments with each international jurisdiction.

Information exchange between FIUs strengthens the global effort to combat money laundering and terrorism financing and benefits the operational work of FIUs and law enforcement agencies tracking the international movement of the proceeds of crime.

As of March 2013, AUSTRAC has exchange instruments with 66 international FIU counterparts.

To view AUSTRAC's Memoranda of Understanding and Exchanges of Letters with foreign counterpart agencies, refer to the exchange instruments list at: www.austrac.gov.au/exchange_instruments.html

Information sources

The information in this report has been generated from the following research material:

- sanitised cases from AUSTRAC's partner agencies
- AUSTRAC strategic and typology research, including previous AUSTRAC typologies and case studies reports
- publicly available information.

A list of sources which inform the content of this report is included in Appendix B.

AUSTRAC acknowledges the use of information provided by a number of its partner agencies, particularly the:

- Australian Crime Commission (ACC)
- Australian Customs and Border Protection Service (ACBPS)
- Australian Federal Police (AFP)
- Australian Securities and Investments Commission (ASIC)
- Australian Taxation Office (ATO)
- Crime and Misconduct Commission (CMC)
- Department of Human Services (DHS)
- New South Wales Crime Commission (NSWCC)
- Queensland Police Service (QPS)
- South Australian Police (SAPOL)
- Victoria Police (VICPOL)
- Western Australia Police (WAPOL).

The contribution made by these agencies complements the research undertaken by AUSTRAC analysts into money laundering and terrorism financing risks and methodologies.

The case studies featured within this report have been sanitised and approved by our partner agencies for public release. AUSTRAC is unable to provide further information on individual case studies within this report.

Terminology

Each case study within this report is accompanied by a summary table highlighting the common elements involved in the money laundering or terrorism financing process. These are:

- **Offence** – the criminal or civil offence involved (these do not necessarily represent actual charges brought against the perpetrators).
- **Customer** – the type of customer/s involved in the offence (this can be an individual, business or foreign entity).
- **Industry** – the industry through which transactions were conducted (some cases involve multiple industries).
- **Report type** – where relevant, the types of financial transaction reports submitted by regulated entities, either under the FTR Act or AML/CTF Act, which contributed to the investigation or operation.
- **Channel** – the means by which the individuals undertook or attempted to undertake transactions (predominantly this comprises transactions conducted in person, via electronic means or through an intermediary/third party).
- **Jurisdiction** – the location (Australian or international) where the transactions originated or were undertaken.
- **Designated service** – the category of 'designated service' (as listed in section 6 of the AML/CTF Act), or other financial product, used in the offence. The case studies within this report have been grouped according to the primary designated services used.
- **Indicators** – the customer behaviours or activities which may have indicated the possibility of money laundering or terrorism financing activity. A consolidated list of key indicators identified in this report can be found in Appendix A.

Typologies & vulnerabilities

Typologies and vulnerabilities

Criminals are adept at identifying and exploiting vulnerabilities in financial products or industry sectors to facilitate financial crime and to launder the proceeds of their illicit activity. Most high-threat criminal enterprises actively seek to insulate their criminal activities by intermingling legitimate and illegal interests. Organised crime groups rely on money laundering as a key method of legitimising or hiding proceeds or instruments of crime.

Criminals consistently seek to exploit financial products or sectors that are perceived to be more lightly regulated than other areas. Criminals looking to launder the proceeds of crime are adept at changing and adapting in response to increasing regulatory controls. While individual criminals and criminal groups vary in sophistication, they are able to purchase specialist advice, exploit corporate structures and conceal this activity within legitimate financial transactions.

The strong regulatory controls in place for mainstream financial institutions in Australia, particularly banks, may displace criminal activity towards products and services considered to attract less regulatory attention.

This chapter of the report examines financial typologies and vulnerabilities involving gold bullion, international trade and politically exposed persons (PEPs).

The gold bullion and international trade typologies are established methods for money laundering. Gold bullion can be converted to various forms enabling criminals to transfer gold domestically and internationally in a form which is easily transportable, with a low risk of detection.[1] Money laundering through international trade also provides criminals with an avenue to move illicit funds across borders.

This section also outlines money laundering vulnerabilities associated with PEPs and corruption.

The typologies and vulnerabilities outlined in this report are intended to inform regulated entities about the various techniques criminals can employ to launder the proceeds of their illicit activity. Indicators are also provided to highlight potential suspicious customer behaviour which may be indicative of money laundering and or other illicit activity. In isolation, these indicators are not necessarily synonymous with illicit activity. However, the appearance of multiple indicators may be indicative of illicit activity. This information is provided to help regulated entities identify activities and indicators which should be monitored and, where appropriate, reported to AUSTRAC.

Previous reports in the AUSTRAC typologies and case studies series have covered a wide range of money laundering methodologies and financial crimes. To find out more about these crimes and methodologies, refer to AUSTRAC's previous reports at www.austrac.gov.au/typologies.html

1 Australian Transaction Reports and Analysis Centre, *Money Laundering in Australia 2011* (MLA 2011), AUSTRAC, West Chatswood, NSW, 2011, p. 25, viewed 20 September 2013, <www.austrac.gov.au/money_laundering_in_australia_2011.html>.

Gold bullion

Criminals buy and sell gold bullion to launder money as it has high intrinsic value, can be converted (and melted down) into various forms and enables anonymity when transferring value.[2] This makes it easy to conceal and move across borders, domestic and international, and convert back to legitimate funds with a low risk of detection.[3]

Money laundering vulnerabilities

The money laundering vulnerabilities associated with gold bullion include:

- **The high intrinsic value of gold bullion** makes it a popular asset for criminals to store, invest and conceal the proceeds of crime.
- **The opportunity to make anonymous transactions** hampers the ability of authorities to follow the money trail. Gold bullion may be used by criminals as an instrument of crime to pay for, or receive funds from, the sale of illicit goods and services.
- **Gold bullion is available in, and can be converted to, various forms** enabling criminals to transfer gold domestically and internationally to third parties in a form which is easily transportable, with low risk of generating suspicion or detection.[4] Gold bullion can take the form of authenticated bars, ingots and bullion coins, or it can be melted down and disguised as other items such as nuts, bolts and wrenches, as seen in international cases.
- **Ownership of gold can be disguised using the names of third parties**, providing criminals the opportunity to recruit individuals or professional facilitators to buy gold on their behalf.[5] Third-party ownership assists criminals to disguise the true ownership of criminal assets and complicates asset confiscation efforts.[6]
- **Trade-based money laundering** involving gold bullion (or false invoices purporting to be for gold bullion) may be used to launder illicit funds. Criminals use trade to conceal, transfer and convert the instruments or proceeds of crime into seemingly legitimate and less noticeable assets.[7] Money laundering through international trade is outlined in the next section of this report.
- **Criminals are likely to undertake fraudulent activity** when they purchase gold bullion. Criminals will often use false or fraudulent identification, or use third parties, to buy gold bullion. This hampers the ability of law enforcement to follow the money trail.

---

2 Financial Action Task Force, *Report on Money Laundering Typologies 2002-2003*, FATF, Paris, 2003, viewed 20 September 2013, <www.fatf-gafi.org>.

3 MLA 2011, p. 25.

4 MLA 2011, p. 26.

5 See Glossary for definition of 'professional facilitator'.

6 MLA 2011, p. 25.

7 See Glossary for definition of 'trade-based money laundering'.

Money laundering typologies

AUSTRAC has identified two methods criminals use to launder money through gold bullion trading. These methods are explained below.

Method 1 – Direct purchase from prospector: illicit purchase legitimised

- Criminals will buy gold directly from prospectors, usually with illicit cash. Because the bullion is bought directly from the prospector, the purchaser may be able to negotiate a reduced price.
- Once the criminal buys the gold, they sell it to an unrelated legitimate business which may in turn convert the gold into bullion.
- The criminals declare the profits from the sale of the gold as legitimate income to revenue authorities.
- The legitimate business and prospector are unwitting participants in the scheme.

Figure 2 below depicts this method of using gold bullion to launder money.

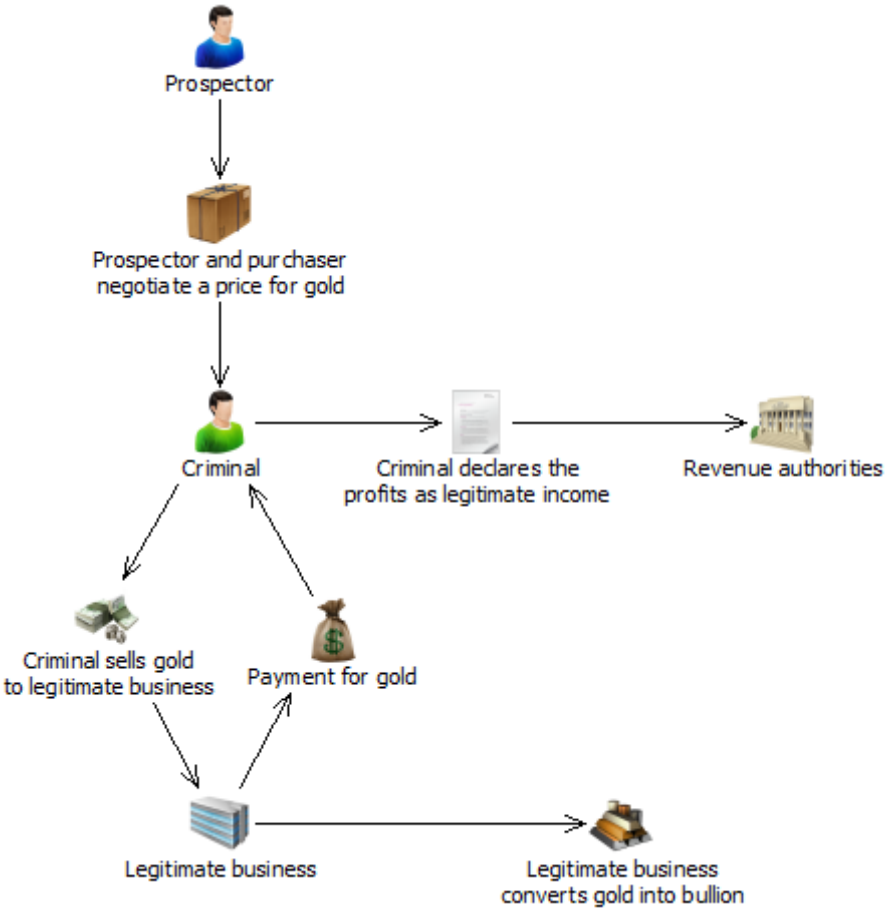


Figure 2: Method for using gold bullion to launder money

Method 2 – Use of false invoices

Another known money laundering method using gold bullion involves the use of false invoices.

International cases show that gold bullion has been melted down into different products, including nuts, bolts and wrenches, making it easier to conceal from border authorities. Criminals may send these disguised gold products overseas. This process may involve altering or creating false invoices to disguise the contents of the consignments and falsify their value (whether over or under the real price or value). In some cases the gold may not actually to be transported physically. In other cases, the gold may not even exist. Rather, criminals cite 'gold' (or some other precious metal) as the good being traded, helping to explain large movements of money, either domestically or across international borders. This is a form of trade-based money laundering.

Reporting obligations

Buying and selling bullion in the course of carrying on a business is a designated service under section 6 of the AML/CTF Act.[8] A reporting entity does not have to specialise in bullion trading to provide this designated service. For example, mining companies or refiners who buy or sell bullion are also reporting entities for this purpose.

For the purposes of the AML/CTF Act, AUSTRAC defines bullion as gold, silver, platinum or palladium which is authenticated (by stamping or hallmarking) or assayed to a specified fineness in mass forms such as bars, ingots, plates, wafers and bullion coins.[9]

Indicators for industry

The following indicators highlight potentially suspicious customer behaviour involved in gold bullion transactions.

- Purchase of gold bullion with bank cheques – may be an attempt to conceal the source and underlying ownership of the funds
- Multiple cash purchases of gold bullion in a short space of time
- Structured cash deposits into an account to finance a single gold bullion purchase
- Foreign nationals purchasing gold bullion through multiple transactions over a short time period
- Established customer (including bullion dealers) dramatically increasing their purchase of gold bullion for no apparent reason
- Customer buying gold bullion and using a general post office or private mail box service provider as their address, without listing a corresponding box number
- Bullion transferred among family members and associates using bullion accounts for no apparent commercial purpose
- Reporting entity unable to establish the original source of funds used by a customer to buy gold bullion
- Occupation inconsistent with customer's financial profile. For example, the customer may list their occupation as 'student' yet transfer large values of funds to bullion accounts

Case study 29 in AUSTRAC's 2008 typologies and case studies report and case study 17 in the 2010 report illustrate the use of gold bullion to commit money laundering and/or tax evasion.

---

8 For further information about what it means to be 'carrying on a business', refer to *AUSTRAC Public Legal Interpretation No. 4 of 2008 – What constitutes a reporting entity*: <http://www.austrac.gov.au/pli.html>.

9 Further information is available from Chapter 11 of the *AUSTRAC Regulatory Guide* <www.austrac.gov.au/rg_11_bullion.html>.

Money laundering through international trade

International trade involves the provision of goods or services, exported or imported, and the reconciliation of payment for those goods or services. Trade-based money laundering (TBML) can occur either through the movement of illicit value through the trade sector, or through the movement of illicit funds through the finance sector, ostensibly for the payment of international goods or services.

TBML can occur without legitimate goods or services being exchanged. For example, trade payments (such as open accounts, letters of credit or international funds transfers), supposedly made to settle invoices, may be used as a cover to conceal and legitimise the movement of illicit funds.[10]

Even in its simplest form, TBML is a complex money laundering method. It typically involves a number of money laundering methodologies used in unison. TBML occurs during the layering and integration stages of the money laundering cycle.[11] Illicit value or funds are placed in the economy before being layered and/or integrated through trade. By the time the money or its value is laundered through trade movements and transactions, significant distance has been created between the predicate offence and the illicit value.[12]

TBML is perpetrated in a number of ways, including through:

- price misrepresentation (the over or under-invoicing of goods)
- fictitious invoicing
- multiple invoicing
- falsely describing goods or misrepresenting the quality or quantity of goods traded
- legitimate shipment of goods to transfer value between criminal groups
- disguising laundered funds as international consultancy service fees
- phantom or ghost shipments where the relevant paperwork is lodged with authorities, although the goods are not shipped.

Some of these methods are similar to those used to commit other offences, such as avoiding Goods and Services Tax (GST) payments or import duties.[13] These methods are also sometimes used by criminal networks to smuggle goods into Australia for illicit markets, such as precursor chemicals or drugs.

10 See Glossary for definition of 'letters of credit' and 'open account'.

11 See Glossary for definition of 'money laundering cycle'.

12 A predicate offence is any offence which generates proceeds of crime.

13 An import duty is a tax collected on imports and some exports by the customs authorities of a country. Also referred to as customs duty, tariff, import tax and import tariff.

Most methods of international trade financing (including open accounts, letters of credit, factoring and forfaiting) are covered by AML/CTF regulations and reporting requirements.[14] However, the nature of these financial instruments means that details about the buyer and seller behind these transactions may not always be reported to AUSTRAC.

Reporting entities such as banks may have limited visibility of the entire transaction due to the complexity of trade financing. It can often involve many links in a long chain of transactions. TBML detection requires intensive analysis of the whole trade transaction – the movement of the goods or service, the method of payment for the trade and, importantly, the origin and purpose of the funds that financed the trade transaction – for illicit activity to be accurately identified.

Money laundering vulnerabilities

Key drivers and enablers associated with TBML in overseas countries and regions can be seen in the Australian trade and crime environments. Several factors attract criminals to use the international trade system to transfer value:

- **The vast volume of international trade** and associated transactions, which increases the scope for suspect trade transactions to be camouflaged, offers opportunities for facilitating large-scale money laundering.
- **The volume of trade not only has the potential to hide individual transactions, but makes oversight and enforcement difficult.** Official regulation and monitoring of trade flows involves a range of agencies in Australia and overseas which adds to the complexity of detecting TBML.
- **The movement of goods through multiple transhipment points** and third parties adds complexity to the money trail and enables criminals to distance themselves from the activity. Variable standards and controls in other jurisdictions can also assist criminals to embed TBML into a complicated chain of trade payments and shipments.
- **Some high-risk countries** do not have well-established banking systems. This is of concern as money launderers may collude with criminal partners located in these jurisdictions to organise TBML activity.

However, a number of factors may also deter criminal groups from exploiting the international trade system to launder funds. These include the involvement of third parties such as financial institutions, customs brokers and freight staff who may inform customs authorities of suspicious cargo or transactions, the costs involved in international trade, and the level of knowledge required to establish the businesses and trading links required to undertake TBML.

14 See Glossary for definitions of 'factoring' and 'forfaiting'.

Indicators for industry and government authorities

The following indicators highlight potential suspicious customer behaviour involving TBML transactions.

- Payments made to consignor/vendor from unrelated third parties
- Suspected false invoicing or reporting, such as misclassification, over-valuation or under-valuation of traded goods
- Goods traded are inconsistent with the nature of the importer or exporter's regular business
- Use of unusual shipping routes or transhipment points by a customer
- Unusual ports of origin for commodities
- Packaging inconsistent with commodity or shipping method
- Shipment size which appears inconsistent with the scale of the exporter or importer's regular business activities
- Significant discrepancies between the description of the goods on the 'bill of lading' and the invoice[15]
- Customers provide vague or incomplete information about personal, company or financial transactions and resist providing additional information

15 See Glossary for definition of 'bill of lading'.

Politically exposed persons and corruption

Corruption can have a significant impact on economic development, political stability and transnational crime.[16] The Financial Action Task Force (FATF) has designated corruption as a predicate offence to money laundering.[17]

Corruption is the misuse of public office by an individual for private gain.[18] It involves acts ranging from abuse of functions, position or influence, bribery of foreign or domestic officials, extortion, embezzlement, and self-dealing.[19] Those seeking to launder the proceeds of corruption may experience a reduced risk of detection if politically exposed persons (PEPs) are involved in the laundering process.

Politically exposed persons

Foreign PEPs are defined as individuals who are, or have been, entrusted with prominent public functions in a foreign country.[20] *Domestic* PEPs are defined in the same way in relation to prominent domestic public functions.[21]

Examples of PEPs include:

- heads of state or government
- senior politicians
- senior government, judicial or military officials
- senior executives of state-owned corporations
- important political party officials.[22]

PEPs also include individuals entrusted with a prominent function by an international organisation such as directors, deputy directors and members of the board or equivalent positions.[23]

Obviously, the simple identification of an individual as being a PEP does not mean that they are corrupt. Rather, it is the potential for PEPs to be corrupt or corrupted which requires businesses and financial institutions that deal with them to exercise enhanced customer due diligence.

---

16 Financial Action Task Force, *Laundering the Proceeds of Corruption*, FATF, Paris, 2011, p. 9, viewed 20 September 2013, <www.fatf-gafi.org>.

17 Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, FATF, Paris, 2012, p. 111, viewed 10 April 2013, <www.fatf-gafi.org>.

18 Financial Action Task Force, *Laundering the Proceeds of Corruption*, FATF, Paris, 2011, p. 6, viewed 20 September 2013, <www.fatf-gafi.org>. Note: this is a functional definition of corruption, not a legal definition.

19 See Glossary for definition of 'self-dealing'.

20 Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, FATF, Paris, 2012, p. 118, viewed 10 April 2013, <www.fatf-gafi.org>. See also FATF Recommendation 12, which includes PEPs.

21 Ibid, p. 119.

22 Ibid, pp. 118-119.

23 Ibid. Also, FATF defines 'international organisations' as 'entities established by formal political agreements between their member States that have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as resident institutional units of the countries in which they are located.' For example, international organisations include the United Nations and affiliated international organisations such as the International Maritime Organisation. For more information see FATF, *International Standards on combating money laundering and financing of terrorism & proliferation*, p. 117.

A corrupt PEP may launder illicit funds derived from criminal activities other than corruption, such as drug trafficking or environmental crime. While corrupt or dishonest PEPs can be found in almost any country, PEPs from countries with widespread corruption can present a greater potential risk.[24]

Money laundering vulnerabilities

Some of the money laundering vulnerabilities associated with PEPs are set out below:

PEPs provide a veneer of respectability which can deflect suspicion about their transactions. The privileged positions of trust and responsibility PEPs hold may be seen as enhancing the legitimacy of their transactions and financial activity, and correspondingly reduces the risk of such activity raising suspicion.

PEPs have a unique position of influence. Because of their position, corrupt PEPs may circumvent or attempt to circumvent AML/CTF regulation by influencing, controlling or evading AML/CTF programs. Corrupt PEPs may also influence or attempt to influence individuals and institutions that guard against criminal activity.

International money laundering typology

An examination of international money laundering case studies reveals that a common method used by PEPs to launder the proceeds of corruption is the use of third parties.

Corrupt PEPs seek to obscure their financial position and use family or associates to access the financial system to launder money. Given the high visibility of some PEPs in and outside their home country, the use of third parties provides a buffer between the corrupt activity and their financial activities and assets. For example:

- A corrupt PEP based overseas may move funds through the bank accounts of their children studying in another country.
- A corrupt PEP may use a close associate to exchange cash for gaming chips or, vice versa, gaming chips for cash, on their behalf at a casino.
- A corrupt PEP may buy property using a third party or family member as a legal owner.

Corrupt PEPs may use a third party's bank account to deposit and withdraw illicit funds. Alternatively, corrupt PEPs may use third parties to undertake transactions on their behalf. The use of third parties distances corrupt PEPs from the illicit funds, disguises ownership of assets and complicates asset confiscation efforts by authorities.

The following is an example of how third parties may be used to launder money:

- Individual A and suspect B are senior politicians and both are considered PEPs.
- Individual A provides confidential information to suspect B about the proposed privatisation of a large government entity.
- After receiving this information suspect B persuades a close associate to buy shares in company X on his behalf. Company X submits a tender for the right to purchase the government entity.
- Suspect B uses his position to improperly exert influence and favour company X as the purchaser of the government entity.

---

24 D Chaikin & J Sharman, *APG/FATF Anti-Corruption/AML/CFT Research Paper*, Asia/Pacific Group on Money Laundering (APG) and FATF, Paris, 2007, p. 36.

- Suspect B indirectly benefits financially from this venture through the profits generated by company X.
- Suspect B's close associate moves the illicit profits through his personal and business accounts. The funds are then given to suspect B and/or his family as needed.
- Suspect B's wife buys a house using the proceeds of the corruption.
- The proceeds of corruption are used to pay individual A for providing confidential insider information.

Figure 3 below provides an overview of this method.

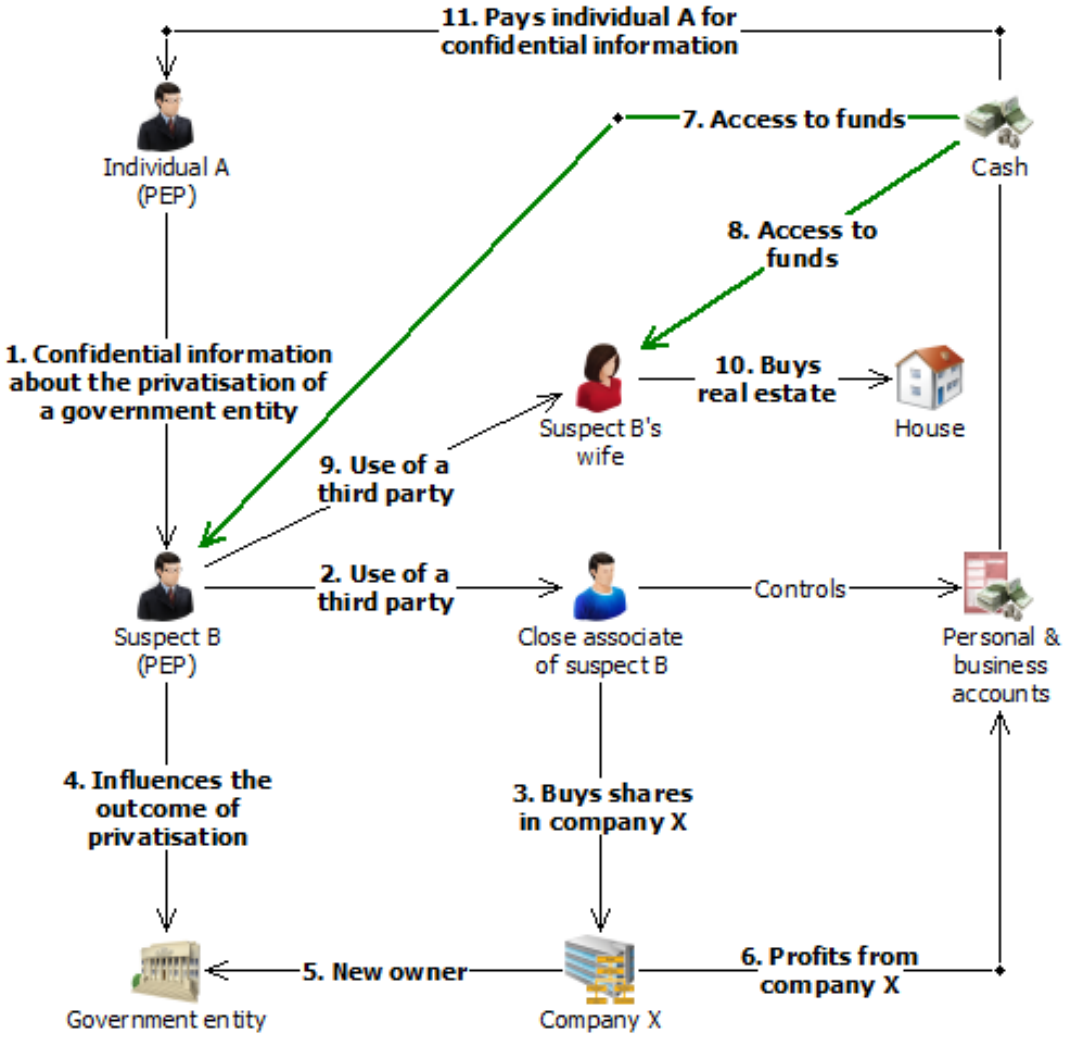


Figure 3: Use of third parties to launder the proceeds of corruption

Reporting obligations

PEPs are considered to be potentially higher risk due to their position and potential access to wealth and resources. The effective implementation of customer due diligence (CDD) is a key element of a reporting entity's AML/CTF program when dealing with PEPs.

Australia's AML/CTF regime requires reporting entities to have an AML/CTF program. The primary purpose of Part A of an AML/CTF program is to identify, mitigate and manage ML/TF risk. In identifying its ML/TF risk, a reporting entity must consider the risk posed by, among other things, its customer types, including any politically exposed persons (PEPs). Part A must include a requirement that, in determining what is an appropriate risk based procedure for inclusion in Part B of the reporting entity's AML/CTF program, the reporting entity must have regard to ML/TF risk relevant to the provision of the designated service. Part B of an entity's program is designed to set out the applicable customer identification procedures of the entity. An entity is required to undertake enhanced CDD requirements when it determines under its risk-based systems and controls that the ML/TF risk is high.[25]

The FATF standards set out specific requirements for foreign, domestic and international organisation PEPs through Recommendations 12 and 22.

Indicators for industry

The following indicators may assist reporting entities to identify potential money laundering involving corruption and PEPs.

- A PEP holds a mortgage or loan account and makes high-value payments into the account
- A PEP uses the bank accounts of dependants living in another country to move funds
- A PEP has significant holdings in bank term deposits and other high-wealth products such as shares and investment portfolios in another country
- A PEP receives large international funds transfers to a gaming account. The PEP withdraws a small amount for gaming purposes and withdraws the balance using cheques
- A PEP receives multiple cash deposits into their bank account from third parties within a short time frame. The cash deposits may consist of foreign currency
- A PEP receives multiple international funds transfers from different beneficiaries in a short time frame or on the same day
- A PEP is unable or reluctant to provide details or credible explanations for establishing a business relationship, opening an account or conducting transactions
- International funds transfers where a PEP is both the ordering and beneficiary customer
- A PEP uses third parties to exchange cash for gaming chips with minimal gaming activity
- A PEP undertakes transactions for no apparent commercial or other reason

25 Chapter 15 of the AML/CTF Rules, see <http://www.austrac.gov.au/aml_ctf_rules.html>.

Case studies

Account and deposit-taking services

Case studies – Account and deposit-taking services

Case 1 – AUSTRAC information revealed complex 'round robin' tax evasion scheme

AUSTRAC disseminated a financial intelligence assessment to authorities, which initiated an investigation into a complex 'round robin' tax evasion scheme.[26] These schemes essentially aim to make funds movements appear as payments to other parties while, in reality, the funds ultimately return to the original beneficiary. AUSTRAC information was the primary source of intelligence throughout the investigation. Part of the investigation focused on two suspects (A and B) who were jailed for evading company and personal income tax of approximately AUD750,000.

The AUSTRAC assessment detailed the financial activities of a Vanuatu-based business. Enquiries identified that the principal promoter and operator of the tax evasion scheme was a senior partner of an accountancy firm based in Vanuatu.

Analysis of AUSTRAC information uncovered the round robin tax evasion scheme which involved the transfer of funds between Australia-based individuals and bank accounts of companies in other countries. The scheme allowed individuals and companies to evade tax in Australia. AUSTRAC searches on bank accounts identified the flow of funds to numerous Australia-based individuals, including suspects A and B.

Enquiries revealed that suspect A was the sole director and shareholder of companies X and Y, and suspect B was the sole director and shareholder of company Z. Both suspects operated businesses which performed contract work through their respective companies in the building industry.

The method used to facilitate tax evasion was:

1. The suspects transferred funds from their companies' accounts to the bank accounts of companies in New Zealand. The New Zealand companies and the bank accounts were controlled by the Vanuatu-based accountant, who was a signatory to the bank accounts.

2. The payments were falsely described in the suspects' companies' records as expenses in the form of 'management and consultancy fees'. False invoices were created for the fictitious expenses. No evidence was available to show that any consulting work had been carried out. The invoice amounts matched the amounts paid to the bank accounts in New Zealand.

3. The false expense payments were claimed as deductible expenses in the tax returns of companies X, Y and Z, thereby fraudulently reducing the companies' taxable income and therefore the amount of tax they were assessed as liable to pay.

4. The accountant then transferred the funds under the guise of international 'loans' through a series of round robin international transactions, through accounts held in the name of companies owned and operated by the accountant.

26 See Glossary for definition of 'round robin tax evasion scheme'.

5. The accountant transferred the funds into the personal bank accounts of the suspects in Australia. The funds were transferred via an overseas company controlled by the accountant, separate to the companies in New Zealand that received the funds originally.

6. In order to disguise the funds being transferred back into Australia as loans, false documents were created purporting to be international loan agreements with a foreign lender. Loans are not assessable income and are tax free.

7. The funds, disguised as international loans, were not disclosed in the suspects' personal tax returns. The suspects were thus assessed as liable for less tax than they should have been, thereby avoiding income tax obligations.

8. Effectively, the 'loans' paid to the suspects were funds from their respective companies but were disguised by the scheme, allowing them to evade company and personal tax.

It was alleged that suspect A engaged in 15 round robin transactions over a one-year period and lodged false tax returns for himself and companies X and Y.

AUSTRAC data showed that over a five-year period suspect A received incoming international funds transfers of approximately AUD540,000 from New Zealand. These funds were sent by a company of which the accountant was a director.

It was alleged that suspect B engaged in 11 round robin transactions over a three-year period. He also lodged false tax returns for himself and company Z. Over a one-year period suspect B made four international funds transfers to bank accounts in New Zealand for amounts ranging from approximately AUD26,000 to AUD40,000. The accountant was a signatory to the New Zealand bank accounts.

Suspects A and B evaded approximately AUD390,000 and AUD360,000 in company and personal tax respectively.

Suspect A pleaded guilty to one charge of obtaining a financial advantage by deception contrary to section 134.2(1) of the *Criminal Code Act 1995*.

Suspect B pleaded guilty to:

1. defrauding the Commonwealth contrary to section 29D of the *Crimes Act 1914*

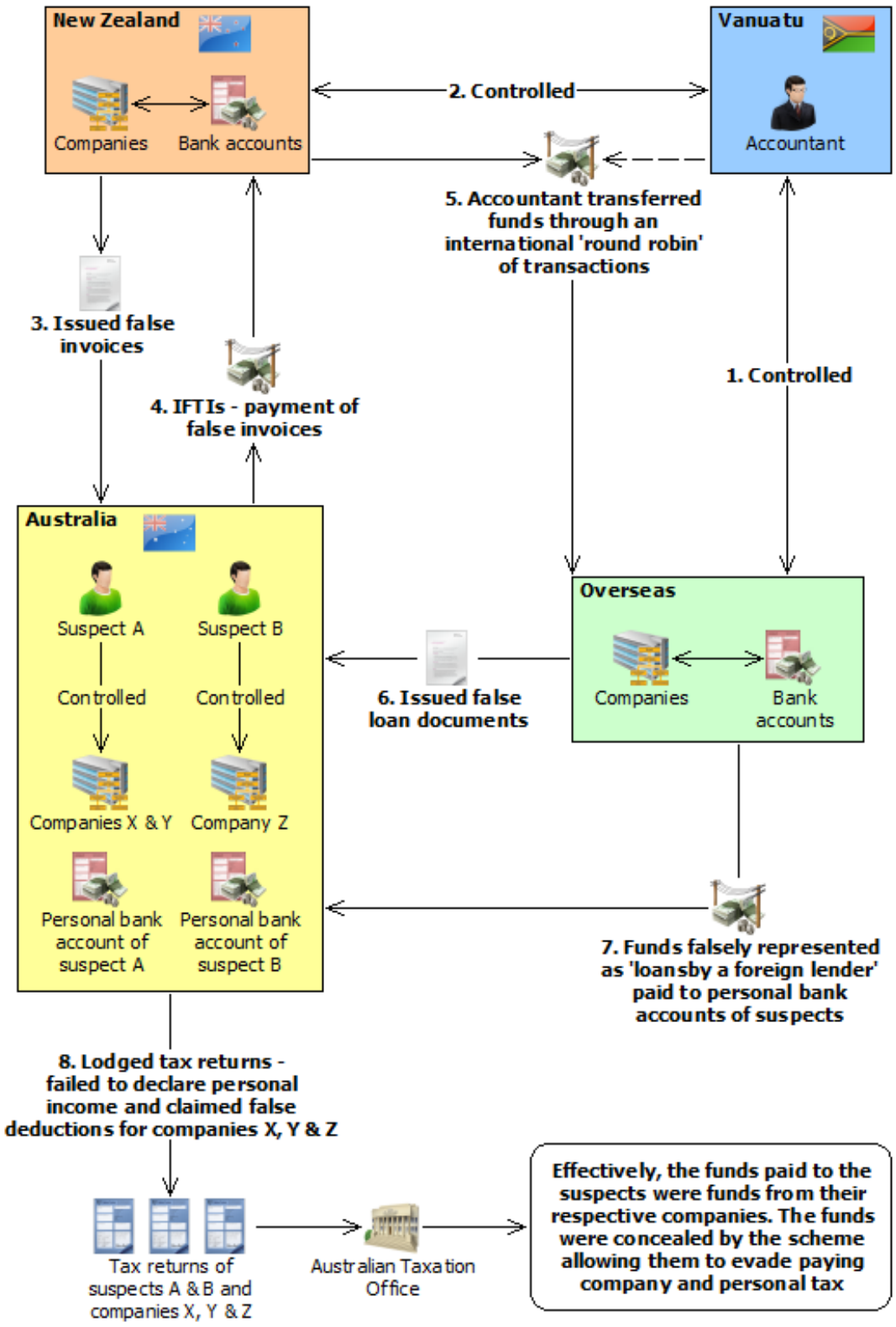
2. obtaining a financial advantage by deception contrary to section 134.2(1) of the Criminal Code Act

3. dealing in proceeds of crime worth AUD100,000 or more contrary to section 400.4(1) of the Criminal Code Act.

Both suspects were sentenced to three years imprisonment.

Suspects A and B also became liable to pay penalties and interest to the Australian Taxation Office of more than AUD1 million and AUD900,000 respectively.

The accountant was convicted of conspiring to defraud the Commonwealth and was sentenced to eight years and 11 months imprisonment.



Case 1 - AUSTRAC information revealed complex 'round robin' tax evasion scheme

Offence	Tax evasion Money laundering
Customer	Business Individual
Industry	Banking (ADIs)
Channel	Electronic
Report type	IFTI
Jurisdiction	Domestic and international – New Zealand, Vanuatu
Designated service	Account and deposit-taking services
Indicators	Account activity inconsistent with customer profile Customer receives international funds transfers declared as loans from a foreign lender Customers undertaking complicated transfers without a business rationale Different ordering customers sending international funds transfers to the same beneficiaries False invoices created for services not carried out International funds transfers to a high-risk jurisdiction Multiple high-value international funds transfers to and from Australia with no apparent logical reason

Case 2 – Investors lost $82 million in Ponzi investment scheme

AUSTRAC information assisted authorities investigating an investment company suspected of running a Ponzi scheme.[27] The investment company's two directors (suspects A and B) accepted AUD70 million worth of funds from investors, promising returns on investment of up to 70 per cent.

The investment company told investors that their funds were being invested in high-risk shares, foreign exchange and commodity markets. However, investigations found that the investment company used newly invested funds to pay dividends to the company's earlier investors.

Ultimately, the investment company collapsed, owing investors more than AUD82 million. Investigations found that both former directors spent a proportion of invested funds on personal expenses, including home renovations, cars, yachts and an adviser, who assisted the directors in deciding which stocks to invest in.

AUSTRAC information included suspect transaction reports (SUSTRs) submitted with regard to fraudulent loan applications undertaken by one of the former directors (suspect A). AUSTRAC received an additional SUSTR reporting that an associate of suspect A had opened an account, over which suspect A held the power of attorney. Subsequently, suspect A began undertaking transactions via the account as if it were his own.

Further investigation revealed that the investment company had received more than AUD1.2 million worth of incoming international funds transfers from the accounts of investment companies based in New Zealand and Vanuatu.

Typically, investors transferred funds into the investment fund via internet banking or through direct deposits into accounts linked to the company. Over 250 people, from Australia and overseas, invested amounts ranging from AUD10,000 to AUD5 million.

The directors of the collapsed investment company faced 243 criminal charges between them, including carrying on a financial services business without a license, engaging in dishonest conduct, using false documents and obtaining property by deception and dishonest use of a corporate position.

Suspect A was sentenced to jail for 13 years and nine months, while suspect B was sentenced to two years and seven months imprisonment.

27 See Glossary for definition of 'Ponzi scheme'.

Offence	Fraud
Customer	Business
Industry	Banking (ADIs)
Channel	Electronic
Report type	IFTI SUSTR
Jurisdiction	Domestic International – New Zealand, Vanuatu
Designated service	Account and deposit-taking services
Indicators	A large number of individuals conducting domestic transfers, and direct deposits, to linked company bank accounts Incoming international funds transfers from offshore company bank accounts to Australian accounts Customer attempts to fraudulently obtain loans with inconsistent or missing customer identification Customer opens bank accounts and arranges for third parties to operate the bank accounts

Case 3 – Syndicate used real estate and trust accounts to launder cannabis cash

An Australian drug syndicate used multiple money laundering methods to launder more than AUD1 million worth of proceeds of crime. Trust accounts, a 'front' company, high-value goods and real estate were used to launder the profits from cannabis sales. The syndicate also misused the services of two 'professional facilitators' (an accountant and solicitor) to facilitate its criminal activity.[28]

The syndicate made significant profits by purchasing bulk amounts of cannabis in one state and then selling the drugs in another state. As a cover for its illicit activities, the syndicate established what appeared to be a transport company. The syndicate purchased a truck and rented a warehouse in the name of the company and used these to traffic the cannabis interstate.

The syndicate used four methods to launder its illicit profits.

- The syndicate members employed a company that specialised in processing wages to pay them a wage from their new transport company. Members of the syndicate deposited the cash proceeds of the cannabis sales into the transport company's account. From this account the funds were transferred to the wage processing company. The wage processing company then paid these funds to the syndicate members, seemingly as legitimate wages. Syndicate members were paid a wage of around AUD100,000 per year.
- The syndicate created trust accounts and investment companies. It gave an accountant AUD100,000 cash from the proceeds of cannabis sales and instructed the accountant to purchase shares in the name of the trust accounts and investment companies.
- One syndicate member purchased a property worth more than AUD700,000 in a family member's name. The property purchase was financed using a mortgage. This is an example of a criminal purchasing high-value goods in the name of a third party to disguise the true ownership of assets. Over a two-month period the syndicate member paid more than AUD320,000 in 16 cash deposits to their solicitor (who provided conveyancing services and acted on behalf of the syndicate member in the transaction) to pay off the mortgage on the property. These cash payments were the proceeds of crime.
- The syndicate members invested the profits from the sale of the drugs to support their lavish lifestyle by using cash to purchase high-value goods including motor vehicles, jewellery, designer clothing and electronics.

Two suspect transaction reports (SUSTRs) submitted to AUSTRAC initially alerted law enforcement to the syndicate's financial activity. These SUSTRs identified one member of the syndicate making multiple cash deposits into their account in amounts just below the AUD10,000 cash transaction reporting threshold.[29] On occasions these deposits occurred on the same day but at different bank branches. The syndicate member explained to bank staff the funds were to purchase a home but could not explain the source of the funds.

---

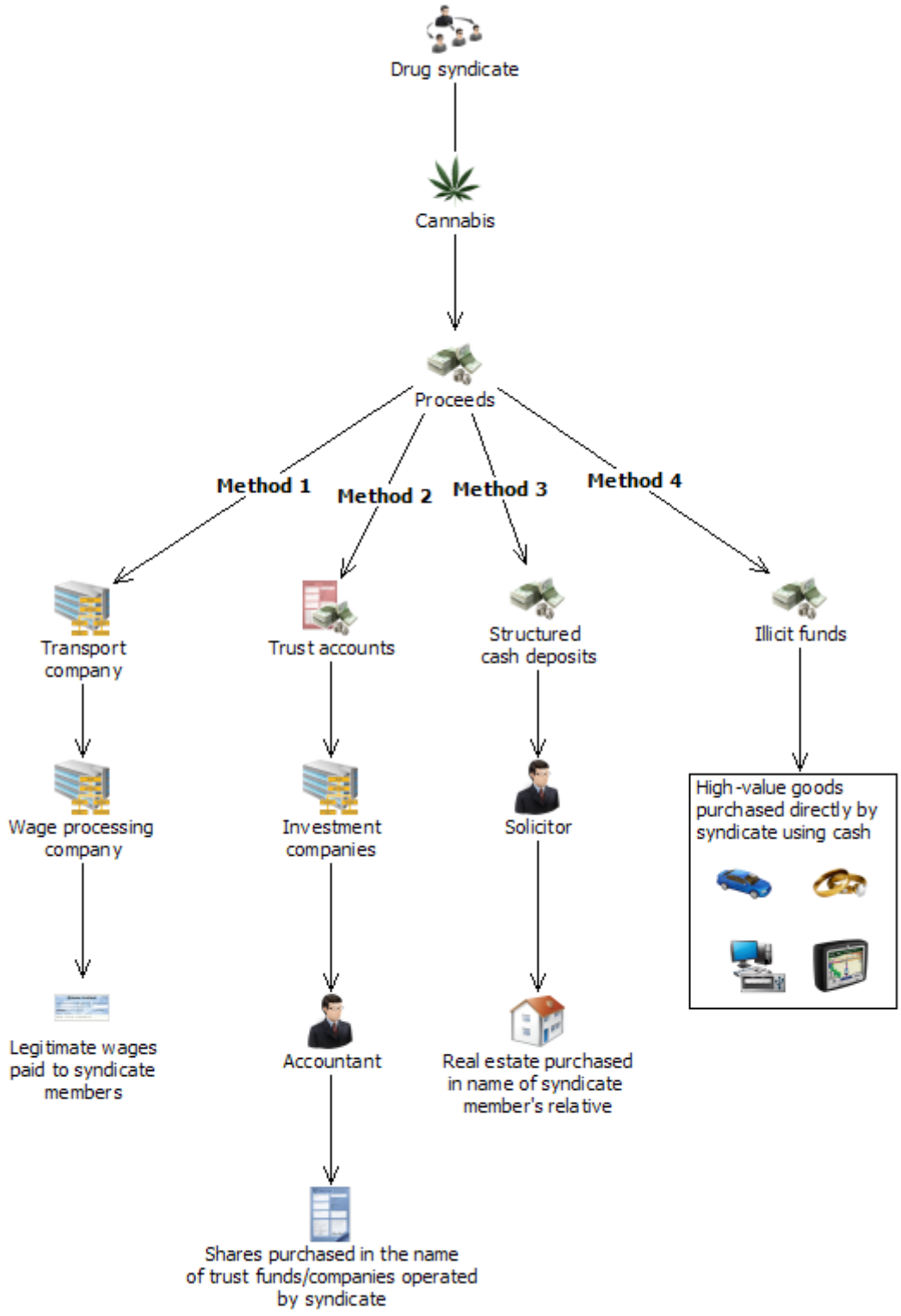
28 See Glossary for definition of 'professional facilitator'.

29 This is an offence known as 'structuring'. See the Glossary for a definition of 'structuring'.

AUSTRAC referred the SUSTRs to law enforcement and also prepared a financial intelligence report detailing the wider financial transactions undertaken by members of the syndicate and associated companies and trust accounts. This report supported existing law enforcement intelligence.

Law enforcement confiscated approximately AUD600,000 worth of assets that were proceeds of crime. Two members of the syndicate pleaded guilty to multiple money laundering and drug trafficking charges and both were sentenced to six years imprisonment.

Offence	Money laundering Drug trafficking
Customer	Individual Business
Industry	Banking (ADIs) Real estate
Channel	Physical Electronic
Report type	SUSTR
Jurisdiction	Domestic
Designated service	Account and deposit-taking services
Indicators	Client pays cash to accountant to purchase shares in the client's trust account and in the name of investment companies Mortgage for real estate taken out in relative's name Purchase of high-value goods in cash Structured same-day cash deposits at multiple bank branches within a two to three-week period Structured cash payments into solicitor's account Use of multiple large cash payments for mortgage repayment Unexplained source of funds used to conduct cash deposits



Case 3 – Syndicate used real estate and trust accounts to launder cannabis cash

Case 4 – AUSTRAC information assisted law enforcement to uncover a sophisticated investment fraud

Cold-call investment fraud involves unsolicited contact, generally by telephone, with victims who are persuaded to invest money in shares that are either worthless or non-existent.

While 'cold-calling' (making unsolicited calls to potential investors) is generally accepted as a legitimate business practice in Australia, these scam operators engage in conduct that is fraudulent, misleading and deceptive to convince potential victims to purchase investments. The callers do not hold an Australian Financial Services Licence (AFSL), which is required to provide investment advice in Australia.

AUSTRAC provided financial transaction reporting and associated analysis to law enforcement agencies which was instrumental in dismantling an investment fraud group operating in Australia.

Investigations identified five Australia-based suspects who used cold-calling tactics and a website to convince potential victims to invest in high-interest managed investment funds. Authorities also identified that several of the suspects were directors of three associated Australian companies which were used in the scam. The suspects promised investors that all funds deposited would be used to buy shares. Investors were assured they would receive a 30 per cent rate of return over a six-month period.

The investigation identified that over three months investors deposited approximately AUD800,000 into the three company accounts. During the same period of time, approximately AUD700,000 was withdrawn in cash cheques, usually on the same day as the deposit or the next day. To date, authorities have not been able to substantiate whether the suspects purchased any shares on behalf of investors. Investigations found that the investment scam resulted in over 35 investors losing approximately AUD700,000.

AUSTRAC analysed financial transaction reports submitted by reporting entities and identified:

- three suspicious matter reports (SMRs) and two suspect transaction reports (SUSTRs) indicating that:
  - » the suspects were conducting significant cash withdrawals from multiple bank branches
  - » the majority of funds had been transferred into the company accounts from multiple superannuation funds and individuals via internet banking, domestic transfers or real-time gross settlement (RTGS) payments[30]
  - » the payments and withdrawals associated with the three companies were inconsistent with their business profiles
  - » withdrawals from company accounts involved cheques being cashed at branches in amounts both above and below the cash transaction reporting threshold
  - » the suspects deposited cash into their personal accounts and then immediately used the funds to pay for outgoing international funds transfer instructions (IFTIs) to third-party and self-named accounts located in New Zealand. The IFTIs were for amounts between AUD1,000 and AUD17,000
  - » one suspect received fortnightly welfare payments, which was particularly suspicious given that funds were also being regularly transferred offshore

30 RTGS ensures that most payments between Australian banks are settled as they arise, using credit funds in the paying bank's settlement account at the Reserve Bank.

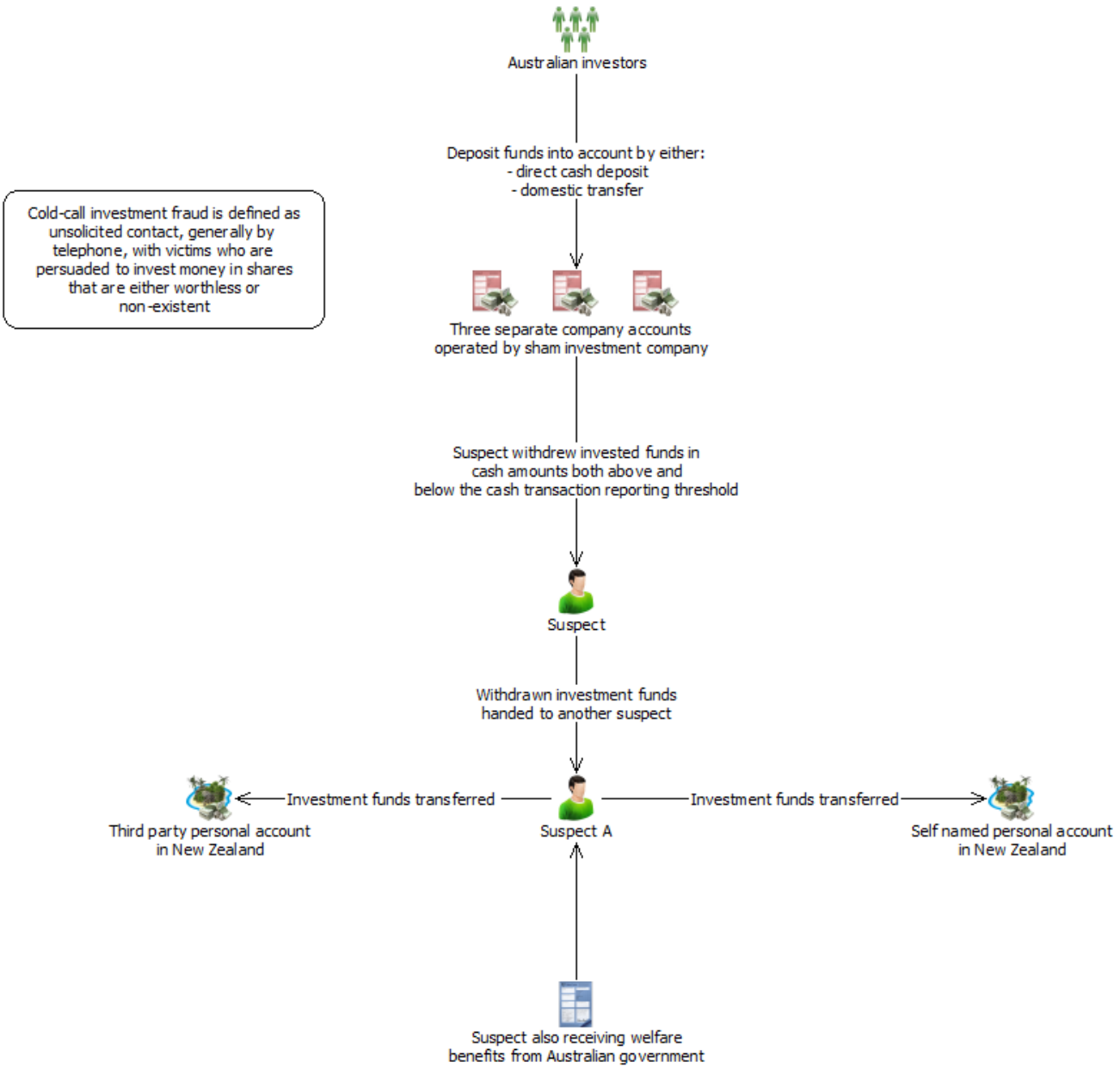
  - » upon questioning by bank staff, one suspect was not forthcoming with the rationale for undertaking transactions
- over a ten-month period approximately AUD160,000 was deposited in cash into one suspect's personal and trust accounts in amounts between AUD10,000 and AUD40,000
- over the same period approximately AUD460,000 was withdrawn in cash from the suspects' three company accounts in amounts between AUD10,000 and AUD50,000.

Search warrants were executed across a number of premises, including a call centre which was allegedly used in the investment scam to target victims. Police seized approximately AUD180,000 after observing three of the five suspects visit various bank branches withdrawing funds.

All five suspects were charged with money laundering offences under section 250 of the *Criminal Proceeds Confiscation Act 2002*. The companies and directors were found to have carried on a financial service business without holding an AFSL in contravention of the *Corporations Act 2001*.

The companies and the directors were restrained from carrying on financial service business in Australia and were ordered to pay the cost of court proceedings. In addition, all three companies were wound up.

Offence	Money laundering
Customer	Individual Business
Industry	Banking (ADIs)
Channel	Electronic Physical
Report type	IFTI SCTR SMR SUSTR
Jurisdiction	Domestic International – New Zealand
Designated service	Account and deposit-taking services
Indicators	Financial transactions inconsistent with established individual profile Same-day cash deposits and cash withdrawals at multiple bank branches Third-party deposits into business accounts which do not hold an AFSL Outgoing IFTI being sent to individuals rather than business for investment purposes Third-party funds transferred into company accounts from multiple superannuation funds



Case 4 – AUSTRAC information assisted law enforcement to uncover a sophisticated investment fraud

Case 5 – AUSTRAC information helped unravel AUD30 million university fraud

AUSTRAC information assisted law enforcement to investigate a network involved in defrauding a university of over AUD30 million and laundering the funds to purchase property and racehorses. Ultimately, law enforcement laid more than 2,000 charges against the suspects involved in the multi-million dollar fraud.

Managers at the university and the directors of construction companies were complicit in a large fraudulent invoice scheme. The managers would officially approve maintenance work to be carried out by the construction companies. The managers approved the payment of highly inflated invoices from the construction companies, as well as approving invoices for work that was never undertaken. Directors of the construction companies used the profits from the fraud to purchase racehorses and property. The managers at the university were repaid with kickbacks or direct shares in racehorses.

AUSTRAC was requested by law enforcement to investigate international funds transfer instructions (IFTIs) undertaken and received by associates of the suspects. The associates were identified as accounting firms which were undertaking the transfers on behalf of the suspects.

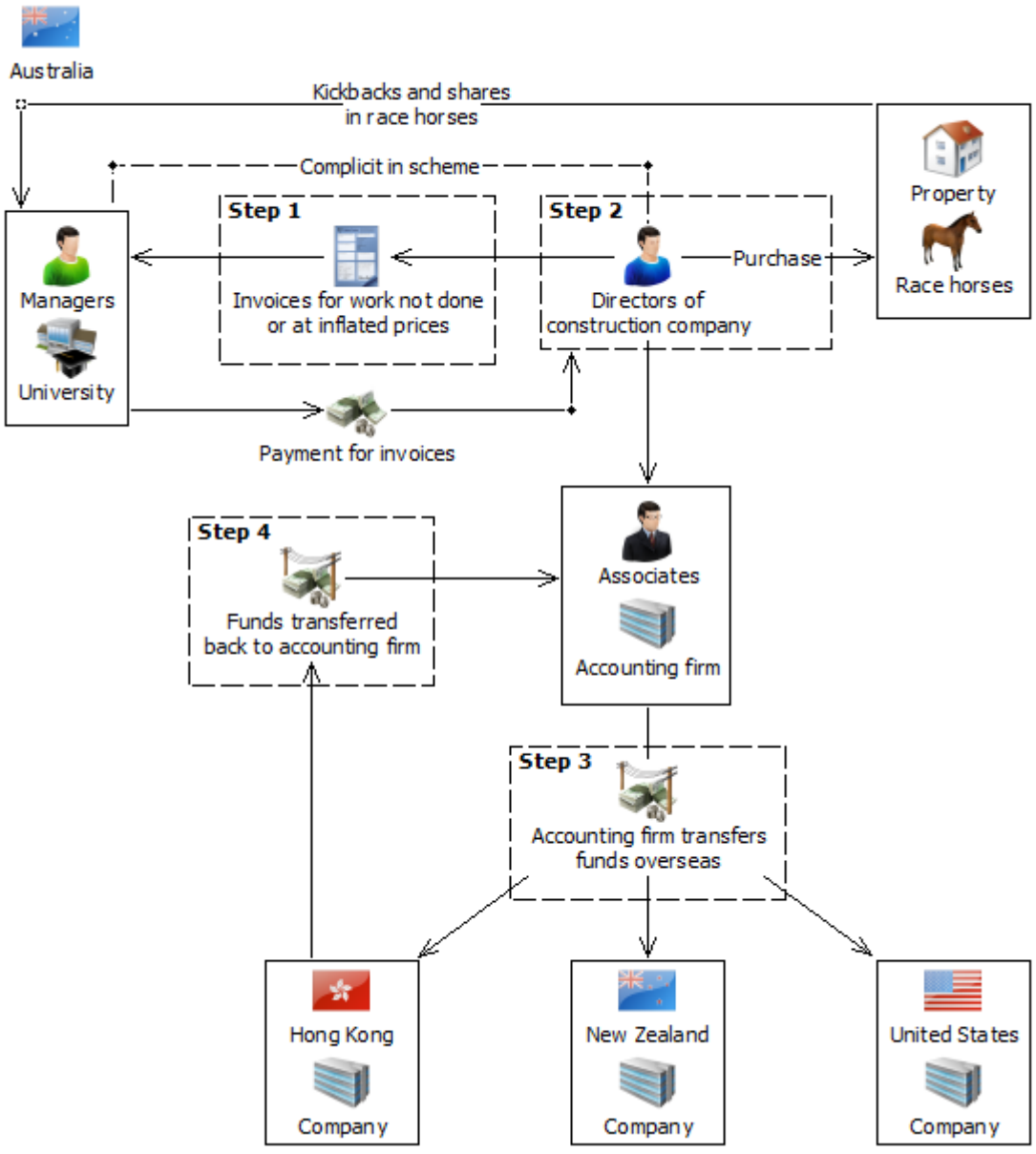
Funds were sent to many countries including New Zealand, Canada, Hong Kong and the USA. A large proportion of the funds were sent to companies linked to the horse racing industry. The accounting firms also received a large number of IFTIs from various overseas entities that were similar in value to the amounts the firms had sent overseas initially. The majority of these transfers originated from Hong Kong. Authorities suspected that the accounting firms were laundering the funds on behalf of the suspects as part of a professional money laundering syndicate.

Authorities believe that the money laundering was an attempt by the directors of the construction company to hide or disguise the ownership of property. The directors also distanced themselves from the racehorses by having the ownership of the horses held in the names of associates. The associates then returned any profits generated by the horses back to the beneficial owners (the directors).

The members of the network were arrested and convicted on a variety of charges, including conspiracy to defraud, obtaining property by deception, theft, aiding and abetting receipt of a secret commission and furnishing false information. The suspects received penalties ranging from fines to six-and-a-half years imprisonment.

Offence	Fraud
Customer	Individual Business
Industry	Banking (ADIs)
Channel	Physical Electronic
Report type	IFTI
Jurisdiction	Domestic International - Canada, Hong Kong, New Zealand, USA

Designated service	Account and deposit-taking services
Indicators	Large number of horses purchased by customers with unexplained wealth and links to horse racing industry Outgoing funds transfers sent to overseas entities matched by incoming funds transfers, in similar amounts, from different entities located in the same countries Sudden increase in purchase of properties inconsistent with customer's established transaction/wealth profile



Case 5 – AUSTRAC information helped unravel AUD30 million university fraud

Case 6 – Casino 'high roller' stole $78 million from Asian banks

AUSTRAC contributed to a joint international investigation sparked by the suspicious behaviour of a prominent Asian businessman. The investigation exposed a multi-million dollar global fraud committed by an Asian finance manager, who was known as a habitual gambler and international casino 'high roller'.

Authorities in Asia suspected that the suspect had defrauded a number of international banks. AUSTRAC received an international request for information from counterparts in Asia, seeking assistance with their enquiries with regard to the financial activity of the target while he was in Australia.

AUSTRAC data identified that the suspect had conducted significant international funds transfers to Australian casinos, had visited Australia to gamble at the casinos, and had left Australia with substantial amounts of money, presumed to be the proceeds of his gambling. This information proved the initial suspicions of AUSTRAC's Asian counterparts that the suspect had transferred funds to casinos in Australia.

The suspect was arrested and subsequently admitted to Asian authorities that he had embezzled approximately AUD78 million from four international banks by forging signatures of executives of his company and opening accounts in the name of his employer.

Over a four-year period the suspect transferred approximately AUD190 million into an Australian casino account via international funds transfer instructions (IFTIs). In addition, the suspect had visited a number of casinos in London, Macau and Malaysia, in some instances placing bets worth up to AUD400,000.

The authorities in Asia requested further assistance from Australian law enforcement to trace additional proceeds of the suspect's fraud. In conjunction with AUSTRAC, Australian law enforcement discovered an additional AUD30 million in accounts with various Australian casinos, held in the name of the suspect. Of this amount, AUD7 million was restrained by Australian law enforcement under the *Proceeds of Crime Act 2002* and a portion of this was repatriated back to the investigating authorities in Asia.

The suspect pleaded guilty in Asia to six counts of forgery and eight counts of cheating and was subsequently sentenced to 42 years imprisonment.

Offence	Money laundering Embezzlement
Customer	Individual Business
Industry	Banking (ADIs) Gambling services
Channel	Physical Electronic
Report type	IFTI
Jurisdiction	International – Macau, Malaysia, United Kingdom
Designated service	Account and deposit-taking services Gambling services
Indicators	Correlation between high-volume account activity and gambling activity Opening and use of business accounts to transfer funds to Australian and offshore casinos Recent business transaction activity inconsistent with previous transaction history Sudden increase in high-value activity in a casino account Sudden increase in incoming/outgoing high-value international funds transfers through a casino account

Case 7 – Suspect used offshore companies to avoid paying millions in tax

A money laundering and taxation investigation commenced into a suspect who, for more than 10 years, declared minimal income to the Australian Taxation Office (ATO) while living a luxurious lifestyle.

The criminal investigation into the financial dealings of the suspect revealed that he attempted to disguise from the ATO income he had derived from the trading of shares on the Australian Stock Exchange (ASX).

The criminal investigation revealed that the suspect created several offshore companies which, on paper, were owned by 'stichtings' (a foundation in which the identity of the beneficial owner is not publicly available) in the Netherlands.[31] He then sold his ASX shares to the offshore companies at a value well below the true market value in an 'off market' trade. By selling his ASX shares at a discounted price the suspect was able to reduce his tax liabilities in Australia while still maintaining control of the ASX shares. The suspect later arranged for the shares to be sold via his offshore companies at market value. The proceeds of the sales were returned to the suspect in Australia disguised as loans from offshore companies.

By disguising the proceeds of the share sales as a loan, the suspect avoided paying tax on the proceeds in Australia. This method of transferring also created distance between the suspect and the ownership of the shares, while still allowing him to ultimately obtain the benefits from their sale.

Analysis of AUSTRAC information identified that, over two years, the suspect arranged 15 international funds transfer instructions (IFTIs) to send funds from offshore companies under his control based in Switzerland to his Australia-based company.

AUSTRAC analysed financial transaction reports submitted by reporting entities and identified:

- All incoming international funds transfers were valued between AUD 50,000 and AUD 1 million, totalling approximately AUD 4.7 million.
- All incoming international funds transfers were conducted via major banks and were sent in the names of offshore companies linked to the 'stichtings' in the Netherlands. These companies were under the suspect's ultimate control.

The suspect was found guilty of dealing in money valued at over AUD1 million which was to become an instrument of crime (money laundering) and dishonestly obtaining a gain from a Commonwealth entity (ATO). He was sentenced to eight-and-a-half years imprisonment.

31 See Glossary for definition of a 'stichting'.

Offence	Money laundering Tax evasion
Customer	Individual
Industry	Banking (ADIs)
Channel	Electronic
Report type	IFTI
Jurisdiction	International – the Netherlands
Designated service	Account and deposit-taking services Securities market/investment services
Indicators	Account activity inconsistent with customer profile Creation of offshore companies Customer declares minimal income, which is inconsistent with the client's luxurious lifestyle Receiving loans from offshore companies Selling shares to offshore company at a reduced value

Case 8 – Senior public servants stole $1.7 million from state government

AUSTRAC assisted law enforcement to investigate two senior public servants charged with stealing more than AUD1.7 million cash from a state government department.

The public servants, who were married, generated false invoices through their own private company for work they never carried out. The suspects submitted the false invoices to a government department, which paid the suspects' private company for the non-existent services.

At the direction of her husband, the female suspect used companies she controlled to launder the illicit funds by commingling the proceeds of the fraud with legitimate funds generated by the companies. The female suspect dealt with the companies' accountant and gave him the false impression that the illicit funds paid to the companies had been earned through legitimate sources. Income tax was paid on the illicit funds to give the transactions a further appearance of legitimacy.

A suspect transaction report (SUSTR) submitted to AUSTRAC identified that a number of domestic electronic transfers from a third party, an Australia-based company, were paid into the business accounts of companies owned by both suspects. Once the funds were paid into the couple's business accounts they were then transferred into personal accounts held in the suspects' names.

AUSTRAC also received three significant cash transaction reports (SCTR) detailing how the suspects withdrew AUD115,000 cash from their personal accounts over a six-week period.

AUSTRAC prepared a financial assessment report which assisted investigating authorities to identify bank accounts linked to the suspects. Of particular interest to authorities were bank accounts held in the names of the suspects' children. AUSTRAC information showed that AUD50,000 had been withdrawn from these accounts, withdrawals that authorities suspected had been undertaken by the suspects.

Suspect A was charged with 17 counts of stealing as a servant and was sentenced to eight years jail. Suspect B was charged with 14 counts of stealing as a servant and was sentenced to four years imprisonment.

Offence	Fraud
Customer	Individual
Industry	Banking (ADIs)
Channel	Electronic
Report type	SCTR SUSTR
Jurisdiction	Domestic
Designated service	Account and deposit-taking services
Indicators	Account activity inconsistent with customer profile Cash deposits into business account followed by transfers to personal account Significant cash withdrawals over a short period of time Use of children's accounts for transactions Use of third-party company accounts in an attempt to lend transactions a veneer of legitimacy

Case 9 – International funds transfers helped uncover counterfeit car parts scam

A law enforcement agency used AUSTRAC financial transaction data to investigate a suspect who was selling counterfeit vehicle parts on the Australian market. Authorities alleged that this activity was costing a motor car company millions of dollars in lost revenue.

Authorities established that the suspect was importing counterfeit parts into Australia from China using a registered Australian business the suspect operated. After importing the car parts, the suspect sold them in Australia through a leading car manufacturer, claiming the parts were legitimate.

AUSTRAC information revealed that the suspect sent many international funds transfer instructions (IFTIs), in both his name and the name of his business, to pay an automotive parts company in China:

- Over a three-year period international funds transfers worth AUD1.3 million were conducted through personal and business accounts operated by the suspect through various banks and remittance services. During this period the suspect's accounts did not receive any incoming funds transfers from overseas entities, nor record any significant cash activity. This indicated that the bank accounts were receiving funds either from domestic electronic transfers or through cash deposits conducted under the AUD10,000 reporting threshold.
- Between 2004 and 2006 the suspect sent 19 IFTIs, worth approximately AUD260,000, to a Chinese beneficiary, who was identified as a producer/supplier of counterfeit goods.

Additionally, AUSTRAC received a suspect transaction report (SUSTR) indicating that the suspect's account had received a AUD26,000 payment for car parts from an overseas purchaser.

During the investigation authorities found that the overseas purchaser had not received the car parts nor heard from the suspect since sending the funds. This led authorities to believe that the suspect had reneged on the sale and kept the payment from the overseas purchaser.

The suspect was not charged in Australia, but over 30,000 counterfeit car parts were removed from the Australian market. Employees of the manufacturing company in China were successfully prosecuted in that jurisdiction.

Offence	Fraud (counterfeit goods)
Customer	Business
Industry	Banking (ADIs) Remittance services
Channel	Electronic
Report type	IFTI SUSTR
Jurisdiction	International – China
Designated service	Account and deposit-taking services Remittance services (money transfers)
Indicators	Multiple international funds transfers to countries of interest where counterfeit goods are suspected Use of remitter to send large amounts of funds overseas Commingling of illicit funds with legitimate sources of income Multiple, high-value international funds transfers sent to a common beneficiary overseas, from both personal and business accounts Frequent high-value outgoing international funds transfers despite account not receiving any incoming international funds transfers or significant cash deposits

Case 10 – Crime syndicate caught out after police discovered drugs in cricket rollers

AUSTRAC assisted a law enforcement investigation into a syndicate importing precursor chemicals for drug manufacturing from South Africa into Australia. The syndicate attempted to import 44kg of phenylpropanolamine (PPA), enough to produce AUD20 million worth of amphetamines. AUSTRAC also sought assistance in this case from an international counterpart.

The consignment of drugs, which was hidden in multi-threaded rollers used for cricket pitches, was discovered by a law enforcement agency when it arrived in Australia. Police removed the PPA from the rollers and continued their surveillance.

AUSTRAC prepared a financial assessment report which detailed the transaction activity of the syndicate over a seven-year period:

- The syndicate received 30 incoming international funds transfer instructions (IFTIs), mainly from the United Kingdom and South Africa, totalling approximately AUD238,000. The IFTIs ranged in value from AUD1,000 to AUD25,000 and were conducted through a bank and deposited into personal accounts in Australia.
- The syndicate was involved in 22 significant cash transaction reports (SCTRs): three significant cash deposits made by members of the syndicate totalling approximately AUD52,000 which were deposited into three personal accounts owned by one member of the syndicate; and 19 significant cash withdrawals totalling AUD215,000 from three different personal and business accounts owned by syndicate members.

Two men from the syndicate were recruited as couriers and transported the rollers from Sydney to Melbourne. The rollers were delivered to a pre-arranged location where the suspects later opened the rollers and discovered they were empty. One of the men left the premises and was arrested later that day. He pleaded guilty to one count of attempting to possess a precursor chemical and was sentenced to 15 months imprisonment and fined AUD15,000.

Offence	Drug importation
Customer	Individual
Industry	Banking (ADIs)
Channel	Electronic
Report type	IFTI SCTR
Jurisdiction	International – South Africa, United Kingdom
Designated service	Account and deposit-taking services
Indicators	Large cash withdrawals and deposits from multiple accounts owned by the same person Multiple large international funds transfers from high-risk jurisdiction

Case 11 – Local post office used for million dollar fraud and tax evasion scheme

AUSTRAC information assisted authorities investigating a multi-million-dollar postal fraud and tax evasion scheme. The investigation revealed that, over a four-year period, a complex arrangement was set up which enabled the suspects to evade paying postage on bulk postal items.

Suspects A and B set up and operated the fraud using their knowledge of postal operating systems. Suspects A and B conspired with suspects C and D to defraud a Commonwealth entity, resulting in a total loss to the Commonwealth of approximately AUD2.4 million.

Suspects A and B were directors of company X, a bulk mail business which produced, printed and lodged bulk mail items with Australia Post on behalf of customers. Suspects C and D were managers of Licensed Post Offices (LPOs).[32]

Suspects A and B had an arrangement with suspect C for the delivery and processing of bulk mail items over a four-year period. Under the arrangement, tens of thousands of bulk mail items were delivered to the LPO on a regular basis, sometimes twice a day. Suspect C processed these items without properly accounting for them in the LPO system. The amount company X paid for postage was substantially less than the standard payment which should have been made. As a result, the arrangement enabled company X to send bulk mail items at a much lower cost than legally required.

Suspects A and B had a similar arrangement with suspect D, which caused an underpayment of postage charges of more than AUD120,000 over a four-month period.

Suspects A and B also plotted to evade tax by providing the Australian Taxation Office (ATO) with false information about the sales and income of company X over a four-year period. Cheques payable to company X for postal services were disguised and redirected to avoid paying tax. Two methods were used.

Method 1

- Company X used bank deposit books to deposit cheques from clients into the company bank account. The bank deposit books were falsified and the cheque deposits were recorded as 'cash'.
- An employee of company X was told to enter these amounts as directors' dividends instead of company income in the company accounting system.
- The cheques were then cashed at a bank. Suspects A and B received these funds disguised as directors' dividends.

Analysis of AUSTRAC transaction data found a number of significant cash transaction reports (SCTRs) over a period of two-and-a-half years, where approximately AUD91,000 worth of cheques were cashed and withdrawn from company X's bank account. The amounts ranged from AUD10,000 to AUD12,000. These funds were believed to represent directors' dividends paid to suspects A and B.

32 Licensed Post Offices (LPOs) are operated under licence from Australia Post. Each LPO forms part of Australia Post's retail and delivery network.

Method 2

- Suspects A and B sent invoices to clients for services provided. These clients sent cheques to company X as payment for the services.
- Approximately 135 cheques made out to company X by these customers were intercepted by suspects A and B.
- The cheques were directed into the personal bank accounts of both suspects.
- These transactions and invoices were not recorded in the company's accounting system. They were also concealed from the company's accountant.
- In doing so, the income of company X was understated and tax was evaded.

Analysis of AUSTRAC transaction data showed a number of SCTRs showing cash withdrawals from suspect A and B's personal accounts. Suspect A withdrew approximately AUD33,000 in cash over a three-year period, and suspect B withdrew approximately AUD20,000 in cash over a three-month period. The amounts ranged from AUD10,000 to AUD12,000.These funds were believed to represent the proceeds stolen by the suspects.

The loss to the ATO was approximately AUD540,000, which included unpaid Goods and Services Tax (GST) and company tax.

The funds generated from the underpayment of postal charges were partly used to fund suspect A and B's gambling habits. A SCTR submitted to AUSTRAC by a reporting entity showed that suspect B deposited AUD30,000 cash into a gaming account held with an online bookmaker.

Suspect C also stole approximately 55 cheques totalling more than AUD120,000. The cheques were made out by company X, payable to Australia Post. Suspect C deposited these cheques into his personal account and a bank account in the name of his son. He also used the cheques to pay for personal or family debts.

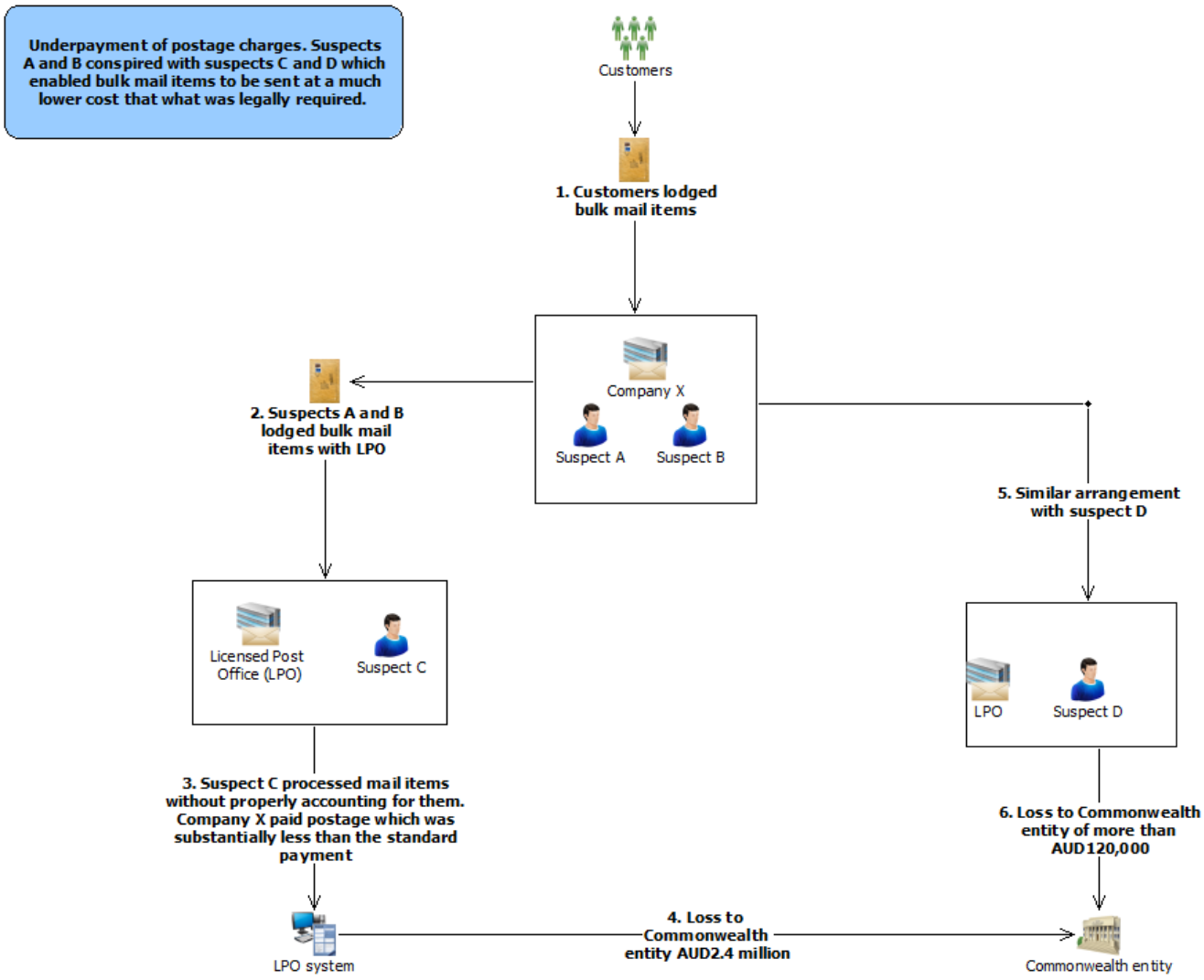
Suspects A and B were convicted of two counts for conspiring to dishonestly cause a risk of loss to a Commonwealth entity. They were both sentenced to seven years and six months imprisonment.

Suspect C was charged with one count of conspiring to dishonestly cause a risk of loss to a Commonwealth entity, and four counts of dishonestly causing a risk of loss to a Commonwealth entity. Suspect C was sentenced to three years and six months imprisonment.

Suspect D was convicted of conspiring to cause a risk of loss to a Commonwealth entity and sentenced to 15 months imprisonment.

Offence	Fraud Tax evasion
Customer	Business Individual
Industry	Banking (ADIs)
Channel	Physical
Report type	SCTR

Jurisdiction	Domestic
Designated service	Account and deposit-taking services
Indicators	Use of third-party accounts Same-day cheque deposits into a business account followed by immediate cash withdrawals of an equivalent value Cheques made out to a company deposited or directed into a personal account of a customer associated with the company Account activity inconsistent with business profile Large cash deposits into online betting account



Case 11 – Local post office used for million dollar fraud and tax evasion scheme

Case 12 – Suspicious transactions revealed Colombian cocaine importations

An Australian law enforcement agency arrested and charged two suspects for importing nearly AUD2 million worth of cocaine into Australia from South America. The international investigation involved Australian, German, and New Zealand law enforcement agencies. AUSTRAC information assisted the investigation by linking the suspects to the purchase of the drugs and the methods used to pay for and import the drugs.

A reporting entity submitted a suspect transaction report (SUSTR) to AUSTRAC highlighting the following activity:

- One of the suspects sent six international funds transfers from five different branches of the same remitter over a one-month period.
- All transfers were for amounts between AUD1,300 and AUD4,200. The total amount transferred was more than AUD20,000.
- The funds were all sent to the same beneficiary in Colombia who collected them from three different locations.
- It appeared as if the suspect may have split the funds transfers into several transactions in attempt to avoid transaction reporting requirements by establishing a number of bank accounts at various banks.

The suspects, originally from New Zealand, flew to Australia to organise the cocaine importation. They transferred funds to Colombia to pay for the cocaine which was hidden in industrial equipment to be shipped to Australia. They also spent over AUD4,000 on arrangements with couriers, mobile phones and apartments, to avoid detection.

German and Australian law enforcement agencies cooperated to intercept the packages in Germany and confirm the presence of the cocaine. Listening devices were attached to the packages which were monitored by Australian law enforcement until they were delivered to the suspects' address in Australia. Telephone calls made by the suspects were also tapped and they were heard discussing the drug shipments.

Both suspects were arrested at their Australian hide-out and charged with attempting to possess a marketable quantity of an unlawfully imported border control drug. The suspects were each sentenced to 11 years imprisonment, with one to be deported to New Zealand upon release.

Offence	Drug importation
Customer	Individual
Industry	Banking (ADIs) Remittance services
Channel	Electronic Physical
Report type	IFTI SUSTR
Jurisdiction	International – Germany, New Zealand, South America
Designated service	Account and deposit taking services Remittance services (money transfers)
Indicators	Multiple international funds transfers conducted at numerous branches over a short period of time to the same overseas beneficiary Multiple international funds transfers below AUD10,000 to avoid reporting obligations International funds transfers to a high-risk jurisdiction

Case 13 – International students used as 'mules' in Pacific drug smuggling ring

An international investigation into drug trafficking revealed a major drug smuggling and money laundering syndicate operating within Australia.

The syndicate operated a sophisticated scheme over a three-year period, using multiple couriers to import cocaine from Colombia to Australia, via New Zealand, the Cook Islands and Tahiti. The syndicate members recruited international students residing in Australia to act as couriers.

The method used by the group to import drugs was:

- Courier A left Colombia for New Zealand or the Pacific Islands, in possession of cocaine.
- Courier B flew from Australia to meet Courier A in New Zealand or a Pacific Island nation.
- Courier A gave the cocaine to Courier B.
- Courier B travelled back to Australia with the cocaine.
- This process was repeated multiple times, using many different couriers.

The syndicate routed the drugs through third-party countries so that the couriers could travel back to Australia without their travel records attracting the suspicion of authorities. Over an 18-month period, the syndicate used this method at least eight times.

Law enforcement counterparts in Colombia informed Australian law enforcement authorities of three individuals residing in Australia who were believed to be part of the syndicate.

Six suspect transaction reports (SUSTRs) detailing financial transactions of these individuals and others attracted law enforcement interest. AUSTRAC produced a financial intelligence assessment on the Australia-based entities which revealed previously unidentified members of the syndicate.

The following financial transactions were recorded on AUSTRAC's database for members of the syndicate during the three-year period:

- Over a two-month period, six SUSTRs were submitted to AUSTRAC by a foreign exchange service. The SUSTRs identified a group of individuals who, on multiple occasions, exchanged Australian currency for United States currency. The SUSTRs indicated that the transactions appeared to be structured to fall under the AUD10,000 cash transaction reporting threshold.[33]
- Over a three-year period, members of the syndicate undertook more than AUD72,000 worth of outgoing international funds transfers. These transactions were primarily sent to beneficiaries in South America and the United States.
- Over this same period, the syndicate recorded a large value of significant cash transaction reports (SCTRs) for cash deposits and withdrawals and the exchange of foreign currency. Forty-two cash deposits (including the purchase of foreign currency) totalling AUD604,000 and 12 cash withdrawals (including the sale of foreign currency) totalling AUD168,100 were recorded.

33 See Glossary for definition of 'structuring'.

International law enforcement agencies worked together to disrupt the activities of the syndicate. The syndicate had planned a one kilogram 'test' run to be sent from Colombia to Australia, via a third county. Unknowingly, the syndicate handed the test package to an undercover law enforcement officer. The package was imported to Australia with the knowledge of Australian authorities and a controlled delivery was conducted. Law enforcement officers arrested three people upon the package's arrival at a domestic address in Australia.

The eight-month international operation resulted in the arrests of 11 members of the syndicate, including two residing in Australia.

One Australia-based syndicate member pleaded guilty to conspiracy to import a commercial quantity of cocaine and was sentenced to 11 years imprisonment. A second member was sentenced to 14 years imprisonment for their involvement.

Offence	Drug importation
Customer	Individual
Industry	Currency exchange Banking (ADIs)
Channel	Electronic Physical
Report type	IFTI SCTR SUSTR
Jurisdiction	Domestic International – Colombia, Pacific Islands, New Zealand, United States
Designated service	Account and deposit-taking services Remittance services (foreign exchange)
Indicators	International funds transfers to a country of interest Structuring of cash deposits and withdrawals A group of individuals undertaking large structured foreign exchange transactions on multiple occasions Foreign currency purchased in structured cash amounts High-volume account activity involving significant amounts of cash funds High-value cash deposits and withdrawals

Case 14 – Syndicate imported 25kg of ecstasy hidden in children's toys

AUSTRAC information initiated a multi-agency investigation into a syndicate responsible for importing more than AUD1.5 million of ecstasy concealed in children's toys.

AUSTRAC referred multiple suspect transaction reports (SUSTRs) to law enforcement, detailing apparent structuring of cash deposits by syndicate members into their bank accounts. Bank staff observed the members of the syndicate undertaking a number of suspicious activities.[34] The suspects:

- arrived at bank branches together
- went to separate bank tellers to conduct structured deposits
- left the bank branches together
- then entered another bank nearby, indicating that the suspects were undertaking structuring activities at multiple banks.

In just four months these accounts received 113 deposits of AUD9,000 each, totalling more than AUD1 million.

Two syndicate members travelled to the United Kingdom to organise the purchase of more than 25 kilograms of ecstasy. In the five months leading up to the importation, the syndicate used multiple banks to send 19 international funds transfer instructions (IFTIs), worth more than AUD250,000, to multiple beneficiaries in the United Kingdom. The syndicate also conducted one funds transfer to Germany worth AUD290,000. Authorities suspected these funds were used to purchase the drugs from overseas suppliers.

Once the drugs were purchased overseas, the syndicate concealed them in children's toys and mailed them to the home address of a syndicate member in Australia. When the shipment of drugs arrived in Australia, authorities replaced the drugs and allowed the packages to be delivered as arranged as part of a controlled delivery.

When the shipment was delivered, law enforcement arrested and charged the suspects with importing a commercial quantity of border-controlled drugs, dealing with proceeds of crime and structuring transactions to avoid reporting requirements. Law enforcement restrained AUD750,000 held in bank accounts operated by the syndicate and AUD100,000 cash found in a safety deposit box.

The syndicate members were sentenced to periods of imprisonment ranging from nine to 14 years.

34 See Glossary for definition of 'structuring'.

Offence	Drug importation Money laundering Structuring
Customer	Individual
Industry	Banking (ADIs)
Channel	Electronic Physical
Report type	IFTI SUSTR
Jurisdiction	Domestic International – Germany, United Kingdom
Designated service	Account and deposit-taking services
Indicators	High-value international funds transfers from Australia with no apparent logical reason Multiple customers attend the same bank branch as a group and conducting simultaneous structured cash deposits Multiple high-value international funds transfers within a short time frame Structuring cash deposits to avoid threshold reporting requirements Sudden increase in transactional activity inconsistent with customer's established profile and/or transaction history

Case 15 – Man convicted after importing human growth hormones from China

AUSTRAC information assisted authorities to identify transactions associated with the illegal importation and possession of human growth hormones (HGH).

Authorities identified a package which had been imported to Australia from China via the postal system. The package was addressed to a post office box in Sydney. Examination of the package showed that it contained 100 vials of a white powder. Subsequent analysis revealed that the powder contained HGH, which was being imported into Australia without approval from the Department of Health and Ageing.

The consignment note for the package listed a billing address for the suspect and a mobile telephone number belonging to the suspect's company. The suspect was also listed as a mail recipient for the post office box in Sydney.

Authorities searched the suspect's home and located his work diary which contained references to HGH. Authorities also found several boxes of vials labelled 'Jintropin' (a form of HGH), a computer containing tracking details for the delivery of the package and files with references to HGH and Jintropin. Enquiries revealed the suspect did not have a permit to import HGH.

Authorities provided AUSTRAC with copies of records obtained from the main suspect, which included information about financial transactions to overseas beneficiaries. Analysis of the AUSTRAC database revealed a strong correlation between these records and outgoing international funds transfer instructions (IFTIs) to China and Lebanon. Authorities determined that the records held by the suspect were instructions to his associates to send funds overseas as payment for the drugs.

AUSTRAC data indicated that the suspect and his wife sent approximately AUD114,000 worth of IFTIs to China, Lebanon, Syria, Kuwait and Qatar over a 10-year period. The data showed that:

- the suspect, a company of which he was a director, and the suspect's wife sent approximately AUD60,000 worth of IFTIs to the same beneficiary in China over a two-year period
- the IFTIs ranged in amounts from AUD1,500 to AUD25,000, and were sent via remittance services, with one IFTI sent via a bank.

AUSTRAC received a suspect transaction report (SUSTR) detailing the activities of the suspect's wife. A reporting entity reported that:

- the suspect's wife had undertaken three 'structured' IFTIs to China and Lebanon totalling AUD23,000 over a 13-day period
- the IFTIs were paid for in cash and were structured in amounts between AUD7,000 and AUD9,000
- two IFTIs were sent to China on the same day from different outlets
- the same beneficiary in China received IFTIs from the suspect, his wife and the suspect's associates
- the suspect's wife provided inconsistent information about her date of birth to reporting entity staff when undertaking transactions.

Under the *Customs Act 1901* the suspect was convicted of intentionally importing a 'tier 1 good', namely HGH, without approval. The suspect received a two-year good behaviour bond.

Offence	Drug importation
Customer	Individual
Industry	Banking (ADIs) Remittance services
Channel	Electronic Physical
Report type	IFTI SUSTR
Jurisdiction	International – China, Kuwait, Lebanon, Qatar, Syria
Designated service	Account and deposit taking services Remittance services (money transfers)
Indicators	International funds transfers to a high-risk jurisdiction Multiple customers conducting international funds transfers under the guidance or instruction of another individual (i.e. use of 'third parties') Multiple customers conducting international funds transfers to the same overseas beneficiary Structuring cash transactions (outgoing international funds transfers) to avoid reporting requirements

Case 16 – Dozens of suspicious cash transfers exposed $2 million unpaid tax bill

AUSTRAC information initiated an investigation into a suspect who had been evading tax for a period of approximately nine years and had an unpaid tax bill totalling over AUD2 million.

Suspect transaction reports (SUSTRs) were submitted by a credit union to AUSTRAC and identified a suspect who was 'structuring' cash withdrawals from his personal bank accounts to avoid the AUD10,000 threshold for significant cash transaction reports (SCTRs).[35] The suspect often made multiple structured withdrawals from each of his bank accounts on the same day.

The suspect made approximately 20 cash withdrawals just below the AUD10,000 threshold from two bank accounts within 30 days, totalling over AUD180,000. During a second 30-day period the suspect withdrew from three different bank accounts a further AUD470,000 cash, structured into amounts of between AUD9,000 and AUD9,900. During this time, a number of SUSTRs were submitted about the suspect's activity. These were disseminated by AUSTRAC to law enforcement agencies who initiated an investigation into the matter. AUSTRAC continued to provide information and assistance throughout the investigation.

Law enforcement officers obtained a restraining order and more than AUD75,000 was restrained from the suspect's bank account, with another AUD680,000 seized when warrants were executed on the suspect's residence. The suspect was found guilty and sentenced to five months jail for conducting transactions to avoid reporting obligations and possessing property from the proceeds of crime.

Offence	Tax evasion
Customer	Individual
Industry	Banking (ADIs)
Channel	Physical
Report type	SUSTR
Jurisdiction	Domestic
Designated service	Account and deposit-taking services
Indicators	High number of cash withdrawals below the AUD10,000 reporting threshold High volume of cash withdrawn from accounts during a short time period, in apparently structured amounts

35 See Glossary for definition of 'structuring'.

Case 17 – Money exchange business laundered millions for drug syndicate

A multi-million dollar money laundering syndicate was dismantled following a 12-month joint agency investigation. The investigation uncovered a currency exchange business being used to launder the proceeds of crime for a European drug syndicate.

Law enforcement officers suspected that the currency exchange business had laundered more than AUD2 million for the drug syndicate. During the law enforcement investigation, financial transaction activity recorded on AUSTRAC's database helped unravel the money laundering process used by the syndicate.

A suspect representing the European drug syndicate arrived in Australia to transfer back to Europe the illicit cash proceeds generated by a drug importation. The following steps outline the method used to launder the funds.

- When the suspect arrived in Australia, European syndicate members informed him that the illicit cash was located in a safe in an apartment. The suspect followed instructions and took possession of more than USD2 million cash.
- Over a 10-day period the suspect delivered the US dollars, in large amounts, to the operators of the currency exchange business.
- The operators of the currency exchange accepted the US dollars and instructed an agent, on their behalf, to deposit the cash into third-party bank accounts in structured amounts worth less than AUD10,000. The agent undertook hundreds of cash deposits, often depositing cash into the same account and on the same day, but at different bank branches. The deposits of US dollars were all in amounts worth less than AUD10,000 to avoid triggering threshold transaction reporting requirements.

The activities of the currency exchange business came to AUSTRAC's attention after it was the subject of a number of suspect transaction reports (SUSTRs) submitted by industry. The SUSTRs detailed the suspicious transactions undertaken by the operators of the currency exchange, including:

- structuring of foreign currency exchange transactions and travellers cheques
- always exchanging the same two currencies: United States Dollar and Hong Kong Dollar.

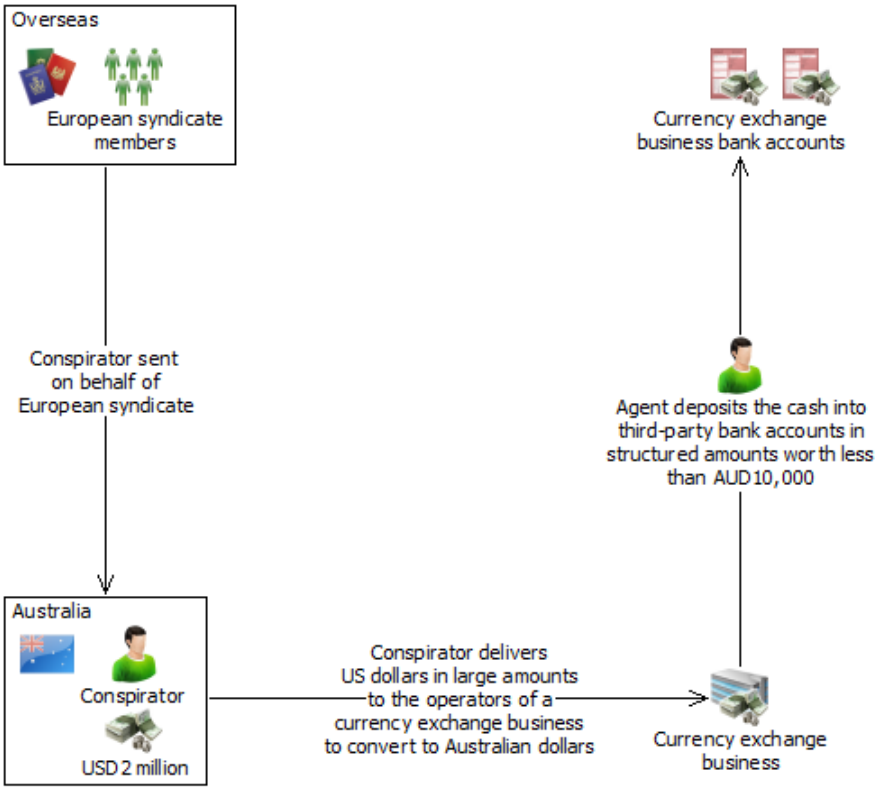
AUSTRAC prepared a financial intelligence assessment on the exchange business's suspicious activity and disseminated it to a law enforcement agency.

The suspect representing the European drug syndicate was arrested in possession of more than 28 kilograms of illicit drugs with an estimated value of AUD8 million.

Law enforcement officers seized a further AUD47,500 cash and restrained approximately AUD247,000 in assets related to the currency exchange operators.

The two operators of the money exchange business were charged, under section 11.5 of the *Criminal Code Act 1995*, on two counts of conspiracy to commit an offence (money laundering) against Commonwealth law. They were convicted and sentenced to seven years imprisonment on each count.

Offence	Money laundering
Customer	Business Individual
Industry	Banking (ADIs) Remittance services
Channel	Electronic Physical
Report type	SUSTR
Jurisdiction	Domestic International - Europe
Designated service	Account and deposit-taking services Remittance services (foreign exchange)
Indicators	Structuring of cash transactions by currency exchange business to avoid reporting requirements Multiple structured cash deposits using a foreign currency Multiple same-day cash deposits into same accounts at different branches Multiple structured transactions to purchase foreign currency and/or travellers cheques



Case 17 – Money exchange business laundered millions for drug syndicate

Case studies

Gambling services

Case studies – Gambling services

Case 18 – Card skimming syndicate laundered criminal proceeds through casinos

Suspect A was arrested by law enforcement upon arrival in Australia, where he was found to be in possession of card skimming technology. This included computer disks, a laptop, a card encoder, an ATM feeder 'face unit' and 31 blank ATM cards. The suspect was an international student residing in Australia.

Upon his arrest, law enforcement commenced an investigation into his activity and discovered a card skimming syndicate operating in Australia which laundered the proceeds of its crimes through casinos. Analysis of AUSTRAC financial transaction data associated with suspect A identified three additional members of the syndicate and their activities.

Members of the syndicate regularly visited casinos. Over a five-month period, AUSTRAC received threshold transaction reports (TTRs) indicating that suspect A had cashed in more than AUD180,000 worth of gaming chips at an Australian casino. However, transaction records showed that the suspect had not previously purchased a corresponding amount of gaming chips at the casino. This suggested that the suspect may have purchased the chips directly from another player before cashing them out, while claiming they were actually his 'winnings'.

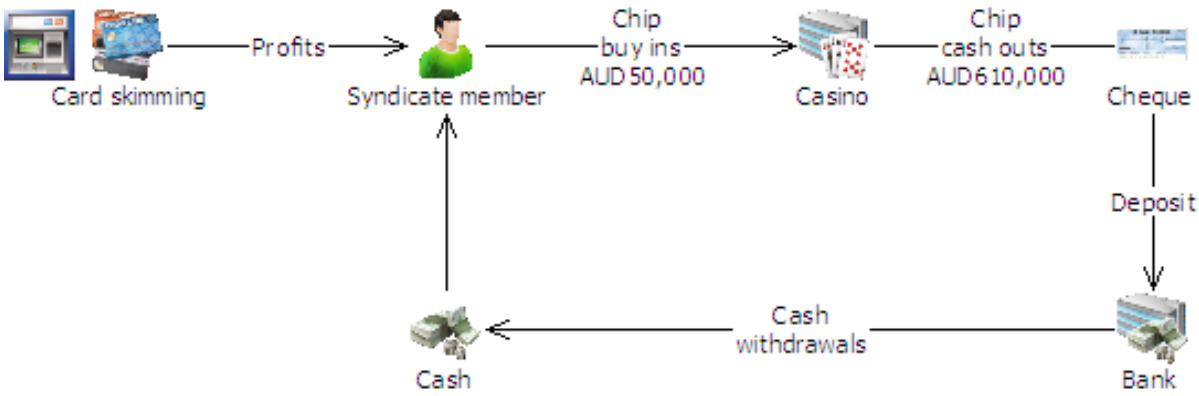
AUSTRAC information was also used to identify the irregular gaming activity of suspect B. Information on AUSTRAC's database indicated that, over a 12-month period, suspect B had purchased AUD50,000 worth of gaming chips at a casino. However, records indicated that the suspect had cashed out more than AUD610,000 worth of gaming chips at the casino. Suspect B also made regular cash deposits and withdrawals, often in amounts over the reporting threshold of AUD10,000, into bank accounts in Australia in the days following the casino transactions.

A suspect transaction report (SUSTR) was submitted by an Australian casino, noting that:

- suspect B presented AUD28,000 worth of casino chips to a cashier to be cashed out, before handing the cash proceeds to another person, believed to be suspect A
- the value of gaming chips cashed out by suspect B did not correspond with the suspect's observed game play at the casino due to the high volumes of winnings compared to funds withdrawn for gambling purposes, nor did it correspond with the expected financial activity of a young university student.

A second SUSTR was also submitted by an Australian financial institution detailing suspicious transactions conducted by suspect B. Over a three-month period suspect B deposited more than AUD155,000 in cash into an account, indicating to bank staff that these funds were casino winnings. The majority of these funds were then withdrawn in cash at the bank and via ATMs at the casino.

Suspect A was charged under section 480.6 of the *Criminal Code Act 1995* for the importation of a thing to dishonestly obtain or deal in personal information.



Case 18 – Card skimming syndicate laundered criminal proceeds through casinos

Offence	Fraud Money laundering
Customer	Individual
Industry	Banking (ADIs) Gambling services
Channel	Electronic Physical
Report type	SUSTR TTR
Jurisdiction	Domestic
Designated service	Gambling services Account and deposit-taking services
Indicators	Casino chip cash outs do not correspond with observed game play Customer undertakes consistent high-volume gaming chip 'cash outs' which are claimed to be winnings, an activity that appears unlikely with the comparatively low amounts of funds withdrawn by the customer for gaming purposes Funds from casino chip cash outs given to third parties Regular cash deposits into a bank account, followed by cash withdrawals High-volume cash deposits over a short period of time that does not match customer's established financial activity profile Account activity inconsistent with customer profile

Case studies

Remittance services

Case studies – Remittance services (money transfers)

Case 19 – Law enforcement investigation closed down Filipino child exploitation ring

AUSTRAC information assisted a law enforcement investigation into a suspected child exploitation website which led to the arrest of more than 20 individuals. Authorities seized more than 300,000 child pornography images and a number of overseas child victims were identified and removed from the risk of further sexual exploitation.

Law enforcement officers uncovered one of the world's largest child exploitation websites, which allowed users to post child exploitation images and request similar images. Upon execution of a search warrant on the Australia-based website administrator and operator, law enforcement officers assumed control of the internationally hosted site.

Law enforcement officers used internet protocol (IP) addresses to monitor offenders who used the website to post and trade child exploitation material. More than 20,000 internet addresses from over 100 countries were used to provide images to the site. Almost 1,000 of the IP addresses used were Australian addresses.

Analysis of AUSTRAC information identified that, over three years, the main suspect in the investigation conducted more than 30 outgoing international funds transfer instructions (IFTIs) to multiple beneficiaries in the Philippines.

Authorities suspect that the outgoing IFTIs were for the purchase of explicit material to feature on the website. The IFTIs were for amounts between AUD18 and AUD480, and totalled more than AUD6,400. All funds were transferred via a remittance business.

The main suspect pleaded guilty to using a carriage service to make child pornography material available and possessing child exploitation material and was sentenced to three-and-a-half years imprisonment.

Offence	Child exploitation
Customer	Individual
Industry	Remittance services
Channel	Electronic Physical
Report type	IFTI
Jurisdiction	International – Philippines
Designated service	Remittance services (money transfer)
Indicators	Multiple low-value international funds transfers to a high-risk jurisdiction Multiple international funds transfers sent to the same beneficiary

Case 20 – 'Cuckoo smurfing' used in million dollar money laundering scheme

AUSTRAC disseminated a suspect transaction report (SUSTR) to a law enforcement partner agency, which sparked an investigation into a widespread money laundering syndicate.

Investigations revealed that the syndicate, which operated in multiple states across Australia, was using a money laundering technique known as 'cuckoo smurfing'.[36]

The criminal syndicate misused the bank account of a legitimate Australia-based export company in its money laundering scheme. The scheme also exploited legitimate international funds transfers made by a customer of the export company, who was based in Pakistan.

The Pakistan-based customer sent funds, via a remittance business in Pakistan, to the Australia-based export company. The funds transfers were payments for legitimate invoices owing to the Australian company.

However, investigations revealed that the Pakistani remitter used to remit the funds had connections with money laundering crime syndicates in Australia.

The following steps outline how the illicit funds were laundered:

1. The Pakistan-based customer of the export company attempted to send funds via a Pakistani remittance business to the export company's Australian bank account, for the payment of legitimate invoices.
2. The Pakistani remitter informed the money laundering syndicate in Australia of the export company's bank account details and the amounts required to be deposited into the company's account in Australia.
3. Australian syndicate members made a number of cash deposits into the Australian account of the export company equal in value to the expected payments from Pakistan. The cash deposits were often made in structured amounts, intended to fall below the AUD10,000 cash transaction reporting threshold.[37] These funds were the proceeds of illicit activities undertaken in Australia.
4. Meanwhile, the remitter in Pakistan transferred the funds provided by the customer in Pakistan into another account in Pakistan, to be later accessed by a member of the syndicate.

Over a 15-month period, 13 SUSTRs were reported to AUSTRAC by major banks, identifying multiple structured cash deposits made by third parties into the export company's Australian bank account.

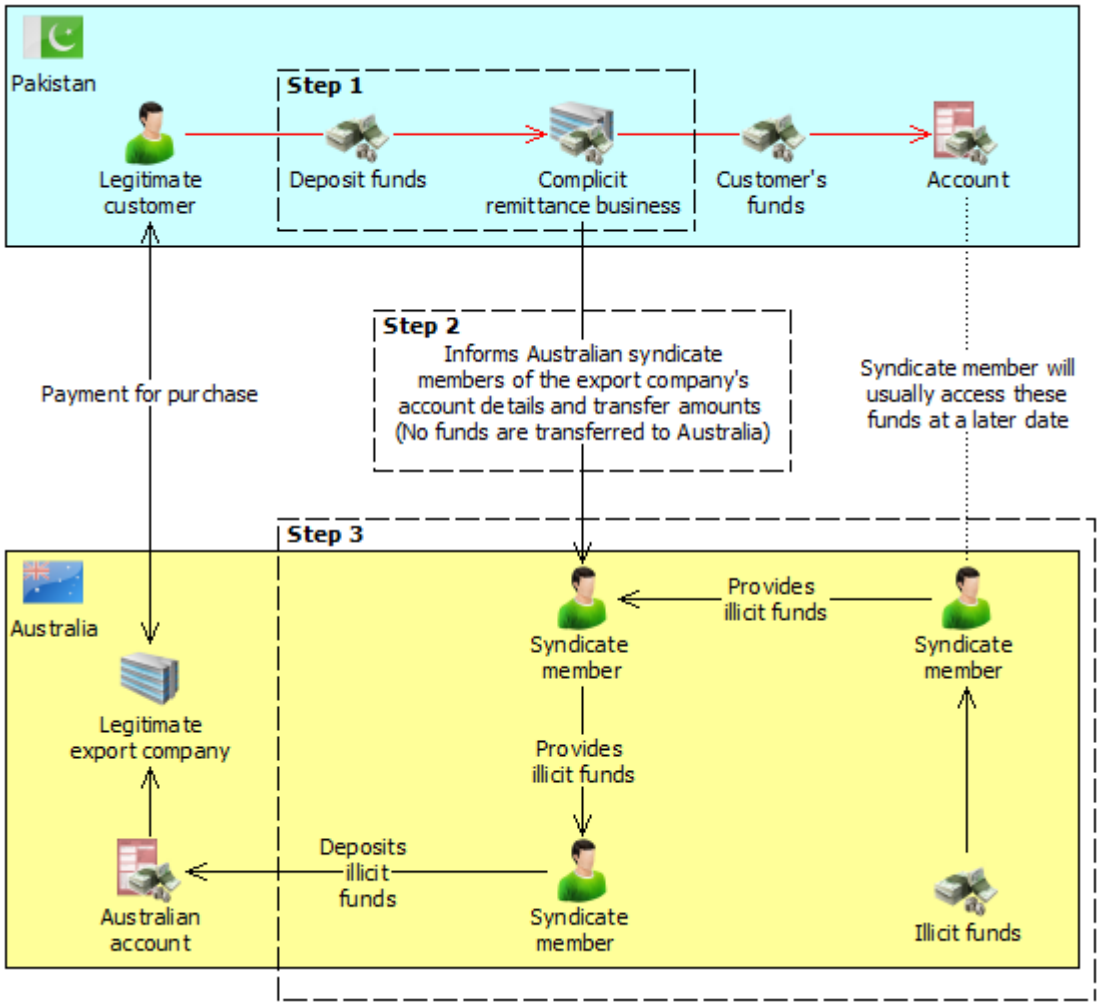
During this period approximately ten syndicate members conducted 217 cash deposits totalling AUD2.1 million into the Australian bank account of the export company. A total of 196 of these cash deposits were structured deposits, totalling AUD1.6 million. The structured deposits were primarily conducted in amounts between AUD8,000 and AUD9,500 at multiple bank branches throughout Sydney and Melbourne.

---

36 See Glossary for definition of 'cuckoo smurfing'. A more detailed explanation of 'cuckoo smurfing' can be found in the *AUSTRAC Typologies and Case Studies Report 2008*, p. 7, <www.austrac.gov.au/typologies_2008.html>.

37 See Glossary for definition of 'structuring'.

The syndicate members were careful to provide the bare minimum of personal information when undertaking the cash deposits. Nevertheless, 18 bank deposit receipts examined by law enforcement revealed identifying characteristics such as phone numbers. This information led to the identification of some of the depositors.



Case 20 – 'Cuckoo smurfing' used in million dollar money laundering scheme

Reporting requirements for threshold transaction reports (TTRs) were strengthened on 1 October 2011 to require reporting entities to include details of the individual conducting a threshold transaction where that individual is not the customer of the designated service.

Effectively, this additional TTR reporting requirement means that reporting entities must report details of any third parties depositing physical currency or e-currency of AUD10,000 or more (or foreign currency equivalent) into an account, a requirement that assists AUSTRAC to identify the use of third parties to launder illicit cash.

Offence	Money laundering
Customer	Business
Industry	Banking (ADIs)
Channel	Physical
Report type	SUSTR
Jurisdiction	Domestic International - Pakistan
Designated service	Account and deposit-taking services
Indicators	Multiple third-party cash deposits into the same account conducted on the same day Third-party cash deposits conducted at multiple branches in the same city Third-party customer undertaking transaction provides the bare minimum of information to reporting entity about the transaction Structuring of cash deposits

Case 21 – Remittance business laundered millions in drug money through student's bank account

A suspect transaction report (SUSTR) triggered AUSTRAC's automated monitoring system, revealing a syndicate using a technique known as 'cuckoo smurfing' to launder funds, suspected to be the proceeds of illicit drug sales.[38]

The SUSTR was submitted after a legitimate customer in Indonesia attempted to transfer AUD1.75 million to his daughter, who was studying in Australia. However, the funds were unlawfully diverted by an Indonesian remittance dealer, who was connected with an international money laundering syndicate operating in Australia.

The money laundering methodology operated as follows:

1. The customer in Indonesia deposited cash into the remittance dealer's bank account in Indonesia. He provided the remittance dealer with his daughter's Australian bank account details and instructed that the deposited funds be transferred to his daughter.

2. Rather than transfer the funds to Australia, the Indonesian remittance dealer informed members of the syndicate in Australia of the daughter's bank account details. The syndicate members in Australia used this information to make a number of 'third-party' cash deposits into the account. The syndicate members made multiple cash deposits at bank branches throughout New South Wales and Victoria. Often these deposits were made on the same day, prompting bank staff to suspect that the cash deposits may have been for illicit purposes.

3. Over a six-week period, the daughter's Australian bank account received 60 cash deposits totalling AUD1.75 million. The cash deposits ranged from AUD3,500 to AUD150,000.

4. The cash the customer had originally deposited into the remitter's bank account in Indonesia was transferred to another bank account (Account X) to be accessed by the syndicate members at a later time.

5. This completed the 'cuckoo smurfing' operation. With the assistance of the complicit remittance dealer, the syndicate had introduced illicit cash into the Australian banking system via the bank account of the unsuspecting customer in Australia. This left the syndicate free to access the 'clean' money, which the Indonesian remitter had transferred into Account X, without attracting the attention of authorities.

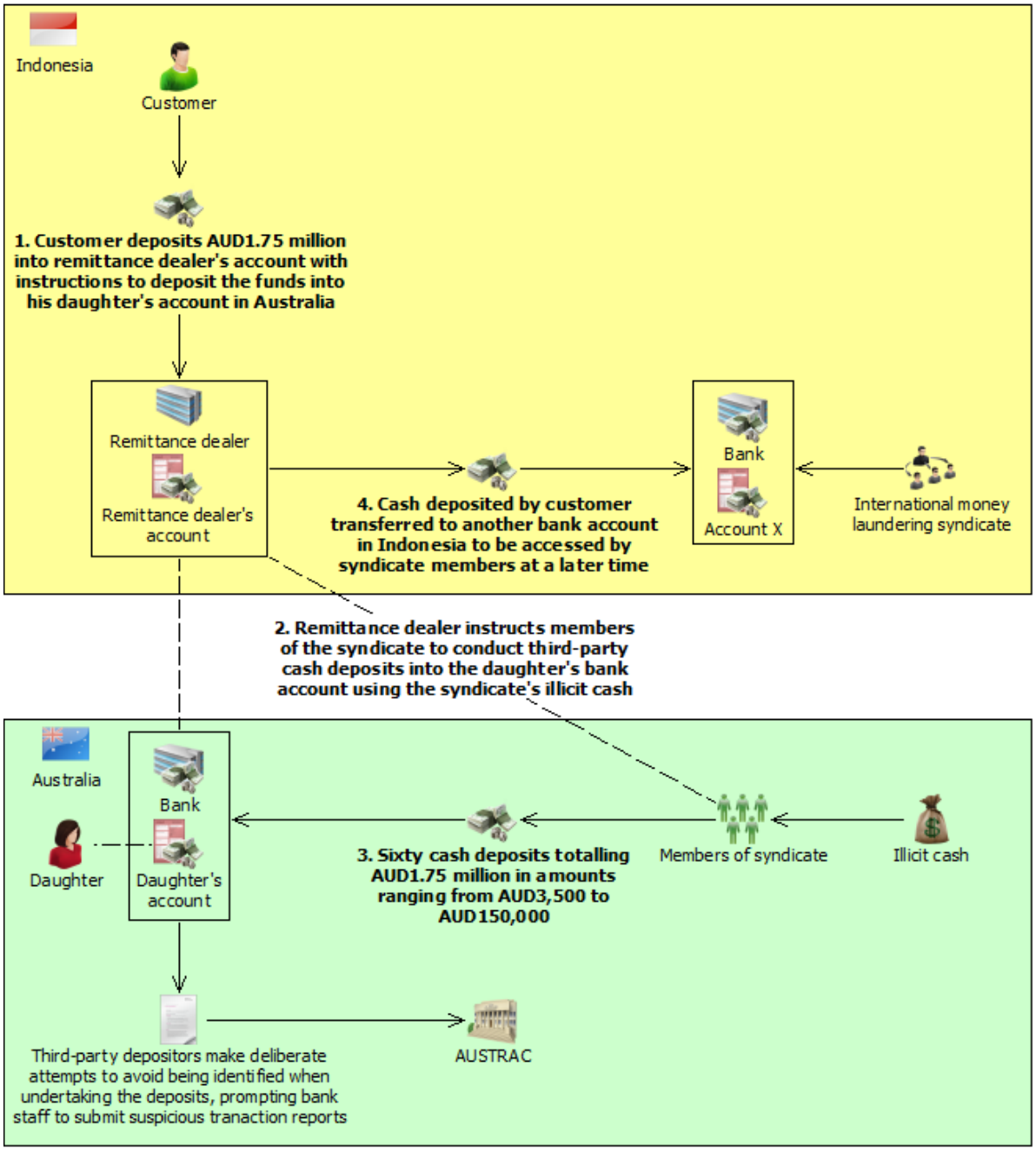
38 See Glossary for definition of 'cuckoo smurfing'. A more detailed explanation of 'cuckoo smurfing' can be found in the *AUSTRAC Typologies and Case Studies Report 2008*, p. 7, <www.austrac.gov.au/typologies_2008.html>.

The third-party depositors made deliberate attempts to avoid being identified when undertaking the deposits, prompting bank staff in Australia to report the transactions to AUSTRAC as suspicious. In particular, four SUSTRs submitted to AUSTRAC detailed how:

- the third-party depositors attempted to avoid being identified by not wanting to provide their names and details on deposit slips and by writing telephone/fax numbers in an illegible manner
- the third-party depositors only used their given names on deposit slips.

Authorities also identified that one of the third-party depositors was involved with a drug syndicate.

Offence	Money laundering
Customer	Business Individual
Industry	Remittance services Banking (ADIs)
Channel	Physical
Report type	IFTI SCTR SUSTR
Jurisdiction	Domestic International – Indonesia
Designated service	Account and deposit-taking services
Indicators	High levels of cash deposits far in excess of expected legitimate banking activity of the account holder Multiple cash deposits, at multiple bank branches, often on the same day Third-party cash deposits made at branches distant from the branch at which the account is held Third-party cash deposits made by unidentifiable persons Third-party deposits made by evasive customers with incomplete identification



Case 21 – Remittance business laundered millions in drug money through student's bank account

Case 22 – Australian jailed after purchasing child exploitation material from Philippines

AUSTRAC information assisted authorities to identify an Australian suspect who was accessing child exploitation material produced in the Philippines.

Australian law enforcement authorities received information from counterparts in the Philippines about an individual they arrested in the Philippines for child sex exploitation-related offences, including the production of child pornography material.

Searches of the AUSTRAC database revealed that the Australian suspect had been sending international funds transfer instructions (IFTIs) to the Philippines-based individual.

Analysis of AUSTRAC information identified that over a 16-month period the Australia-based suspect undertook at least 13 outgoing IFTIs to the individual arrested in the Philippines. The IFTIs were for amounts between AUD55 and AUD680 and totalled more than AUD4,450. All funds were transferred via a remittance business, with the majority conducted online. The IFTIs were payments by the suspect to enable him to access a child pornography website operated by the Filipino suspect.

Australian authorities executed a search warrant at the suspect's home and seized a large amount of child pornography consisting of more than 156,000 images and 1,325 video files.

The suspect was convicted of two counts of using a carriage service to access child pornography material, two counts of using a carriage service to make available child pornography material and possessing child abuse material. He was sentenced to three-and-a-half years imprisonment.

Offence	Child exploitation
Customer	Individual
Industry	Remittance services
Channel	Electronic
Report type	IFTI
Jurisdiction	International – Philippines
Designated service	Remittance services (money transfer)
Indicators	Multiple low-value international funds transfers to a high-risk jurisdiction Multiple international funds transfers sent to the same beneficiary

Case 23 – Suspect jailed after internet drug purchase

AUSTRAC assisted a law enforcement investigation into the importation and distribution of mephedrone (MCAT), an amphetamine-type stimulant imported from Israel.

The suspect bought MCAT (also known as 'Miaow' or 'Mm-cat') over the internet through a business-to-business trading website, blended the drug with caffeine powder and then sold it in capsules. The suspect imported approximately four kilograms of the drug and used employees from his cleaning business to convert the drug into capsule form.

AUSTRAC disseminated an intelligence assessment to law enforcement detailing that the suspect had, over a two-year period, sent a number of international funds transfer instructions (IFTIs) to Israel, worth a total of AUD102,000. The IFTIs were sent via a remittance service provider.

Two suspect transaction reports (SUSTRs) were also submitted to AUSTRAC regarding the suspect's international funds transfers, indicating that the suspect undertook numerous same-day international transfers through different branches of a remittance service provider. The transactions appeared to be structured to fall below the AUD10,000 cash reporting threshold.

Analysis of the AUSTRAC database also identified additional Australia-based entities that had sent funds to the same beneficiary in Israel. Authorities believed these transfers were also payments for the importation of MCAT.

The suspect was arrested at an Australian casino in possession of AUD24,000 worth of cash and casino chips. Authorities searched the suspect's property and discovered an additional AUD100,000 cash.

The suspect was charged with drug importation and attempting to pervert the course of justice against the *Criminal Code Act 1995* and was sentenced to eight years imprisonment.

Offence	Drug importation
Customer	Individual
Industry	Remittance services
Channel	Electronic
Report type	IFTI SUSTR
Jurisdiction	International – Israel
Designated service	Remittance services (money transfer)
Indicators	Multiple same-day international transfers to the same overseas beneficiary Multiple international transfers paid for in structured cash amounts below the AUD10,000 cash reporting threshold International funds transfers to high-risk jurisdiction

Appendix A & B
Case study index
Glossary & abbreviations

Appendix A – Indicators of potential money laundering/terrorism financing activity

There are numerous indicators which may assist reporting entities to identify potential money laundering or terrorism financing activity.

Although the existence of a single indicator does not necessarily indicate illicit activity, it should prompt 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 informs its response to the situation.

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

Money launderers and terrorism financiers will continually look for new techniques to obscure the origins of illicit funds and lend their activities an appearance of legitimacy. AML/CTF officers should continually review their products, services and individual customers to maximise the effectiveness of their organisation's internal AML/CTF systems and training.

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

- A group of individuals undertaking large structured foreign exchange transactions on multiple occasions
- A large number of individuals conducting domestic electronic transfers and direct deposits to linked company bank accounts
- Account activity inconsistent with customer profile
- Customer receives international funds transfers declared as loans from a foreign lender
- Customer undertakes consistent high-volume gaming chip 'cash outs' which are claimed to be winnings, an activity that appears unlikely given the comparatively low amounts of funds withdrawn by the customer for gaming purposes
- High-value cash deposits to pay for international funds transfers
- High-volume account activity involving significant amounts of cash funds
- High volume of cheques cashed
- International funds transfers to a high-risk jurisdiction
- Large cash deposits into an online betting account
- Multiple customers conducting international funds transfers to the same overseas beneficiary
- Multiple customers conducting international funds transfers under the guidance or instruction of another individual (i.e. use of 'third parties')
- Outgoing funds transfers sent to overseas entities matched by incoming funds transfers, in similar amounts, from different entities located in the same countries
- Opening and use of business accounts to transfer funds to Australian and offshore casinos
- Regular or multiple cash deposits below the AUD10,000 reporting threshold (i.e. structured cash deposits)
- Sudden increase in purchase of properties inconsistent with customer's established transaction/wealth profile
- Third-party cash deposits made at branches distant from the branch at which the account is held
- Third-party cash deposits made by unidentifiable persons or by evasive customers with incomplete identification
- Use of multiple large cash payments for mortgage payments

Appendix B – Report references and further reading

References

- Australian Transaction Reports and Analysis Centre, *AUSTRAC Regulatory Guide*, AUSTRAC, West Chatswood, NSW, 2009
- Australian Transaction Reports and Analysis Centre, *AUSTRAC Typologies and Case Studies Report 2008,* AUSTRAC, West Chatswood, NSW, 2008
- Australian Transaction Reports and Analysis Centre, *Money Laundering in Australia 2011*, AUSTRAC, West Chatswood, NSW, 2011
- Chaikin D & Sharman J, *APG/FATF Anti-Corruption/AML/CFT Research Paper,* Asia/Pacific Group on Money Laundering (APG) and FATF, Paris, 2007
- Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation,* FATF, Paris, 2012
- Financial Action Task Force, *Laundering the Proceeds of Corruption*, FATF, Paris, 2011
- Financial Action Task Force, *Report on Money Laundering Typologies 2002-2003*, FATF, Paris, 2003

Case study index

	Case study no.
real estate/property	2, 3, 5, 16
remittance services (money transfers) (designated service)	9, 12, 13, 15, 17, 19–23
scams (inc. 'cold-call' investment and Ponzi scams)	2, 4, 9
SCTRs (significant cash transaction reports)	4, 8, 10, 11, 13, 16, 21
securities market/investment services (designated service)	2, 3, 4, 7
solicitor	3
structuring (of transactions)	3, 13–17, 20, 23
SUSTRs (suspect transaction reports)/SMRs (suspicious matter reports)	2, 3, 4, 8, 9, 12–18, 20, 21, 23
taxation (evasion of, fraud)	1, 7, 11, 16
third parties	2, 3, 4, 8, 11, 15, 17, 18, 20, 21
trust accounts/funds	3, 4
TTRs (threshold transaction reports)	18, 20
unexplained income	3, 5, 18

Glossary and abbreviations

Glossary

beneficiary (or beneficiary customer)	The person (or organisation) who is the ultimate recipient of funds being transferred.
bill of lading	A document signed by a carrier (a transporter of goods) or the carrier's representative and issued to a consignor (the shipper of goods) that evidences the receipt of goods for shipment to a specified designation and person.
cold-calling	Cold-calling is the marketing process of approaching prospective customers or clients – typically via telephone, by email or through making a connection on a social network – who were not expecting such an interaction. The word 'cold' is used because the person receiving the call is not expecting a call or has not specifically asked to be contacted by a sales person. A cold call is usually the start of a sales process.
commingling	The process of combining illicit funds with legitimate business funds to make the illicit funds appear legitimate.
cuckoo smurfing	A money laundering typology in which perpetrators seek to transfer wealth through the bank accounts of innocent third parties. The term 'cuckoo smurfing' originated in Europe because of similarities between this typology and the activities of the cuckoo bird. Cuckoos lay their eggs in the nests of other species of birds which then unwittingly take care of the eggs believing them to be their own.
factoring	The purchase of a seller's debts, often without recourse, by a factoring company which then undertakes all credit control, collection and sales accounting.
forfaiting	The purchase of an exporter's receivables (the amount importers owe the exporter) at a discount by paying cash. The forfaiter, the purchaser of the receivables, becomes the entity to whom the importer is obliged to pay its debt.
high-risk jurisdictions	'High-risk jurisdictions' are jurisdictions known to be a source or conduit of narcotics or other significant criminal activity, any jurisdiction subject to sanctions, jurisdictions known to be a secrecy haven or preferential tax regime, or jurisdictions linked to proscribed terrorist organisations.
investment fraud	Investment frauds convince investors to make purchase or selling decisions on the basis of false information. Most investment frauds target the general public or a particular community within the general public. Investment frauds may take the form of telemarketing, direct mail, seminars or door-to-door selling schemes.
letter of credit	A letter of credit is a common method of financing international trade. A letter of credit is a commitment to pay between the importer's bank, known as the issuing bank, and the exporter's bank, known as the accepting or negotiating bank. It guarantees payment of a specified sum in a particular currency, as long as defined conditions are met, including submitting prescribed documents within a fixed time frame.

money laundering cycle	The money laundering cycle describes the typical three-stage process criminals use to conceal the source of illicit funds and make funds appear legitimate: Placement – Introducing illegal funds into the formal financial system (for example, making 'structured' cash deposits into bank accounts). Layering – Moving, dispersing or disguising illegal funds or assets to conceal their true origin (for example, using a maze of complex transactions involving multiple banks and accounts, or corporations and trusts). Integration – Investing these now distanced funds or assets in further criminal activity or legitimate business, or purchasing high-value assets and luxury goods. By this stage in the cycle the funds or assets appear to have been legitimately acquired.
money laundering syndicate	A criminal group, based in Australia or overseas, that provides specific money laundering services to domestic and international crime groups operating in Australia. Also called specialist money laundering syndicates because money laundering is the primary or only illicit activity such groups engage in, unlike other crime groups where money laundering is a secondary enabling activity for their primary criminal activity (such as drug trafficking).
open account	Open account is remittance undertaken through a bank by international funds transfer instruction (IFTI) or through the purchase from a bank of a bank draft. In Australia, open account facilities are reportedly the most frequently used method to settle trade debts due to their speed, reliability and the funds – once received – being immediately available to the exporter.
Ponzi scheme	One of the simplest, yet most effective scams is the Ponzi scheme. In these schemes the promoter promises investors a very high return on their investment, while assuring investors the investment is secure. Part of the money deposited by early investors is used by the scheme's promoter to pay subsequent investors their first dividend cheques or interest. These initial returns help convince victims that the scheme is both lucrative and sound. In the early stages of a Ponzi scheme, only a few investors are required for the scheme to be successful. The promoter continues paying the investors dividends until the investors are comfortable with their investments and willing to invest more.
proceeds of crime	Any money or other property that is wholly or partly derived or realised, directly or indirectly, by any person from the commission of an offence against a law of the Commonwealth, a state, a territory or a foreign country that may be dealt with as an indictable offence (even if it may, in some circumstances, be dealt with as a summary offence).
professional facilitator	'Professional facilitators' or 'gatekeepers' act as an entry point for those seeking to use financial and corporate systems. Examples of professional facilitators include legal practitioners, accountants and financial planners.
remittance services/ remittance dealer (remitter)	Also known as 'money transfer businesses', these are financial services that accept cash, cheques, other monetary instruments or other stores of value in one location and pay a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, transfer or through a clearing network to which the money/ value transfer system belongs.

round robin tax evasion scheme	A scheme where money is transferred to an overseas account and then returned 'tax free' to personal accounts, usually disguised as a loan.
self-dealing	Where a public official has an undisclosed personal financial interest in an entity which does business with the government. The public official uses their position to influence decisions and outcomes involving their financial interest for personal gain.
stichting	A foundation formed under Dutch legislation which is 'a separate entity' distinguished from its founders or directors. Stichtings are designed to act as charitable foundations, to accept assets and disperse funds to persons on the basis of their needs rather than their relationship with the provider of the asset. There is nothing that prevents stichtings from being used contrary to this purpose.
structuring	A money laundering technique which involves the deliberate division of a large amount of cash into a number of smaller deposits to evade threshold reporting requirements. Under section 142 of the AML/CTF Act structuring is punishable by up to five years imprisonment and/or 300 penalty units. Structuring can also involve the layering of funds for international funds transfers in an effort to avoid the transfers attracting undue scrutiny from authorities.
third parties	To avoid direct involvement in the money laundering process, criminals may use 'third parties' to undertake certain high-risk transactions that might expose the criminals to law enforcement or regulatory bodies.
trade-based money laundering (TBML)	This methodology involves the use of trade to legitimise, conceal, transfer and convert the instruments or the proceeds of crime into less conspicuous assets, commodities or services. In turn these goods, services, or their value are transferred worldwide to evade financial transparency laws and regulations. In practice, this can be achieved through the misrepresentation of the price, quantity or quality of imports or exports. Trade-based money laundering has continued to evolve, and common methods include: • over and under-invoicing of goods and services – misrepresentation of the price of the goods and/or services in order to transfer additional value between the importer and exporter • over and under-shipment of goods and services – overstating or understating the quantity of goods being shipped or services provided. In some cases, no goods are shipped • multiple invoicing of goods and services – issuing more than one invoice for the same trade transaction • falsely describing goods and services – misrepresenting the quality or type of goods and services.

Abbreviations

ADIs – authorised deposit-taking institutions

AFSL – Australian Financial Services Licence

AML/CTF – anti-money laundering and counter-terrorism financing

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

ASX – Australian Stock Exchange

ATM – automatic teller machine

ATO – Australian Taxation Office

AUD – Australian dollar

AUSTRAC – Australian Transaction Reports and Analysis Centre

FATF – the Financial Action Task Force

FIU – financial intelligence unit

FTR Act – *Financial Transaction Reports Act 1988*

GST – Goods and Services Tax

HGH – human growth hormones

IFTI – international funds transfer instruction

LPO – Licensed Post Office

MLA 2011 – *Money laundering in Australia 2011*

PEP – politically exposed person

RTGS – real-time gross settlement payment

SCTR – significant cash transaction report

SMR – suspicious matter report

SUSTR – suspect transaction report

TTR – threshold transaction report

USD – United States dollar