Australian Government
Australian Transaction Reports and Analysis Centre

AUSTRAC typologies and case studies report 2012

ISSN 1838-0026

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

Australian Government

Australian Transaction Reports and Analysis Centre

AUSTRAC typologies and case studies report 2012

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 sellers, 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 supervises 'cash dealers', as defined in the FTR Act.

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 2012* is one example of such guidance, and the case studies within this report highlight the value of industry's reporting of financial transactions and suspicious matters to AUSTRAC.

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.

A number of case studies within this report 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 by detailing successes achieved through AUSTRAC and revenue and law enforcement agencies working together and sharing information about criminal activities.

Money laundering: the Australian context

In 2011 AUSTRAC conducted a major intelligence assessment of the current money laundering environment in Australia. Drawing on classified operational intelligence from AUSTRAC's partner agencies and other sources, the *National threat assessment on money laundering 2011* (NTA 2011) report assembled a consolidated picture of current levels of money laundering activity, vulnerabilities and emerging threats. Overall, NTA 2011 confirmed the view formed in law enforcement strategic assessments that money laundering is one of the critical organised crime risks to the Australian community. Commonwealth, state and territory law enforcement, intelligence, revenue, regulatory and policy making bodies are using the NTA 2011 to inform their response to organised crime.

Money laundering in Australia 2011 (MLA 2011), a public report derived from the classified NTA 2011 (available at www.austrac.gov.au/money_laundering_in_australia_2011), complements the *AUSTRAC typologies and case studies report 2012*. It provides a contextual overview of the Australian money laundering environment, allowing a broader understanding of the methodologies and individual case studies detailed in this report.

The MLA 2011 report identified a number of key characteristics of money laundering in Australia, three of which feature in some of the case studies within this report:

- **Intermingling (or co-mingling) legitimate and illicit financial activity.** This process of reinvesting criminal proceeds and providing a cover for criminal enterprise (for example, through cash-intensive businesses and front companies) is a well-established money laundering methodology.
- **Engaging specialist money laundering syndicates.** Specialist syndicates, based in Australia and overseas, are providing specific money laundering services to domestic and international crime groups operating in Australia.
- **The 'internationalisation' of the Australian organised crime environment.** There is almost always an international component to the money laundering cycle for major crime groups operating in Australia.

Key money laundering channels

The MLA 2011 report identified the banking system, money transfer and alternative remittance services, the gaming sector and high-value goods as major money laundering channels. The significance of these channels to launder illicit funds is highlighted in this 2012 report, with a high proportion of case studies demonstrating their use.

A considerable amount of money laundering activity begins or makes its way through the banking system at some stage of the money laundering cycle. For criminals, the size of the sector and utility of general banking services to hold and move funds may outweigh the risks of detection.

The remittance sector is attractive to money laundering abuse as some remittance providers operate outside the formal banking system and can provide a cheap, quick and reliable method of sending funds internationally. There is also a perception among some criminals that remittance channels provide a reduced risk of detection.

A number of less-visible money laundering channels identified in the MLA 2011 report include professional advisers, legal entity structures, cash intensive businesses, electronic payment systems, cross-border movement of cash and bearer negotiable instruments, international trade, and investment vehicles. Case studies involving these channels or entities also appear in this report.

The financial intelligence available about the use of these less-visible money laundering channels is greatly enhanced by information reported in suspicious matter reports submitted to AUSTRAC. Many of the less-visible channels are not directly covered by AML/CTF regulation, but other reporting entities may be in a unique position to identify unusual or suspect behaviour which can provide important leads for tracking illicit financial activity.

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.

Reporting entities must submit a range of reports to AUSTRAC. These include reports of threshold transactions (TTRs) involving cash transaction of AUD10,000 or more, reports of international funds transfer instructions (IFTIs), and suspicious matter reports (SMRs) detailing financial activity they consider suspicious. AUSTRAC assesses and disseminates relevant SMRs to law enforcement and other agencies for their action.

AUSTRAC assists reporting entities to detect and deter money laundering by increasing their understanding of the ML/TF vulnerabilities for their industry and the designated services they provide. AUSTRAC participates in industry presentations and forums, and publishes information on the AUSTRAC website. 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. In many cases, suspicious matter reports have been the main trigger for an investigation. Transaction reporting provides key intelligence to support law enforcement agency investigations, including identifying new relationships, funds flows 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, protect both themselves and their customers from criminal activity and improve the quality of their reporting to AUSTRAC.

Information sources

The information contained 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 also acknowledges its use of information provided by a number of partner agencies, particularly the Australian Federal Police (AFP), Australian Crime Commission (ACC) and Department of Human Services (DHS), to complement research undertaken by AUSTRAC analysts into money laundering and terrorism financing risks and methodologies.

In their current sanitised form, the case studies presented in this report have been approved by our partner agencies for external use. AUSTRAC is unable to provide further information on individual cases.

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 or suspicious matter reports submitted by reporting 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 designated services used.
- **Indicators** – the customer behaviours or activities which could indicate the possibility of money laundering or terrorism financing activity. A consolidated list of major indicators identified in this report can be found in Appendix A.

Typologies

1

Established typologies

Potential vulnerabilities

Typologies

As outlined in AUSTRAC's *Money laundering in Australia 2011* report, money laundering is a critical risk to Australia. It is the common denominator of almost all serious and organised crime and continues to pose a threat to the integrity of Australia's business and financial systems. Money laundering exploits vulnerabilities in products and services in an attempt to conceal the proceeds of illicit activities and to commit financial and other serious crimes. Money laundering is also intrinsic to serious tax crimes and a threat to revenue.

Advances in technology and increased globalisation, combined with the diversification and transnational nature of organised crime, continue to influence current and emerging threats to the Australia's financial system.

The Typologies chapter of this report comprises two sections: 'Established typologies' and 'Potential vulnerabilities'.

The 'Established typologies' section examines two typologies used to enable and commit transnational crimes and tax evasion which are currently of particular interest to law enforcement, namely, the use of cheques to evade tax and the use of third-party cash couriers to undertake money laundering.

The 'Potential vulnerabilities' section examines a number of channels vulnerable to money laundering and terrorism financing, including digital currencies and virtual worlds, voucher payment systems, and offshore online money remitters. Although limited evidence exists to date of criminal misuse of these channels in Australia, overseas cases illustrate some of the ways in which they can be exploited. The growth in cybercrime in Australia suggests the vulnerabilities these channels present may be exploited in the future for financial crime and money laundering.

A number of the money laundering channels examined in this section of the report fall outside the direct regulatory controls of Australia's AML/CTF regime. Having said this, at some point some of the illicit funds which pass through these channels can be expected to be used in a manner which is caught under the AML/CTF Act; for example, bank transactions or gaming activities. The methods and vulnerabilities outlined in this report are intended to inform reporting entities about the various techniques which criminals can employ. This information is provided to help those entities to 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.

Established typologies

Cheques

The use of cheques is an established method of money laundering and taxation evasion. Cheques are used to pay false invoices and fraudulently inflate business expenses for the purpose of evading tax obligations. Cheque deposits are then cashed out and the funds returned to the originator to complete this method of tax evasion.

Money laundering vulnerabilities

Cheques present a number of vulnerabilities:

- **Cheques are vulnerable to being used for fraud** – they may be forged, altered, duplicated, counterfeited or stolen
- **Cheques may be used to allow criminals to deposit funds anonymously** – criminals may deposit cheques into third-party accounts to conceal the source of the funds, the link to criminal entities and any subsequent use of the funds.

Money laundering typology

Law enforcement investigations continue to identify the use of cheques as a means to undertake taxation fraud and money laundering. A common pattern observed by law enforcement is as follows:

- The first company makes out a cheque to another company for fictitious (or inflated) business expenses.
- In return, a fraudulent tax invoice is issued by the second company in an attempt to legitimise the cheque deposit made by the first company.
- The second company draws upon the cheque, withdrawing the funds as cash (sometimes in structured amounts) and returning the funds, minus a handling fee, to either the first company to pay cash wages to its employees or that company's directors to fund their lifestyles–thereby avoiding various tax obligations.
- The cheque deposits and cash withdrawals are often conducted on the same day via multiple bank branches.

AUSTRAC and law enforcement agencies recognise that this typology may also provide a means to launder the proceeds of crime. Criminals seeking to evade tax or launder funds may write cheques for false or inflated business costs which can then be drawn upon and the funds returned in cash to the originating company or writer of the cheque, minus a small handling fee. Use of business cheques gives a veneer of legitimacy to the transaction and enables illicit funds to be co-mingled with genuine business income to cover the money trail. When used in this fashion the typology operates to both launder the illicit cash and conceal the identity of the underlying criminals.

Reporting obligations

The provision of cheques and chequebook services are a designated service under the AML/CTF Act. Reporting entities which offer these services are required to report specific cheque transactions (that is, issuing of bank cheques, cashing of cheques, issuing of travellers cheques) to AUSTRAC when the cheques are purchased wholly or partly with AUD10,000 or more cash. Regardless of their value, cheque deposits are not captured under the AML/CTF Act, unless the transaction is the subject of a suspicious matter report (SMR) or the cheque deposit occurs in conjunction with a cash transaction of AUD10,000 or more.

Indicators for industry

The following indicators highlight potentially suspicious customer behaviour involved in the use of cheques. In isolation, individual indicators do not necessarily signify money laundering and/or tax evasion. However, the appearance of multiple indicators may be indicative of illicit activity:

- Cheque deposits into business accounts followed by immediate cash withdrawals at different branches (regardless of whether the withdrawals are over or under the cash reporting threshold).
- Newly registered businesses establishing accounts which experience minimal day-to-day business activity, but instead see large numbers of large cheque deposits and/or cash withdrawals, including ATM deposits, quick cash and night deposits services.
- Business accounts which operate for only 1–2 years before a new account is opened and operated under the name of another business, in circumstances where both the new and old business are owned by the same parties and undertake the same commercial activity.

Case study 10 is an example of a law enforcement investigation into the use of cheques to launder illicit funds and evade tax.

Third-party cash couriers – a variation of the cuckoo smurfing typology

Criminal syndicates have been observed using third-party cash couriers to undertake money laundering transactions. Syndicates are known to have recruited cash couriers to physically transport cash into or out of Australia.[1] The couriers may be directly connected to the original criminal offence and resulting proceeds of the crime, or recruited specifically for the task of moving the money offshore without having any connection to the underlying crime or criminals.

The third parties are recruited from overseas to travel to Australia, often to courier significant amounts of illicit cash either into Australia or alternatively to deposit funds once in Australia for subsequent transfer to foreign countries. This activity of recruiting overseas third parties is a variation on an established money laundering model and shares similarities with both an informal remittance arrangement, and a money laundering typology known as 'cuckoo smurfing'.[2]

Money laundering vulnerabilities

There are various methods used by third-party cash couriers in an attempt to avoid or reduce the risk of detection:

- **Structuring of deposits to avoid a paper trail** – deliberately structuring cash deposits to fall below the AUD10,000 cash reporting threshold, often at different branches or banks, to avoid triggering the submission of a TTR to AUSTRAC
- **Using branches that commonly receive large and regular cash deposits** – using busy bank branches handling large cash volumes to make deposits, so that the deposits are less likely to attract attention
- **Use of third-party accounts** – using the accounts of third parties who may have wittingly or unwittingly provided access to their account to accept cash deposits which represent the proceeds of crime
- **Smurfing/scattering illicit funds** – splitting large cash amounts between multiple couriers and/or accounts to reduce the chance of the entire proceeds of crime being detected or seized.

---

[1] See Glossary for definition of 'cash couriers'.

[2] See Glossary for definition of 'cuckoo smurfing'. For further information about cuckoo smurfing, refer to the *AUSTRAC typologies and case studies report 2008.*

Money laundering typology

The use of third-party cash couriers by a criminal syndicate is often typified by the following:

- A cash courier is recruited in their home country and offered a monthly fee to act as a courier in Australia.
- The cash courier is provided with one or more mobile phones, which may be shared among couriers, to allow contact with the money laundering syndicate to coordinate handling of the cash.
- Once the couriers arrive in Australia, individuals who are linked to one or more criminal syndicates hand them the funds for depositing, along with instructions on where to deposit the cash.
- Cash couriers who have been prepared in this manner often attend bank branches with a slip of paper, or a series of slips, containing names and bank account details. The couriers may also have prepared or been provided with a 'cover story' to give the impression that they are conducting a legitimate business in Australia.
- The syndicates may use multiple cash couriers to ensure consistent patterns of account deposits.
- The funds are often deposited into a variety of accounts, all of which are linked to the criminal syndicate, and shortly thereafter transferred overseas to pay for imports of illicit commodities or to 'park' illicit income overseas.

Recently enhanced reporting obligations

October 2011 amendments to the AML/CTF Rules introduced new obligations on threshold transaction reporting which require reporting entities to report the identification details of third parties involved in cash deposits of AUD10,000 or more. This requirement applies even if the third party is not a customer of the reporting entity.[3]

The third-party TTR reporting obligation provides valuable intelligence to help AUSTRAC identify patterns of potentially illicit transactions involving third-party deposits. This information includes: full name of the individual conducting transaction; date of birth; residential and postal addresses; phone number; occupation; how the identity of the individual was verified; type of authorisation used; and the third-party's relationship to the customer.

[3] <http://www.austrac.gov.au/ttr_form_changeover.html>

Indicators for industry

Reporting entities should remain alert to patterns of customer behaviour or transactional activity which may indicate the use of third-party couriers to launder illicit funds. In isolation, individual indicators do not necessarily signify this typology. However, the appearance of multiple indicators may be indicative of third-party courier activity:

- Numerous third-party cash couriers may make regular trips to bank branches to deposit significant amounts of cash into a range of third-party business and personal accounts.
- The cash deposits may occur at one particular bank branch, or at a series of bank branches.
- Where cash deposits are made at a series of different bank branches, the branches are often close to each other or located near major transport routes.
- The individuals making deposits may refer to their activity of making deposits in multiple locations and/or branches.
- When making cash deposits cash couriers may carry large amounts of cash, often in bundles of similar denominations, particularly high-value notes.
- Cash deposited into accounts held in the name of a business may constitute transaction activity which is inconsistent with the stated nature of that business.
- Soon after the cash is deposited, internet banking may be used to quickly move the funds to overseas personal accounts (which are often controlled by individuals linked to the criminal syndicate).

Potential vulnerabilities

In recent years there has been a significant increase globally in the use of electronic payment systems and new payment methods (NPMs) to transfer funds and enable payments to be made. AML/CTF authorities worldwide recognise that certain features of these new systems, such as the anonymity they may afford users and the reduction in face-to-face business relationships and transactions, offer fresh opportunities for exploitation by criminals.

AUSTRAC has conducted research on a number of electronic payment systems and NPMs to assess their presence in Australia and potential money laundering/terrorism financing (ML/TF) risk. While some low-value transactions to purchase illicit goods and services using these systems have been observed by Australian law enforcement agencies, the extent of their use by organised crime groups is unknown. As electronic payment systems and NPMs evolve to handle high value amounts and broaden in global reach, the potential for organised crime to misuse these systems may increase on the basis of growth in cyber crime and the displacement effect of stronger AML/CTF measures on criminal misuse of established financial services.

The appeal of electronic payment systems and NPMs is likely to depend on the predicate offence and the way proceeds of crime are derived. For example, cyber or online crimes are likely to generate proceeds electronically, compared to the largely cash-basis of illicit drug crime. Where criminal proceeds are generated in an online environment, laundering the funds using electronic payment systems and NPMs may appear relatively easier to criminals and with less risk of detection than using other channels.

Digital currencies and virtual worlds

'Digital currencies' and so-called 'virtual worlds' offer opportunities for criminals to launder money due to their global reach, lack of face-to-face transactions and the convenience of using electronic commerce.

While the nature and extent of money laundering through digital currencies and virtual worlds are unknown, it is important to recognise their potential for criminal exploitation, particularly in response to tighter regulation of established or traditional financial channels.

Overview of digital currencies

The evolution of digital currencies has led to the development of internet-based, electronic means of transferring 'real-world' value. In contrast to the traditional physical currencies issued by national governments, digital currencies (such as Bitcoins, SolidCoins and Linden dollars) are issued by commercial enterprises. They are not issued by or under the authority of a government body. Nor are they backed by traditional currencies, precious metals or other physical commodities.

Digital currencies potentially allow individuals and entities to conduct quick and complex international funds transfers outside the regulatory requirements of the traditional financial system. Digital currencies that are not backed, either directly or indirectly, by precious metal or bullion are not regulated by the AML/CTF Act.[4]

Some digital currencies can be purchased with traditional currencies through online digital currency exchanges (DCEs) such as Mt.Gox, VirWoX and LindeX.[5] Bitcoins can be exchanged for stored value cards, while other digital currencies can be exchanged for gold, silver and online goods and services.

Figure 1, below, depicts the typical process of purchasing digital currencies through an online DCE.

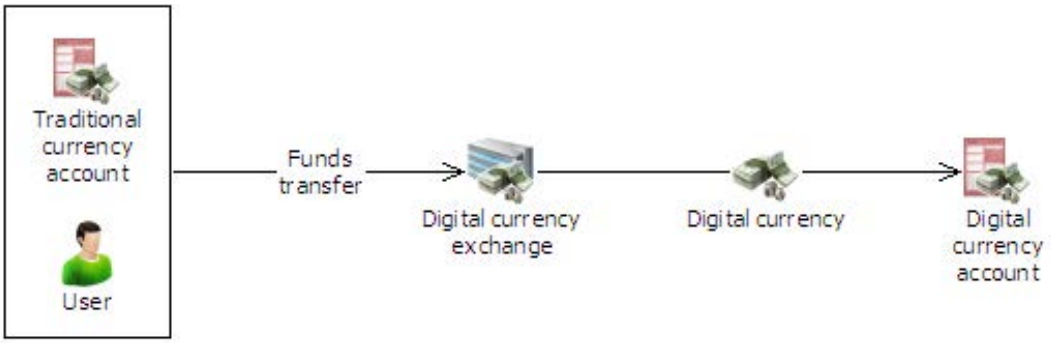


Figure 1: Purchasing digital currency through an online DCE

The anonymous nature of digital currencies may appeal to criminal groups and individuals who seek to use digital currencies as an instrument of crime to pay for illegal goods and services and obscure the source of illicit funds or evade tax. Criminal groups and individuals may increasingly use digital currencies, as opposed to online trading of real currency, due to the anonymity some digital currencies provide. These digital currencies present challenges for government agencies in following the money trail.

On the other hand, there are some disadvantages for criminals using digital currencies for illicit purposes. In general, digital currencies at this time are not widely accepted as payment for goods and services. This limits the avenues through which digital currency can be used to convert, move and launder illicit funds. The limited size of digital currency markets, in turn, reduces the extent to which large amounts of illicit value can be moved. In contrast, traditional financial channels (such as banks and remittance services) interact with a wide range of economic sectors through which illicit funds in large volume can be moved, co-mingled and concealed. The overall utility of digital currencies for criminals at this point may currently be limited to niche crimes in the cyber environment and individual or smaller scale illicit activity.

[4] See the definition of 'e-currency' in section 5 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*

[5] Mt Gox. and VirWoX have their own websites, while LindeX (Linden Dollar Exchange) is accessed via the virtual world of *Second Life*

Overview of virtual worlds

Virtual worlds (also known as gaming platforms, 3D environments and massive multiplayer online games) are internet-based simulated 'worlds' with their own virtual 'economy'. Examples include *Second Life* and *World of Warcraft*.

The economy of a virtual world is generally based upon a digital currency which can be purchased and/or converted into real currency.[6] Users interact with each other in a virtual environment, purchasing virtual property, trade goods, services and currency.

By definition, virtual worlds operate in a borderless environment. They provide potential for criminals to launder money with anonymity. For example, the potential exists for virtual world users to purchase 'virtual real estate' using illegally obtained money in an attempt to legitimise the transfer of funds to a third party. The proceeds of these transactions can subsequently be converted into real currencies or transferred offshore or to third-party accounts.

Figure 2, below, illustrates how a virtual world could potentially be used to launder the proceeds of crime.

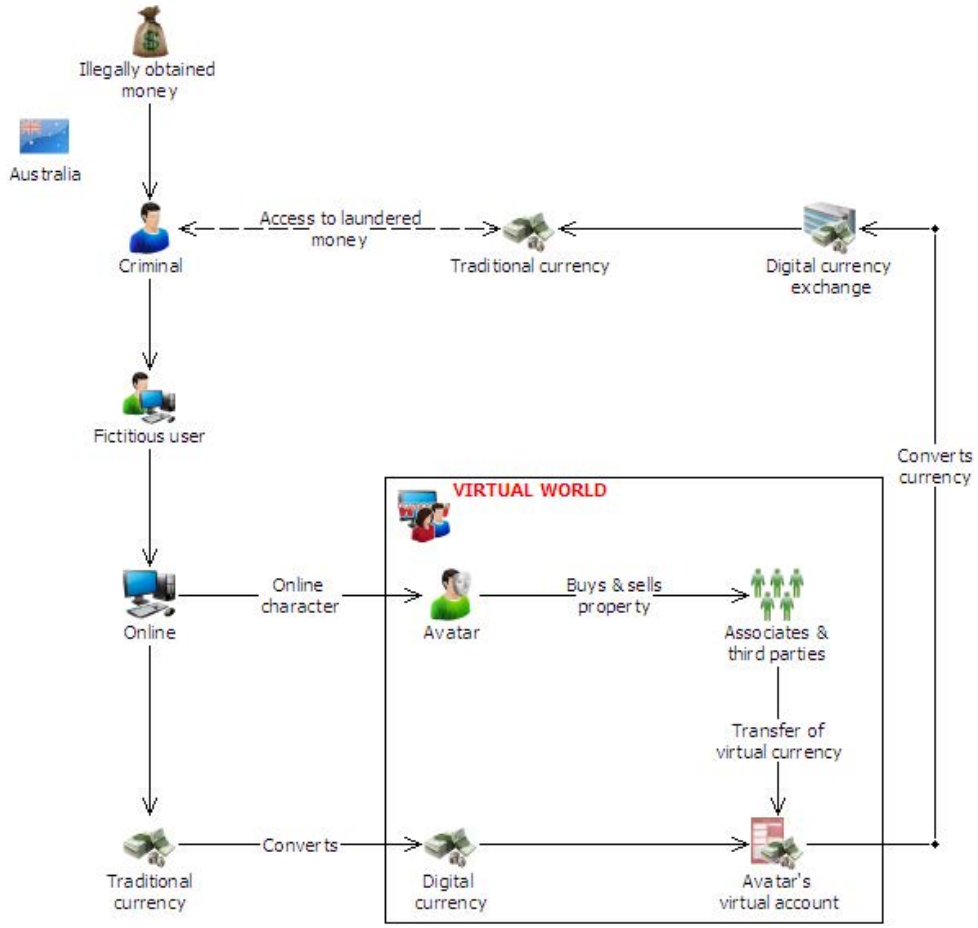


Figure 2: Money laundering using virtual worlds – indicative only

[6] Financial Action Task Force (FATF), *Money Laundering using New Payment Methods*, FATF Paris, October 2010, p.116.

Money laundering vulnerabilities

The vulnerabilities associated with digital currencies and virtual worlds include:

- Digital currencies and virtual worlds are generally not captured by anti-money laundering and counter-terrorism financing (AML/CTF) legislation around the world. Because there is limited or no regulation of digital currency transactions, authorities have difficulty monitoring criminal activity which exploits digital currencies.
- Online DCEs provide the opportunity for criminals to exchange digital currencies for other digital currencies (for example, exchanging Bitcoins for Linden dollars), before converting them into real world currency. This provides additional 'layering' in the money laundering cycle.
- Criminals can use their illegally obtained physical currency to purchase the digital currency of a virtual world. Depending on the virtual world platform or online DCE, digital currency can be purchased using a debit card, credit card, internet payment service provider or, in some instances, using an online voucher payment.
- The proceeds of some transactions can be converted into traditional or real currency by linking a virtual account to a debit card or through DCEs. These channels would allow individuals to trade digital currencies and receive payment via a debit card, credit card or internet payment service provider.

International examples

International cases illustrate the potential vulnerability for digital currencies and virtual worlds to be misused by criminals.

Case 1: Potential misuse of virtual worlds and digital currency exchanges[7]

An international investigation by a foreign law enforcement agency and FIU identified an international internet payment service provider who was suspected of laundering illicit proceeds derived from fraudulent schemes.

The complex money laundering investigation revealed multiple DCEs, precious metals providers and stored value card providers implicated in the scheme, either unwittingly or otherwise.

The potential of virtual worlds to launder funds was also highlighted. One of the stored value card providers allowed its product to be used in a virtual world – where it could be used to fund a virtual world account and exchanged through an online DCE or ATM for real world currency. The ability to use stored value cards in virtual worlds, in conjunction with virtual currency, DCEs or ATMs, could provide criminals with an additional channel to conceal and launder illicit funds.

[7] Financial Action Task Force (FATF), *Money Laundering using New Payment Methods*, FATF, Paris, Case 30, p. 44, October 2010.

Voucher system products

Voucher system products have already been used by criminals overseas for financial crime and money laundering. The FATF has identified cases which demonstrate their potential for misuse.[8]

FATF defines cash vouchers as 'a prepaid product which can be purchased at several retailers and used for person-to-business (P2B) or person-to-person (P2P) transactions on the Internet'.[9] Voucher system products may also be considered as a type of 'cash voucher'. They provide a prepaid online payment facility for individuals to purchase goods and services from participating online retailers and gaming websites. The voucher system products discussed here are issued for low values of between AUD5 and AUD500.

Store gift cards and similar types of coupon products do not fall within the scope of online voucher systems for the purpose of this overview. These products are used in-store and in-person, without a connection to an online environment.

How voucher system products work

Vouchers can be obtained, transferred and exchanged in a number of ways, including in-store and online.

Vouchers can be purchased with cash in-store from participating outlets. They come with a printed voucher containing a unique code that can be used to pay for goods or services online. There are generally no customer identification requirements for the in-store purchase of vouchers.

Vouchers can also be purchased online, whether directly from the product provider, from an authorised reseller who is approved by the product provider to resell vouchers to customers, a third-party seller, online exchange or digital currency exchange (DCEs). Online purchasing of vouchers occurs as follows:

- An individual registers with a voucher system product via the website of the provider or an authorised reseller.
- The individual selects the value of the voucher they wish to purchase and pays for the voucher via online bank transfer, credit or debit card or through an online payment system.
- After payment is accepted, the unique voucher code is delivered to the individual online and can be redeemed to pay for goods and services at participating online outlets.

Customer identification requirements and procedures vary among voucher product providers.

[8] Financial Action Task Force (FATF), *Money Laundering using New Payment Methodologies*, October 2010, Case 8 p.38 and Case 10 p. 39.

[9] ibid. p. 112.

Figure 3, below, depicts the typical process for purchasing vouchers in-store or online.

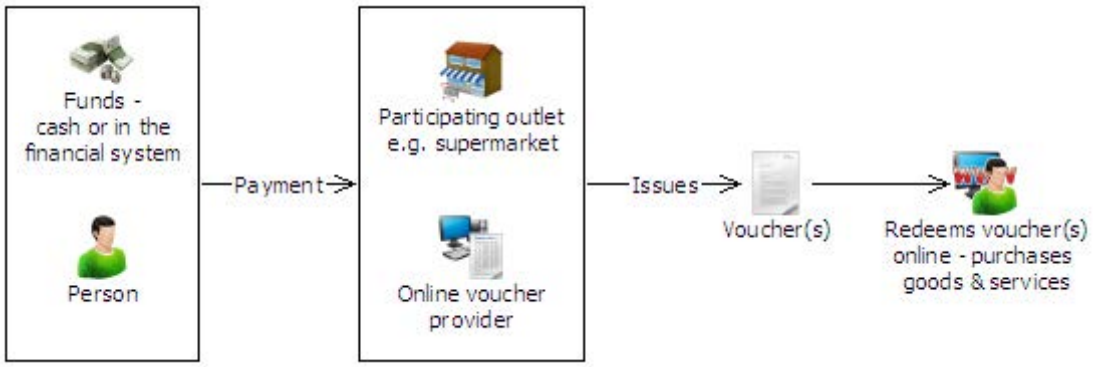


Figure 3: Purchasing voucher products in-store or online

Vouchers and AML/CTF regulation

The characteristics and monetary value associated with voucher products will determine whether they are regulated under the AML/CTF Act.

The voucher system products described in this overview are generally issued for low-value amounts of between AUD5 to AUD500. Due to their low value, they are unlikely to be classified as designated services and are generally not regulated under the AML/CTF Act.

However, voucher products which possess some of the attributes of a 'stored value card' are likely to be captured by the definition in section 5 of the AML/CTF Act. A voucher may be classified as a 'designated service' under items 21 or 22 of the AML/CTF Act when:

- it is issued or can be increased in value for amounts greater than or equal to AUD1,000 and
- the whole or a part of the monetary value stored in connection with the voucher may be withdrawn in cash.

Alternatively, a voucher may be classified as a designated service under items 23 or 24 of the AML/CTF Act when:

- it is issued or can be increased in value for amounts greater than or equal to AUD5,000 and
- no part of the monetary value stored in connection with the voucher may be withdrawn in cash.

Vulnerabilities

Money laundering vulnerabilities associated with voucher system products include:

- Vouchers can be purchased with cash, which potentially allows criminals to use or exchange illegally obtained funds anonymously. The absence of identification requirements provides a layer of anonymity for criminals to exploit.
- Vouchers are easily transferrable, meaning they can be transferred to third parties without record of the transaction, therefore avoiding monitoring by authorities.
- Third-party resellers, DCEs and other online exchanges provide criminals with the opportunity to exchange vouchers for traditional currencies, digital currencies or other online payment products. This provides an additional opportunity to 'layer' illegally obtained funds.
- Some vouchers allow individuals to shop and play online without having to divulge bank account and credit card details. The voucher product providers receive payments via direct cash deposits or domestic transfers into their bank accounts. Unless they involve AUD10,000 or more, the cash deposits are not required to be reported to AUSTRAC as threshold transactions (although it is possible that a reporting entity may decide to submit a suspicious matter report for a cash deposit below the AUD10,000 reportable threshold, depending on the circumstances).
- Vouchers may be used to transfer illicit funds or value offshore to accounts in jurisdictions with weak AML/CTF regimes, facilitating the layering and/or integration of the funds into the legitimate economy.
- Where vouchers can be exchanged in virtual world environments, criminals can use illegally obtained funds to purchase the virtual world currency, potentially enabling them to deposit illegally obtained funds in 'virtual accounts'. Selected virtual worlds provide an option for transferring virtual currency to real world bank accounts, potentially enabling criminals to integrate illegally obtained funds.

Money laundering methods

The following is an example of how a voucher product system could potentially be used to launder money:

A criminal (or a third-party 'mule' operating on their behalf) attends multiple participating outlets where the participating logo is displayed (for example newsagents, convenience stores and petrol stations) on the same or successive days and uses illicit cash to purchase a number of vouchers.

- The criminals may choose to purchase vouchers at the highest possible value, to maximise the amount of illicit cash they can launder. Alternatively, a network of mules could be used to purchase a large volume of lower-value vouchers.
- The criminal uses the vouchers to pay for goods or service online, online gambling, or exchanges the vouchers for traditional currency or other commodities.
- Alternatively, the criminal may send voucher numbers or scanned copies of vouchers by email to a third party who uses the voucher codes to purchase goods and services online or for online gambling.
- Several vouchers of smaller amounts could be purchased at multiple locations and then combined in value to purchase goods and services online.

- Online gambling can facilitate criminals opening several gaming accounts with false identification details. The vouchers may be used at online gambling sites to facilitate a high number of low-value transactions. The criminals gamble a portion of illicit funds through online gambling then withdraw the balance to give the funds the appearance of legitimate 'winnings'.
- Vouchers may be used as an alternative payment method for online gambling to bypass authorities in those countries where online gambling is illegal.

The methods described above may also allow vouchers to be exchanged for illicit commodities such as drugs. In this way, the vouchers allow for the exchange of 'value', while avoiding the use of money or financial instruments and thus circumventing financial regulation and possible detection.

Vouchers may be moved offshore via online exchange services or DCEs to assist criminals to layer illegally obtained funds or to assist individuals to evade tax.

Printed vouchers could be moved offshore in bulk via third parties or couriers for use overseas or, alternatively, vouchers (or voucher codes) could be sent from abroad to Australian-based criminals.

International case studies

Two cases from Germany highlight the way criminals can employ the use of vouchers to fraudulently obtain funds.

Case 1

In the first case, a criminal sent an extortion letter to a German company and demanded to be paid in EUR250,000 in cash vouchers issued by an internet payment services provider based in the United Kingdom. The payment services provider was able to work with law enforcement to catch the extortionist.[10]

Case 2

The second case concerned a financial agent who was involved in a phishing scam.[11] The financial agent accepted illicit funds extracted from bank accounts in Germany and transferred to his personal account. The financial agent withdrew the illicit funds in cash and kept a portion of the funds as commission. The agent used the remaining cash to purchase cash vouchers worth up to EUR500 each at petrol stations and newspaper kiosks. The purchases were anonymous and did not identify the agent as the buyer. The financial agent emailed the voucher number or a scanned copy of the voucher to the perpetrator of the scam. The perpetrator used the voucher codes on the internet at gambling websites and to pay for goods and services online. The use of cash vouchers obscured the flow of illicit funds. Law enforcement authorities were unable to trace the transactions to determine the final destination of the illicit funds.[12]

Conclusion

Given that the maximum value of voucher products is currently capped at relatively low amounts (AUD500 or below), the use of voucher system products at this stage is likely to be limited to low-value purchases and trades in medium volumes. For criminals, vouchers may be an alternative to established money laundering channels for types of crime involving low-value financial activity (for example, illicit internet pornography).

---

[10] Financial Action Task Force (FATF), *Money Laundering using New Payment Methodologies,* October 2010, Case 8 p.38.

[11] Refer to glossary for definition of 'phishing'.

[12] Financial Action Task Force (FATF), *Money Laundering using New Payment Methodologies*, October 2010, Case 10 p. 39.

Offshore online money remitters

AUSTRAC has identified growth in the use of offshore-based online money remitters in Australia. While based in foreign countries, these businesses can facilitate international funds transactions to or from customers in Australia.

Reporting obligations

The provision and use of offshore online remittance services in Australia are legal; however, these services fall outside AML/CTF regulation. Remittance businesses with no permanent establishment in Australia but which provide financial services to Australian customers are not subject to AML/CTF Act provisions and therefore have no obligation to report transactions or suspicious matters to AUSTRAC.

This typology focuses on offshore-based online money remitters, outlining how they operate and their vulnerabilities to criminal misuse. It does not examine established network or corporate remittance providers which have a permanent presence or geographic link to Australia, either through themselves or affiliates or franchises.

Money laundering vulnerabilities

For Australian authorities and reporting entities, different AML/CTF frameworks and transaction reporting regimes in different countries can provide opportunities for criminal networks to exploit online money remitters. Online remittance is particularly vulnerable to criminal misuse due to the potential lack of face-to-face contact between customers and remittance businesses. This lack of contact could permit the person instructing or undertaking the international funds transfer to remain unidentified, or it could mean that their identity remains unverified.

In general, the vulnerabilities associated with online remitters include:

- a lack of face-to-face contact between remitters and customers, which may:
  - make it more difficult for a remitter to perform enhanced customer due diligence
  - allow third parties to use existing online remittance accounts to anonymously transfer funds internationally
  - enable operation of accounts using false names and addresses
  - increase opportunities for identification theft/fraud.
- limited financial reporting obligations, which may:
  - obscure the details of the ordering and beneficiary customers involved in a transaction, including their location
  - hamper identification of suspicious behaviour.
- minimal 'paper trails' for the related domestic transfers that occur prior to and after an international transfer, which may:
  - limit the available information about the actual ordering and beneficiary customers
  - present difficulties for authorities attempting to trace all stages involved in an international funds transfer.

- criminal use of offshore online remittance to undertake low-value international funds transfers to:
  - » disguise the purpose of the transaction
  - » transfer illicit funds to offshore accounts in jurisdictions with weaker AML/CTF regimes
  - » enable layering and integration of proceeds of crime.

Operating model

A typical example of how an offshore online remittance business operates is as follows:

- A customer in Country A (Person A in Figure 4 on the following page) wishes to send funds to a friend in Australia (Person B) and engages an online remittance provider to facilitate the transfer.
- The online remitter (based in Country A) requires the customer to register online to provide their personal details. The online remittance business may also require a one-off, face-to-face meeting with the customer during the registration process. However, depending on the AML/CTF requirements in their home country, not all online remittance businesses will undertake this face-to-face stage of the registration process.
- The customer makes an online domestic funds transfer (equal to the amount they wish to send to Australia) into a bank account also located in Country A which is owned by the remitter.
- The remitter conducts the international funds transfer, and the funds appear in an Australian account owned by the remitter. The receiving institution (for example, a bank) where the online remitter's Australian account is held is obligated to report the transaction to AUSTRAC as an IFTI into Australia.
- At this stage the incoming IFTI is reported to AUSTRAC – the online money remitter business is recorded as both the 'ordering' and 'beneficiary' customer for the purposes of this transaction.
- The online remitter then conducts an online domestic transfer from their Australian account into the account of the intended Australian beneficiary (Person B).
- At no stage are the details of the ultimate ordering customer (Person A) or the ultimate beneficiary customer (Person B) reported to AUSTRAC.

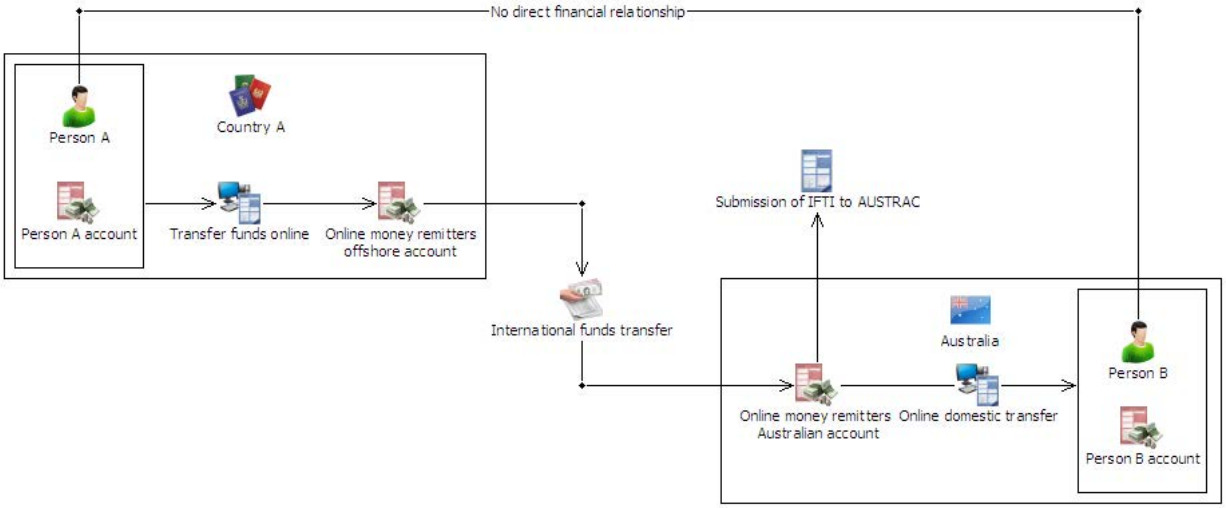


Figure 4 - Operation of a typical offshore online money remitter receiving incoming IFTIs

Money laundering indicators

The current limited visibility for authorities of transactions involving offshore online remitters, coupled with money laundering vulnerabilities of these systems, requires further development of indicators of suspicious activity. Until indicators of money laundering via online remitters can be better defined, the following activity may suggest closer scrutiny for institutions which hold accounts of, or transact, with online remittance businesses:

- transactions in which the 'ordering' and 'beneficiary' customer names are the same
- accounts of an Australian-based online remitter which are being used as a clearing account, receiving or sending bulk international transfers to self-named business accounts in Australia or abroad
- domestic transfers which are sent via internet banking to an ultimate beneficiary customer, soon after the receipt of the funds from offshore
- Australian-based accounts operated by offshore entities receiving regular deposits (whether direct cash deposit or domestic transfers) from Australian customers, followed by equivalent international transfers to offshore accounts operated by the same entity.

Case studies
Account and deposit-taking services

2

Case studies – Account and deposit-taking services

Case 1 – Suspects attempted to smuggle native reptiles hidden in stuffed toys

AUSTRAC information led to the arrest of two Hong Kong nationals based in Australia suspected of being involved in the illegal exportation of Australian native reptiles.

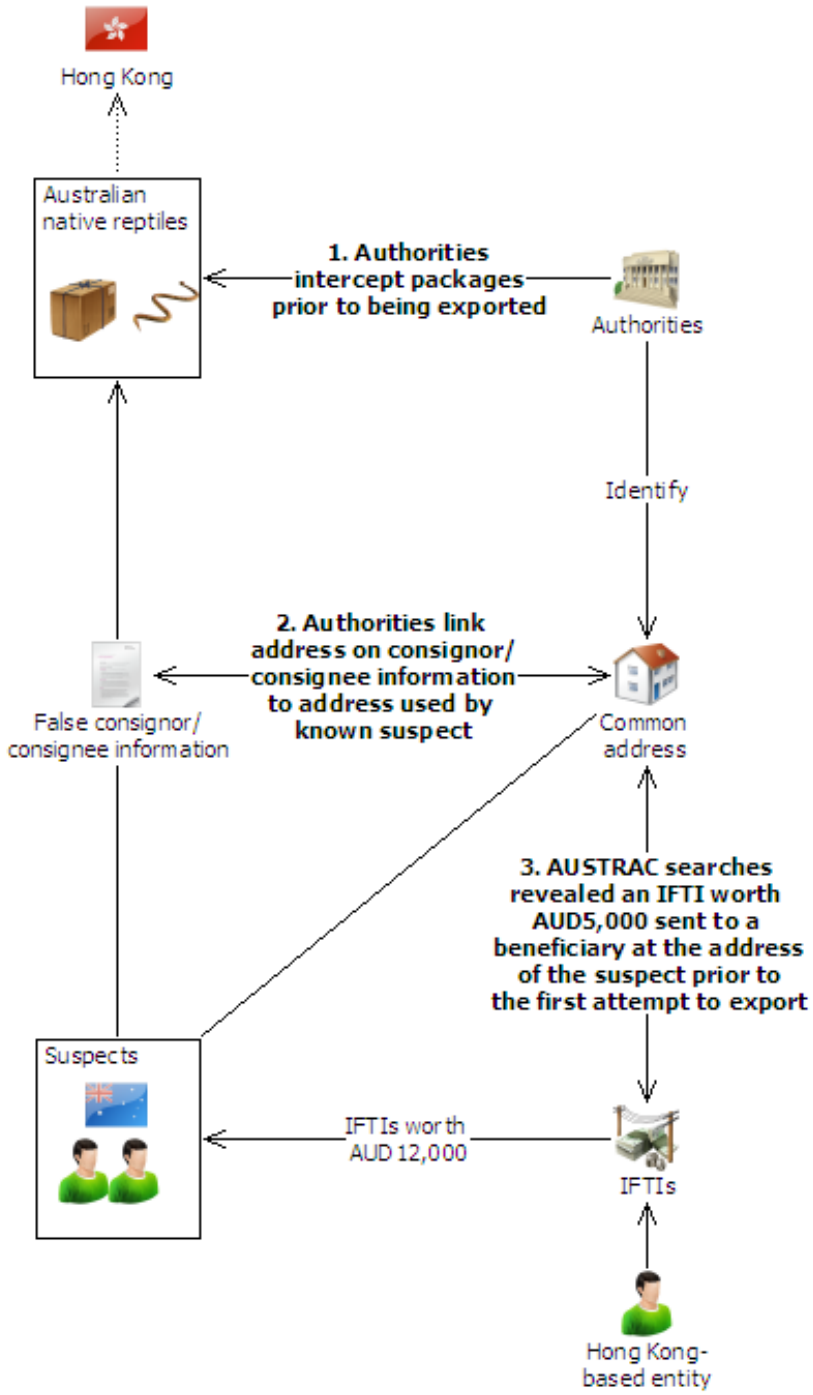
Authorities intercepted a parcel destined for Hong Kong which contained native Australian reptiles concealed in stuffed toys. The suspects used false consignor and consignee information in an attempt to evade detection by Customs authorities. AUSTRAC information revealed a link between the address listed on the parcel and an address associated with a person previously suspected of involvement in wildlife smuggling.

Searches of the AUSTRAC database revealed an incoming international funds transfer instruction (IFTI) report for AUD5,000 (which included the same address as the one on the intercepted parcel) that was sent to a person based in Australia. The funds were sent from Hong Kong to Australia a week before the attempted export.

Over a 12-week period a total of six packages in four consignments were intercepted by authorities. Further searches of AUSTRAC information identified that the Australian-based suspect was the beneficiary of incoming international fund transfers totalling more than AUD12,000 from the same Hong Kong-based entity. The incoming international funds transfers were made shortly before each attempt to export wildlife.

Authorities executed a search warrant on a residential property in Australia and seized various Australian native reptiles, soft toys, packaging and postage material. The Australian-based suspect and an associate were arrested for attempting to export Australian native reptiles. Both were convicted for offences under environmental protection law.

Offence	Reptile smuggling
Customer	Individual
Industry	Banking (ADIs)
Channel	Electronic
Report type	IFTI
Jurisdiction	International – Hong Kong
Designated service	Account and deposit-taking services
Indicators	Multiple low-value international funds transfers



Case 1 - Suspects attempted to smuggle native reptiles hidden in stuffed toys

Case 2 – Company evaded millions in cigarette tax through duty free fraud

AUSTRAC information assisted authorities with an investigation into a company suspected of a multi-million dollar duty free fraud. The investigation resulted in the company and its two directors being convicted of fraud-related charges.

The investigation revealed that, over a three-year period, a complex arrangement was set up where the directors of the company, which traded as a duty free store, sold large quantities of 'underbond' cigarettes (cigarettes on which excise duty had not been paid).[13] The directors sold the cigarettes and profited by avoiding paying the required customs and excise duty. In total, authorities believe that the suspects evaded more than AUD2.5 million tax.

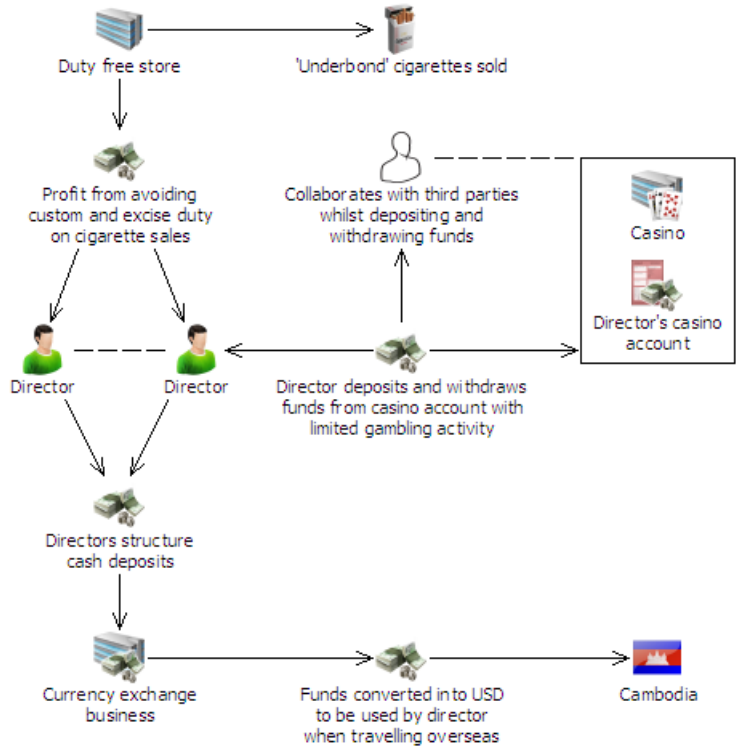
In accordance with AML/CTF reporting requirements, reporting entities submitted a range of financial transaction reports indicating suspicious activity by the company and its directors, involving currency exchange business and casinos. Authorities believe the suspects undertook a range of activities to launder and hide the substantial proceeds of the cigarette sales:

- One of the directors travelled regularly to Cambodia and would visit currency exchange businesses in Australia to convert funds to US dollars before each trip. When converting currency amounts worth more than AUD10,000, the two directors regularly refused to complete significant cash transaction reports (SCTRs), instead opting to structure the cash into smaller amounts to avoid the SCTR reporting requirement.
- This structuring activity led to a total of 44 suspect transaction reports (SUSTRs) being submitted about the two directors, with the majority coming from a currency exchange business. It was also reported that the suspects had asked reporting entities whether or not their transactions would be recorded and reported to the Australian Taxation Office (ATO), a further indication that they were involved in illegal activity and were concerned about attracting the attention of authorities.
- AUSTRAC also received SUSTRs from a casino highlighting one suspect's continued use of a casino account to deposit and withdraw funds, despite undertaking limited gambling activity. The reports indicated the suspect was a regular patron at the casino. While the suspect's gambling activity remained limited, the amounts gambled had increased substantially over an eight-year period. It was also reported that the suspect had collaborated with a number of third parties while depositing and withdrawing funds at the casino.
- In all, AUSTRAC information showed that the two directors and associates made cash deposits worth more than AUD20 million into their business banking account.

The company and its directors were convicted and ordered to repay the AUD2.5 million in tax they had evaded. In addition they were ordered to pay penalties of more than AUD600,000, as well as the Commonwealth's legal costs of AUD140,000. The convictions finalised a long-running and complex investigation.

---

[13] See the Australian Taxation Office website for more information: <www.ato.gov.au/businesses/content.aspx?doc=/content/49158.htm>, viewed 5 April 2012.



Case 2 – Company evaded millions in cigarette tax through duty free fraud

Offence	Structuring Tax evasion
Customer	Business Individual
Industry	Banking (ADIs) Currency exchange services Gambling services
Channel	Electronic Physical
Report type	SCTR SUSTR
Jurisdiction	Domestic International - Cambodia
Designated service	Account and deposit-taking services Gambling services
Indicators	Customer refuses to submit a significant cash transaction report (SCTR) or transaction threshold report (TTR) Customer shows unusual interest in/concern about the reporting of transactions to authorities Significant increase in amounts gambled Structuring of multiple cash deposits below AUD10,000 conducted on the same day to avoid reporting obligations. Third parties involved in depositing and withdrawing of funds at casino

Case 3 – Mining company accountant siphoned $1 million into offshore accounts

An Australian-based mining company initiated an internal investigation after it was suspected an employee had stolen more than AUD1.1 million over a three-year period.

The company identified the suspect through internal audit processes and the matter was referred to law enforcement authorities for further investigation.

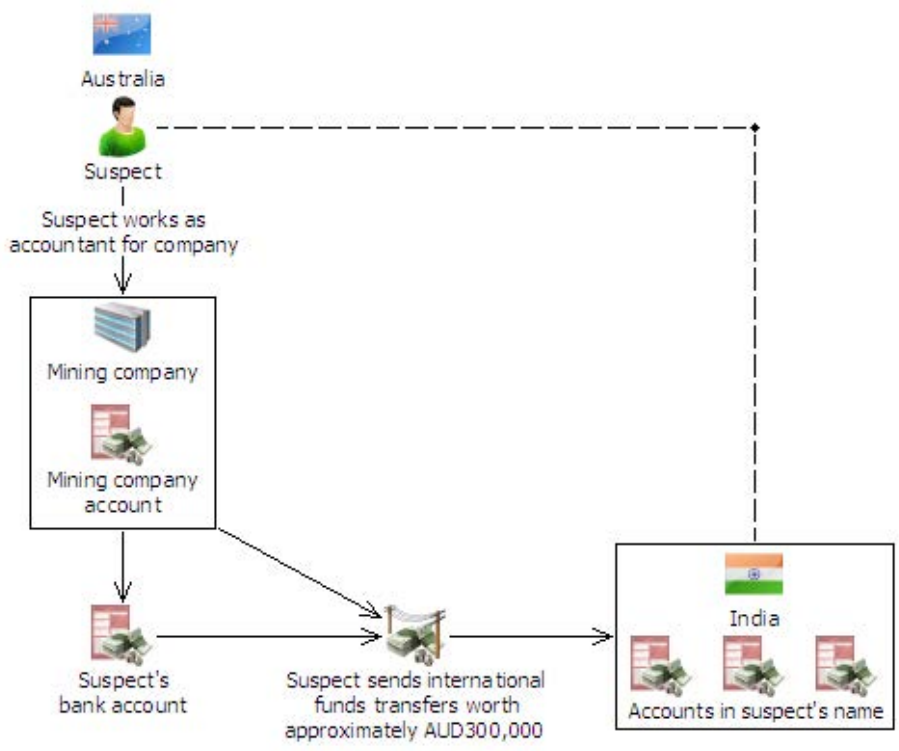
The law enforcement investigation revealed that the suspect, an accountant employed by the company, had abused his position of trust by systematically making a series of unauthorised international transfers over a three-year period. The transfers were made from a company account to a number of offshore accounts held in the suspect's name and a number of his family members' names.

A suspect transaction report (SUSTR) submitted by a bank suggested that an outgoing international funds transfer instruction (IFTI) of AUD27,500 from the suspect's personal account appeared to be sourced from company funds. The suspect was the beneficiary of the IFTI and bank staff noticed that four days prior to the IFTI, the exact amount of AUD27,500 was transferred into the suspect's account from a company account.

AUSTRAC analysis found a number of transaction reports linked to the suspect. These supported the allegation of theft and identified the significant extent of the financial activity undertaken by the suspect.

AUSTRAC information revealed that the suspect was the beneficiary of 17 outgoing IFTIs to India in amounts of between AUD2,400 and AUD33,400. Funds were sent from either the suspect's personal Australian-based bank account or from the company's account. In total, approximately AUD300,000 was transferred, all believed to be the proceeds of the theft.

Law enforcement officers contacted the suspect while he was overseas. The suspect surrendered to authorities on his return to Australia. The suspect was charged with 10 counts of stealing and sentenced to seven years imprisonment. After serving four years the suspect was deported from Australia.



Case 3 – Mining company accountant siphoned $1 million into offshore accounts

Offence	Theft
Customer	Individual
Industry	Banking (ADIs)
Channel	Electronic Physical
Report type	IFTI SUSTR
Jurisdiction	International – India
Designated service	Account and deposit-taking services
Indicators	Customer receiving multiple large-value domestic transfers into their personal account from a company account, followed by an outgoing international funds transfer equivalent in value to the domestic transfer International funds transfers from an individual's account to several offshore accounts held in the same name International funds transfers inconsistent with transaction history

Case 4 – Conned investors lost millions in investment Ponzi scheme

A law enforcement agency conducted an investigation into a suspect who operated a Ponzi scheme in which approximately 220 victims lost more than AUD15.5 million they believed had been invested legitimately.

Over a nine-year period the suspect maintained a facade of heading a successful investment business. As the director of a group of companies, the suspect claimed to operate a legitimate managed investment scheme, including self-managed superannuation funds (SMSFs). The suspect claimed to trade in global derivatives and equity markets, promising extraordinarily high returns to potential investors.

The scheme grew by word of mouth with friends, relatives and acquaintances of the suspect and victims investing in the scheme. Victims of the scheme were from Australia, South Africa and the United Kingdom. While some victims initially received money from their investment, the majority lost their investments, including family inheritances, retirement funds and savings.

AUSTRAC information contributed to the investigation by identifying bank accounts, international funds transfer instructions (IFTIs) and transactions made by victims. AUSTRAC information identified bank accounts in Vanuatu linked to the suspect. Some victims reported signing contracts and transferring money to a company based in Vanuatu. AUSTRAC information indicated that money transferred to Vanuatu was later transferred to Australia, predominantly for the benefit of the suspect.

All IFTIs linked to the scheme were made through banks and some incoming IFTIs represented transfers from overseas victims. AUSTRAC information showed that over a four-year period:

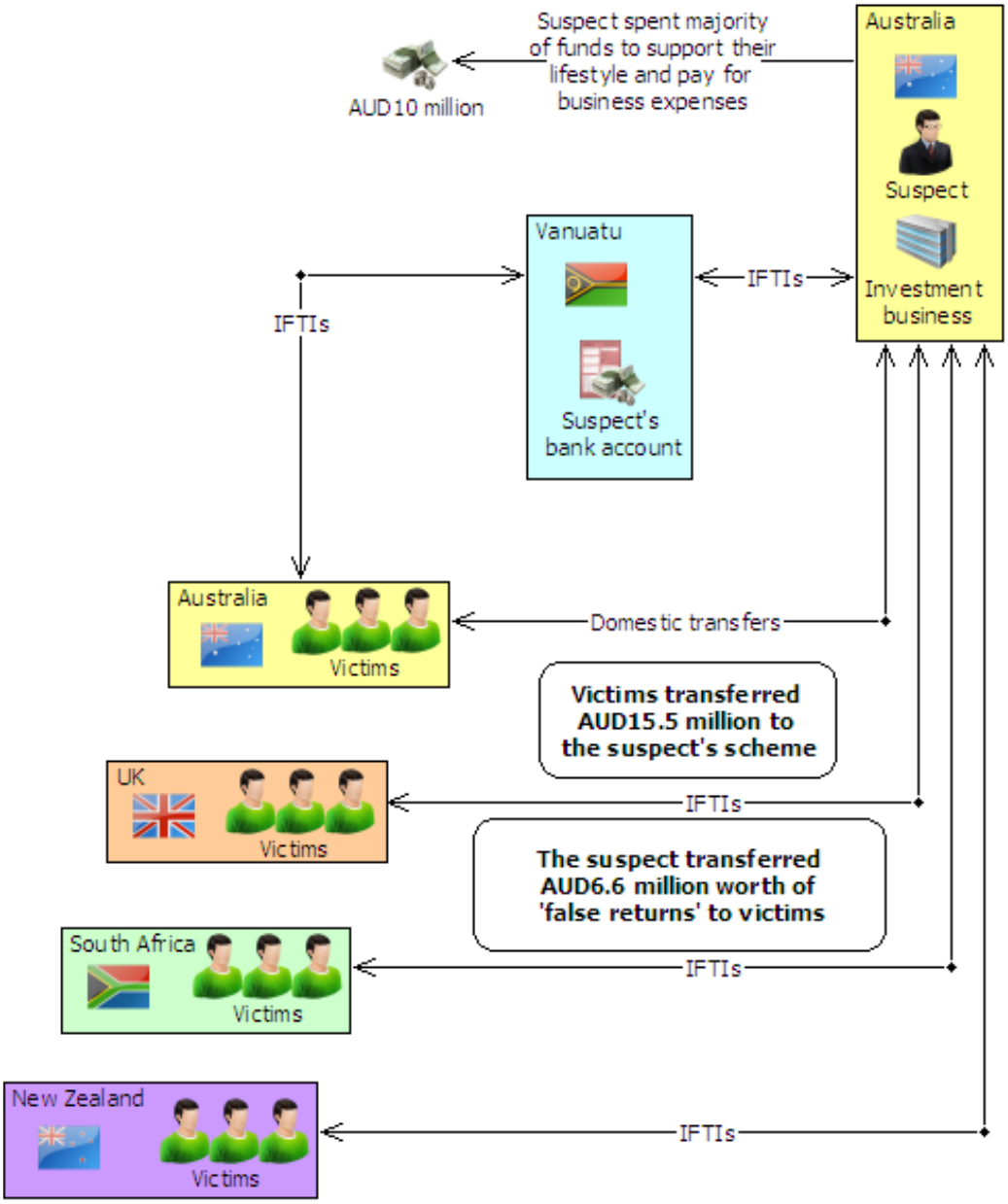
- incoming IFTIs totalled more than AUD1.4 million, with the majority of the funds transferred from Vanuatu and New Zealand. IFTIs were also received from the United Kingdom
- outgoing IFTIs totalled more than AUD610,000, of which more than AUD500,000 was transferred to Vanuatu.

Analysis of the transaction data showed most of the funds the suspect received from victims were applied for purposes other than investment. Of the AUD15.5 million received from victims, AUD6.6 million was returned to investors as either 'false returns' or as payments when investors left the scheme. More than AUD2.8 million was invested in high-risk derivative trading which returned only AUD900,000.

More than AUD10 million was spent to support the suspect's lifestyle and pay for business expenses. Significant business expenses were outlaid to maintain the illusion of a successful managed investment scheme, including rent for a well-appointed office in a popular location.

Subsequent analysis of financial data showed monthly transfers between AUD30,000 and AUD50,000 from the accounts of the group of investment companies to the suspect's credit card account. The suspect also raised more than AUD36,000 in donations for two charities, which the suspect used for personal and investment purposes.

The suspect was charged with seven offences relating to fraud and forgery, and was sentenced to 13 years imprisonment.



Case 4 – Conned investors lost millions in investment Ponzi scheme

Offence	Fraud
Customer	Individual Business
Industry	Banking (ADIs)
Channel	Electronic
Report type	IFTI
Jurisdiction	International – New Zealand, South Africa, United Kingdom, Vanuatu
Designated service	Account and deposit-taking services Securities market/investment services
Indicators	High-value international funds transfers to/from Australia for no apparent logical reason High-volume account activity involving significant amounts of funds International funds transfers to a high-risk jurisdiction Multiple customers conducting international funds transfers to the same overseas beneficiary Use of overseas bank accounts

Case 5 – Suspicious cash transactions helped undo Nigerian fraud suspect

AUSTRAC alerted law enforcement authorities to fraud facilitated by a suspect in Australia who was part of a large-scale Nigerian fraud network. The suspect allegedly scammed more than AUD500,000 from overseas victims via the internet.

The suspect came to AUSTRAC's attention after a suspect transaction report (SUSTR) was submitted by a reporting entity. The report, which had triggered AUSTRAC's automated monitoring system, revealed that the suspect had conducted unusually high-volume and high-frequency international funds transfer instructions (IFTIs) to Nigeria. The funds transfers were paid for in cash and appeared to be structured to avoid the threshold transaction reporting requirements. Authorities established that the suspect used variations of her name when conducting transactions.

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

- over a 10-month period the suspect undertook 35 outgoing IFTIs totalling approximately AUD160,000. The funds were consistently sent to two recipients in Nigeria.
- international funds transfers were conducted through a remittance service provider and paid for with cash. The cash payments were seemingly structured into amounts of less than AUD10,000 to avoid the cash transaction reporting threshold.
- over a 10-month period the suspect was the recipient of nine incoming IFTIs from the United States totalling approximately AUD140,000, suspected to be the proceeds of the fraud.
- the suspect conducted numerous large cash withdrawals and deposits which were detailed in significant cash transaction reports (SCTRs) submitted to AUSTRAC. Over a two-month period the suspect withdrew cash totalling more than AUD86,000 and deposited cash totalling more than AUD52,000.
- over an 11-month period, reporting entities submitted seven SUSTRs to AUSTRAC about the suspicious activities of the suspect. The SUSTRs identified unusually large cash transactions to fund IFTIs to Nigeria and the apparent structuring of transfers to avoid the cash threshold reporting requirements.

AUSTRAC identified that the funds sent to Nigeria appeared to be sourced from a number of cash withdrawals made from the suspect's account and from funds sent from an individual in the United States directly to the suspect. A portion of the funds remained in the suspect's bank account and were believed to represent a commission.

The resulting law enforcement investigation revealed the suspect operated the fraud from home and used various names to communicate with victims over the internet. The suspect secured payments from victims by asking for financial help.

AUSTRAC searches were conducted on additional name variations the suspect used to perpetrate the scam. AUSTRAC information showed the suspect was the subject of an additional eight SUSTRs. Reporting entity staff observed that:

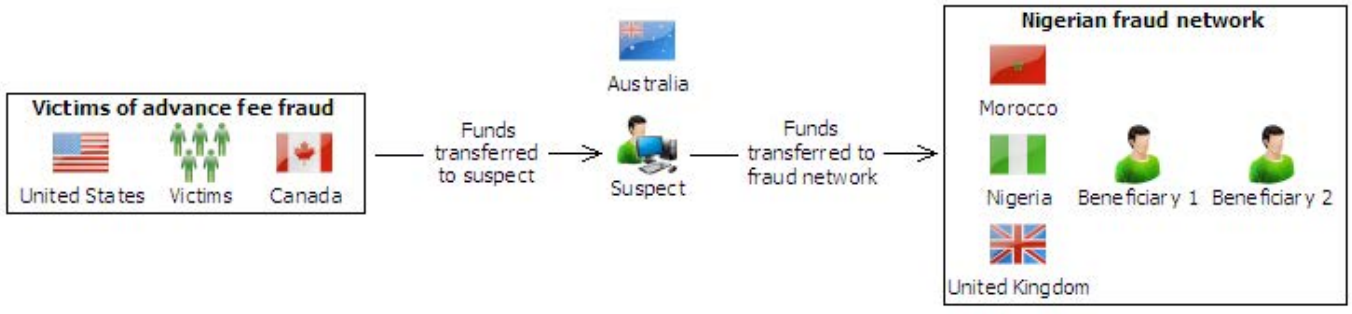
- within one month of opening a bank account, the suspect received approximately AUD150,000 and withdraw all the funds
- the suspect's income and occupation were inconsistent with the high value of transactions she was undertaking
- the suspect became evasive and upset when asked routine questions about a transaction requiring the submission of a SCTR
- the suspect changed the method of withdrawing funds seemingly to avoid threshold reporting requirements, by withdrawing the daily limit of AUD3,000 on a daily basis at various bank branches, then withdrawing another AUD1,000 from automatic teller machines (ATMs).

Further searches were conducted on name variations used by the suspect and identified that the suspect:

- received an additional AUD318,000 in incoming IFTIs from the United States and Canada
- sent an additional AUD207,000 to beneficiaries in Nigeria, the United States, United Kingdom and Morocco
- was the subject of an additional eight SCTRs for deposits totalling approximately AUD124,000 and 11 SCTRs for cash withdrawals totalling approximately AUD172,000
- may have provided false identification to conduct outgoing IFTIs to Nigeria.

Law enforcement officers executed a search warrant on the suspect's premises and seized cash totalling approximately AUD29,000.

The suspect was arrested and charged with six counts of fraud and one count of possessing tainted property. The suspect was convicted and sentenced to six years imprisonment.



Case 5 – Suspicious cash transactions helped undo Nigerian fraud suspect

Offence	Fraud
Customer	Individual
Industry	Banking (ADIs) Remittance services
Channel	Electronic Physical
Report type	IFTI SCTR SUSTR
Jurisdiction	International – Canada, Morocco, Nigeria, United Kingdom, USA
Designated service	Account and deposit-taking services Remittance services (money transfers)
Indicators	Cash withdrawals conducted at various bank branches and ATMs on the same day Customer undertaking transactions which appear to be inconsistent with their profile and/or transaction history High-value cash deposits to pay for international funds transfers High-value international funds transfers to/from Australia for no apparent logical reason Multiple high-value international funds transfers to a high-risk jurisdiction Structured cash payments just below the cash reporting threshold used to pay for international funds transfers Use of false identification to conduct transactions

Case 6 – Australian fraud victims persuaded friends to invest millions in Nigerian scam

AUSTRAC information alerted law enforcement authorities to a Nigerian advance fee fraud involving two Australian-based victims. The victims subsequently became complicit in the scam, after dishonestly persuading friends and associates to contribute funds to the scam. Over an eight-year period approximately AUD3.8 million was sent to fraudsters in Nigeria.

AUSTRAC's monitoring systems identified suspect transaction reports (SUSTRs) and related outgoing international funds transfer instructions (IFTIs) to a beneficiary in Nigeria. The SUSTRs and IFTIs were all linked to one individual in Australia. The circumstances initially suggested the individual and her husband were victims of an advance fee fraud.

Law enforcement enquiries revealed that the husband and wife had been initially contacted via fax and invited to invest in an oil company purportedly based in Nigeria. Over a period of eight years, AUSTRAC information detailed that the husband and wife had contributed more than AUD3.8 million to the non-existent oil company.

The husband and wife had daily telephone contact with the Nigerian fraudsters and engaged a legal professional in South Africa to assist with their 'investment'. The Nigerian fraudsters instructed the husband and wife that all payments were to be conducted via a specific remittance service provider and that international transfers were to be for amounts under AUD10,000.

Law enforcement officers contacted the husband and wife on numerous occasions to warn them that they were being scammed. A Nigerian official accompanied law enforcement officers to visit them to reinforce police advice that they were being scammed, warning them not to send any more money. Convinced the scam was a legitimate investment, the husband and wife continued to send funds.

When their own funds were depleted, the husband (Suspect A) and wife (Suspect B) dishonestly involved friends and associates in the scam. As a result, more than 20 victims lost more than AUD6 million, with some victims losing their houses and businesses.

The husband and wife convinced friends there were two large boxes of cash valued at USD22 million secured in a building at the Reserve Bank of South Africa. They claimed the cash had been marked using a special black coating (purportedly to avoid detection by customs) which needed to be removed using a special chemical. In an attempt to extract more money from victims, the suspects claimed that the cost associated with the money cleaning process was exorbitant. This is a variation on a scheme commonly referred to as a 'black money scam'. In this instance, it appeared to be an element of the larger advance fee fraud, used to maximise the amount scammed.

As a result, Suspect A obtained AUD90,000 from victims, ostensibly for the purpose of chemically cleaning the cash and to also pay for fictitious 'anti-terrorism, anti-money laundering and anti-drug' certificates.

Over a two-year period the suspects cashed 45 cheques totalling approximately AUD1.2 million. A closer examination of AUSTRAC information showed a consistent pattern whereby the suspects conducted IFTIs directly after cashing cheques. In one instance, the suspects deposited a cheque worth AUD90,000 and subsequently conducted 10 outgoing IFTIs to Nigeria for amounts between AUD6,000 and AUD7,000 over the following seven days. This pattern of activity occurred several times following the cashing of cheques.

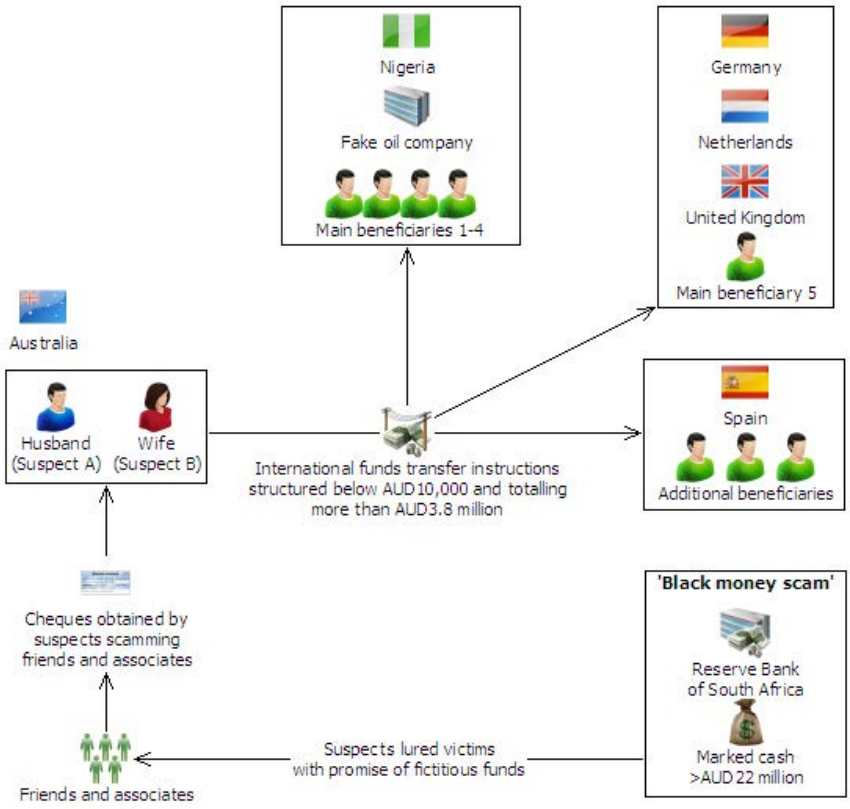
AUSTRAC information identified that:

- the suspects and victims sent IFTIs to the same beneficiaries in Nigeria
- four of the top five offshore beneficiaries of outgoing IFTIs were based in Nigeria
- another of the main offshore beneficiaries of outgoing IFTIs received funds in Germany, the United Kingdom and the Netherlands
- over a 16-month period, Suspects A and B sent IFTIs worth more than AUD305,000 to beneficiaries in Spain
- SUSTRs linked to Suspects A and B highlighted an unusually high frequency and high volume of low-value outgoing IFTIs
- SUSTRs also highlighted that outgoing IFTIs were funded by amounts of less than AUD10,000, apparently to avoid the requirement for reporting entities to report to AUSTRAC cash transactions of AUD10,000 or more
- a reporting entity reported that Suspects A and B sent funds to Nigeria in five transactions from four different remittance service outlets on the same day.

Suspect A was convicted of five fraud-related offences and sentenced to four years imprisonment, suspended after 12 months.

Suspect B was convicted of two fraud-related offences and sentenced to three years imprisonment, suspended with immediate release.

The suspects are believed to be Australia's first advance fee fraud victims to be convicted of fraud because they dishonestly used other individuals to assist them in sending funds offshore.



Case 6 – Australian fraud victims persuaded friends to invest millions in Nigerian scam

Offence	Fraud
Customer	Individual
Industry	Banking (ADIs) Remittance services
Channel	Electronic Physical
Report type	IFTI SUSTR
Jurisdiction	Domestic and international – Germany, the Netherlands, Nigeria, Spain, United Kingdom
Designated service	Account and deposit-taking services Remittance services (money transfers)
Indicators	Multiple international funds transfers below AUD10,000 Multiple international funds transfers conducted via the same remittance service on the same day at multiple locations Multiple international funds transfers sent to the same beneficiary Multiple international funds transfers to a high-risk jurisdiction

Case 7– Major interstate syndicate dismantled in $1.4 million 'ice' bust

Authorities dismantled a major interstate drug syndicate and seized AUD1.4 million worth of crystal methamphetamine hydrochloride ('ice') destined for sale to the public.

Law enforcement officers suspected the criminal syndicate travelled to Sydney to purchase drugs and transported them back to Melbourne by motor vehicle, for distribution and sale. The investigation resulted in the interception of two motor vehicles in transit from Sydney to Melbourne, with drugs located during a search of the vehicles.

Search warrants were executed on residential properties and law enforcement officers confiscated assets including approximately AUD65,000 cash, a luxury motor vehicle, motorcycles and jewellery. Unlicensed weapons, ammunition and a small quantity of ecstasy tablets were also seized.

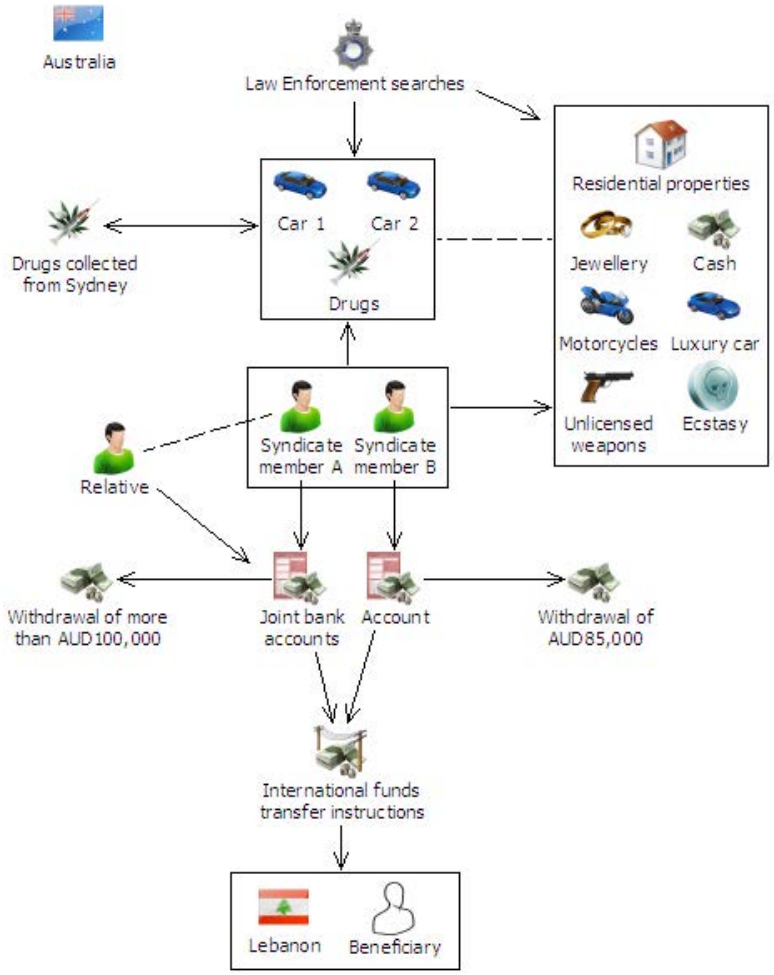
AUSTRAC information supported the investigation which established a link between two syndicate members. Analysis of international funds transfer instructions (IFTIs) showed the syndicate members both sent AUD9,000 on the same day via the same remittance service outlet, to the same beneficiary in Lebanon.

Analysis of AUSTRAC information showed that the financial activity of one syndicate member was closely linked to that of a relative. Both the syndicate member and the relative held joint bank accounts and sent funds to common beneficiaries in Lebanon. An analysis of IFTIs showed that over a six-year period the pair had sent more than AUD46,000 to Lebanon via a remittance service and a financial institution.

Significant cash transaction reports (SCTRs) revealed the syndicate member and the relative had withdrawn more than AUD100,000 in cash from bank accounts over a five-year period. One SCTR showed a significant cash withdrawal of more than AUD37,000.

AUSTRAC information identified that another syndicate member conducted two cash withdrawals of AUD30,000 and AUD55,000 within a seven-month period.

Two men were charged with trafficking a large commercial quantity of drugs and conspiracy to traffick a large commercial quantity of a drug of dependence. A third man was charged with conspiracy to traffick a large commercial quantity of a drug of dependence.



Case 7– Major interstate syndicate dismantled in $1.4 million 'ice' bust

Offence	Drug trafficking
Customer	Individual
Industry	Banking (ADIs) Remittance services
Channel	Physical
Report type	IFTI SCTR
Jurisdiction	Domestic and international - Lebanon
Designated service	Account and deposit-taking services Remittance services
Indicators	International funds transfers to a high-risk jurisdiction Large cash withdrawals within a short timeframe Multiple cash withdrawals from accounts Multiple customers conducting international funds transfers to the same overseas beneficiary in one day

Case 8 –Superannuation accounts targeted in a multi-million dollar identity theft

AUSTRAC information was used extensively by a law enforcement agency to investigate a multi-million dollar identity theft and fraud syndicate that targeted superannuation accounts.

Members of the syndicate stole cheques, superannuation statements and personal bank statements from the mailboxes of unsuspecting victims and used this information to produce high-quality counterfeit identity documents. These documents were then used to conduct frauds.

Syndicate members also approached some victims directly, offering them early access to their superannuation funds and requesting details of their funds to facilitate access to their superannuation benefits.

The criminal syndicate carried out four variations of the fraud, using the following methods to obtain superannuation funds from unsuspecting victims:

1. The syndicate member steals a victim's identification papers and opens a self-managed superannuation fund (SMSF) in the victim's name. The syndicate member then sets up a linked, but fraudulently obtained, bank account using the details of the new SMSF. Assuming the victim's identity, the syndicate member contacts the victim's superannuation provider and requests that they 'roll over' the funds from the legitimate superannuation fund into the new, fraudulent SMSF. The syndicate member then withdraws the funds from the new SMSF account and sends them to the syndicate member's offshore account using remittance service providers.
2. The syndicate member offers a victim the chance to access their superannuation funds early. Scammers usually target victims who are struggling with debt, unemployed and from non-English speaking backgrounds. The victim, enticed by the offer, provides their financial and identification details to the syndicate member to facilitate the early release of the funds. The syndicate member withdraws the funds and takes approximately 20 per cent as their fee. The balance is paid to the victim in cash.
3. As a variation of the above method, the syndicate member offers early access to superannuation funds to lure a victim to provide their financial and identification details. In this instance, the syndicate member uses this information to steal all the victim's superannuation funds. The victim receives nothing.
4. The syndicate member offers to roll over a victim's superannuation into a legitimate fund that they claim will offer a better return. The victim provides the syndicate member with their financial and identification details. The syndicate member rolls over the victim's funds into the syndicate member's fraudulent SMSF and then withdraws the funds from the bank account.

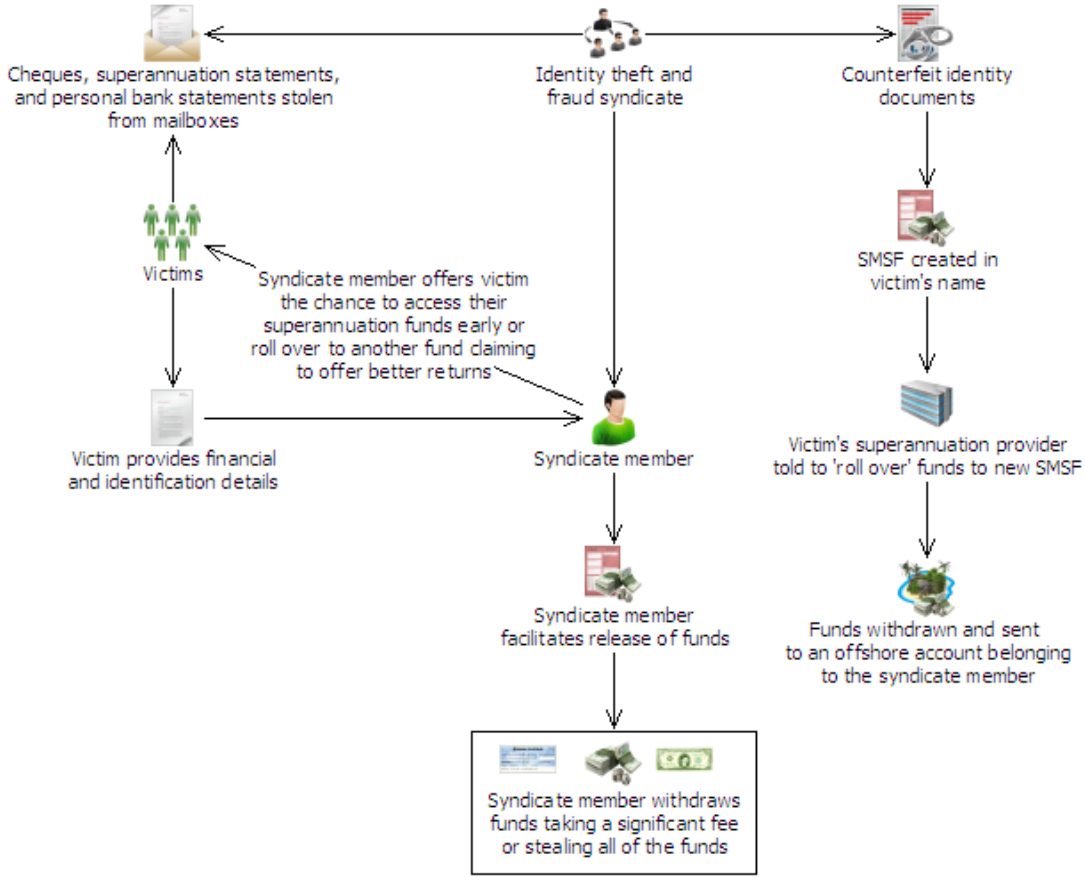
AUSTRAC received suspicious matter reports (SMRs) and suspect transaction reports (SUSTRs) detailing information about individuals suspected of perpetrating the fraud. Information in these reports, combined with further AUSTRAC analysis, identified a large criminal syndicate which was:

- receiving regular cheque deposits into newly opened accounts and paying an additional fee to ensure the cheques cleared quickly. Once the cheques were deposited, the funds were withdrawn from the accounts, either via cash (in amounts of AUD1,000–AUD20,000) or via cheques (valued at between AUD6,500 and AUD45,000) made payable to third parties. The cash withdrawals of AUD10,000 or more were reported to AUSTRAC as significant cash transactions.
- submitting fraudulent applications to roll over funds from victims' superannuation funds managed by retail or industry fund managers, into accounts held by the syndicate members.

One particular SMR alerted a law enforcement agency to the suspicious activities of a syndicate member. The SMR identified the syndicate member as the signatory to two business cheque accounts which had been newly opened to operate two SMSFs. Over a three-month period these accounts received more than AUD500,000 worth of funds which had been rolled over from several superannuation funds. Once the funds were deposited into the new cheque accounts, they were immediately withdrawn by the syndicate member. Information about the international transfers was submitted by reporting entities to AUSTRAC via international funds transfer instructions (IFTIs).

A total of 25 syndicate members were charged with more than 2,500 offences involving the laundering of over AUD8 million in fraudulently obtained funds.

The head of the syndicate, who controlled three bank accounts which turned over AUD1.6 million, was charged and found guilty of 57 counts of identity fraud and money laundering relating to transactions valued at more than AUD550,000.



Case 8 –Superannuation accounts targeted in a multi-million dollar identity theft

Offence	Fraud Money laundering
Customer	Business Individual
Industry	Banking (ADIs) Remittance services
Channel	Electronic Physical
Report type	IFTI SCTR SMR SUSTR
Jurisdiction	Domestic International
Designated service	Account and deposit-taking services Remittance service (money transfers)
Indicators	Customer submits a fraudulent application to roll over funds from a superannuation account into a newly opened account Customer undertaking large deposits and cash withdrawals inconsistent with their established customer profile Significant cash and cheque deposits/withdrawals from newly opened accounts Significant value and volume of cash deposits into newly opened bank accounts Significant value of funds rolled over into a recently opened SMSF account, followed by immediate cash withdrawals Use of false identification

Case 9 – Missing stamp duty led authorities to uncover large-scale cocaine importations

A joint-agency investigation into cocaine distribution was initiated by law enforcement agencies, with AUSTRAC information proving to be of vital importance. The investigation uncovered a large-scale drug importing syndicate operating within Australia.

Law enforcement agencies were made aware that a key suspect had recently purchased a home for more than AUD1 million, from two known associates. Further enquiries revealed that the purchase was partially financed through a series of structured cash deposits totalling approximately AUD385,000.

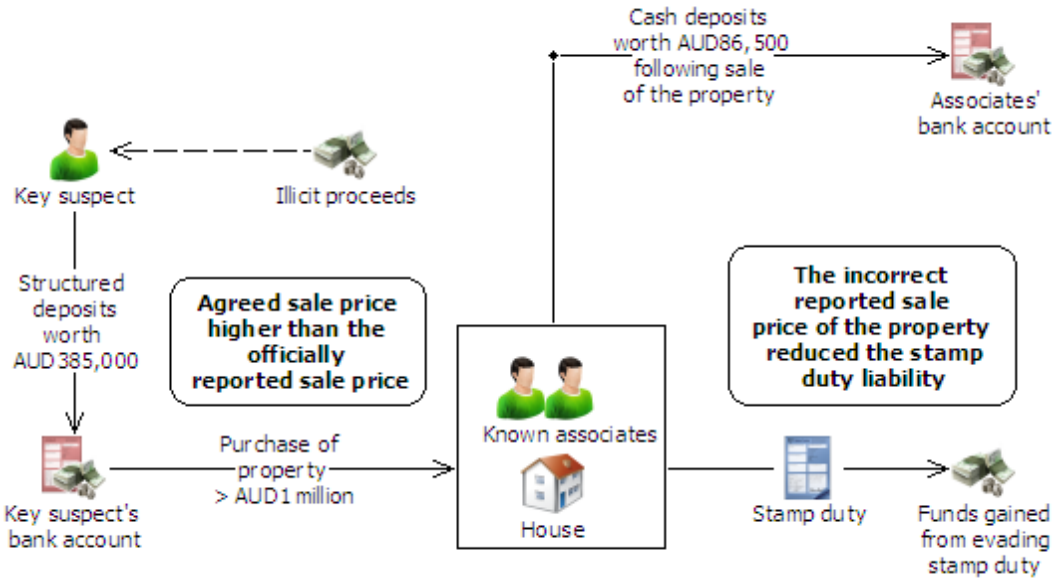
Law enforcement agencies investigating the suspicious purchase searched AUSTRAC's financial transaction data. They found nine cash deposits totalling more than AUD86,000 were made by the vendor of the property following the sale. These deposits suggested the vendor received additional cash funds after the sale of the property. This indicated the actual sale price was higher than the officially reported sale price and this would have reduced the stamp duty liability. This activity is an indicator of money laundering and a methodology for stamp duty evasion.

Further investigations into a number of suspects revealed that over an 18-month period, one suspect made 114 structured cash deposits totalling more than AUD600,000. During this time, a second suspect had deposited approximately AUD360,000 in 50 structured deposits. This activity appeared to be a further attempt to launder the proceeds of crime.

At that stage, law enforcement agencies believed that a number of suspects were conspiring to import drugs into Australia. AUSTRAC alerted the law enforcement agencies to one suspect and his family who had sent multiple international funds transfers to Lebenon with a total value of approximately AUD100,000. Law enforcement agencies, using AUSTRAC information, investigated the circumstances around the money sent to Lebanon. As a result, a series of search warrants were executed at a number of locations.

As a result of this joint-agency operation, 13 people were arrested and charged with offences relating to possession of drugs, firearms offences and money laundering. In addition, AUD13.5 million in cash, two kilograms of cocaine, 17 firearms, a number of prestige cars and a house were seized.

Seven of the 13 persons arrested were sentenced to jail for periods ranging from five to 30 years. Four persons, who assisted the key syndicate members in laundering the proceeds of crime, received good behaviour bonds.



Case 9 – Missing stamp duty led authorities to uncover large-scale cocaine importations

Offence	Drug trafficking Money laundering
Customer	Individual
Industry	Banking (ADIs) Real Estate
Channel	Electronic Physical
Report type	IFTI
Jurisdiction	Domestic International - Lebanon
Designated service	Account and deposit-taking services
Indicators	Customer undertaking transactions which appear to be inconsistent with their profile and/or transaction history International funds transfers to a high-risk jurisdiction Structured deposits into a bank account, used to purchase high-value assets (real estate) Structuring of cash deposits over an extended period to avoid reporting requirements

Case 10 – Shell companies and cash payments used in million dollar tax fraud

The activities described in the case below are an example of the money laundering typology involving the use of cheques, outlined earlier in the report in the 'Established typologies' section.

AUSTRAC information assisted law enforcement to identify a criminal syndicate which was facilitating large-scale tax evasion for a number of clothing manufacturers.

Investigations revealed that, over a three-year period, more than AUD52 million was deposited into and withdrawn from accounts operated by the syndicate. Many of these transactions were reported to AUSTRAC by reporting entities via the submission of significant cash transaction reports (SCTRs). During this period the annual financial activity of the syndicate increased dramatically from approximately AUD750,000 in the first year to more than AUD17.5 million in the last year. The syndicate would receive cheques from the manufacturing businesses and deposit them into accounts linked to 'shell companies'. Once the cheques had cleared, the syndicate would withdraw the cash in multiple amounts and secretly return the cash to the businesses.

Two suspect transaction reports (SUSTRs) submitted by reporting entities triggered AUSTRAC's automated monitoring system. The information in the SUSTRs, along with AUSTRAC's additional analysis of related financial activity, identified 10 clothing manufacturing businesses in one geographic location which had been conducting large cash withdrawals over an extended period of time.

The SUSTRs also identified unusual financial activity involving members of the syndicate who were frequently depositing cheques into company accounts, followed by cash withdrawals equivalent in value to the cheque deposits, on the same day. This information prompted AUSTRAC to produce a financial intelligence assessment report for law enforcement agencies about these businesses.

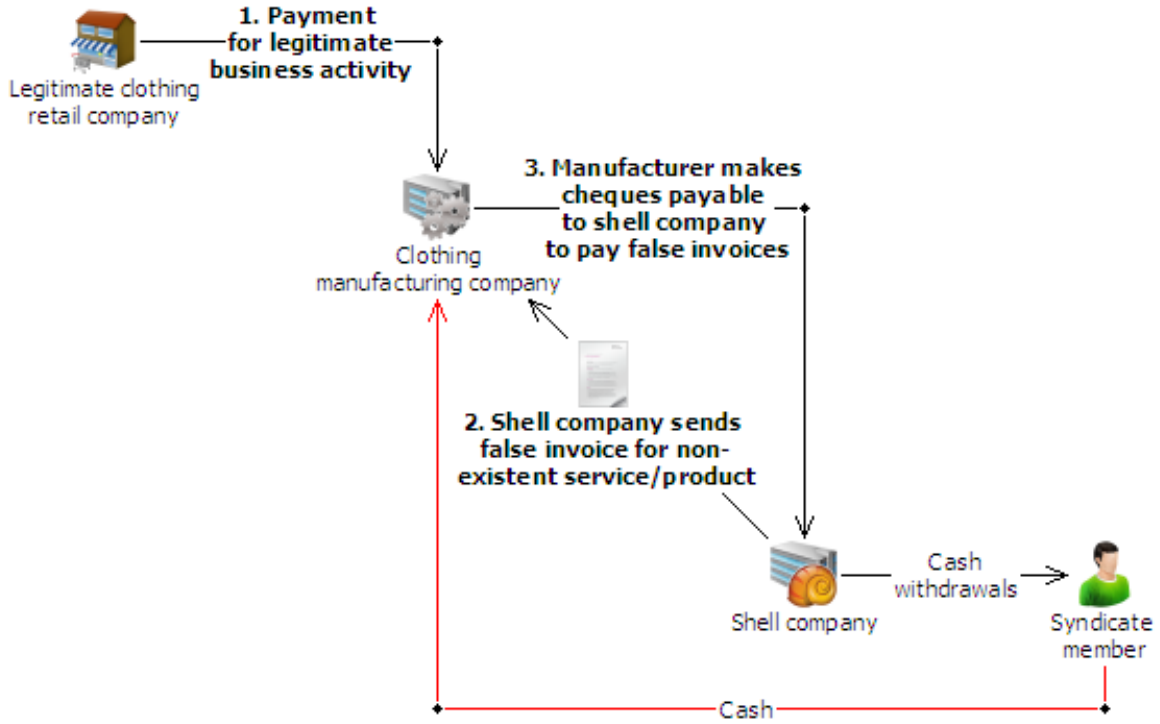
The fraud allowed the manufacturing companies to evade income tax and other taxation obligations, and move their profits into the cash economy. Authorities believe that, because employees working for the manufacturing companies were paid in cash, they were also able to claim welfare benefits while working.

The method used by the syndicate to facilitate tax evasion is as follows:

1. A number of legitimate clothing retail companies paid a clothing manufacturing company for the production of garments. These payments were for legitimate business activity and the retail companies were not complicit in the scheme.
2. The promoters of the scheme made approaches to the garment makers and offered to help them to reduce the amount of tax they were paying, less payment of a commission to the promoters of between 5 percent and 10 percent.
3. A series of shell companies were set up using details of members of the group of companies who had been approached by the promoters and paid a small amount of money for their personal details. These details were then used to register the companies, obtain workers compensation insurance and open bank accounts in order to create a facade of legitimacy.
4. With the assistance of the promoters, the shell companies created false invoices and issued them to the clothing manufacturers for the provision of fictitious goods and services. These false invoices enabled the manufacturer to claim tax deductions for subcontracting expenses that were never incurred.

5. The manufacturers made cheques payable to the shell companies to pay the false invoices.
6. Members of the syndicate deposited the cheques into the accounts of the shell companies.
7. Once the cheques had cleared, the syndicate members withdrew the funds from the accounts via multiple cash withdrawals using debit cards issued to the accounts of the shell companies. These withdrawals were undertaken across various bank branches.
8. The syndicate returned the cash to the manufacturer, minus a commission.
9. The manufacturers used the cash to fund their lifestyles and pay cash wages to their employees, thereby avoiding income tax obligations.

The diagram below provides a visual representation of the methodology.



Case 10 – Shell companies and cash payments used in million dollar tax fraud

Further investigations revealed that a bank assistant manager had maintained a close relationship with the syndicate. The assistant manager used her influence over other bank staff to ensure AML/CTF reporting procedures were ignored. Members of the syndicate had also offered gifts to bank tellers to build rapport and encourage them to skip some stages of their AML/CTF program, thereby helping the syndicate avoid detection by AUSTRAC. Typically, a complicit staff member would allow a syndicate member to withdraw funds from multiple shell company accounts at the same time, even though they did not have the right to do so. The promoters actively sought the services of these bank staff, even knowing which staff would be working on particular days of the week.

The good working relationship law enforcement had with members of the bank's AML/CTF team proved to be vital in the ultimate success of the law enforcement investigation.

AUSTRAC also received a number of suspicious matter reports (SMRs) from reporting entities which helped reveal the methodology used by the syndicate. Within the SMRs, reporting entities identified the following 'grounds for suspicion':

- Several cheques written by the manufacturing companies were deposited (often several times in one day) by the syndicate members into multiple accounts operated by the shell companies. The syndicate members repeatedly requested quick clearances for the cheques.
- Funds were withdrawn from accounts as cash as soon as the proceeds of cheque deposits cleared, often on the same day, across multiple branches.

The manufacturing businesses were associated with more than AUD16 million in cash withdrawals over a twelve-month period.

When law enforcement officers moved to stop the syndicate, they restrained more than AUD1 million in cash, as well as a number of properties. Two members of the syndicate who facilitated the scheme were charged with dealing in proceeds of crime worth AUD1,000,000 or more, contrary to Section 400.3(1) of the *Criminal Code Act 1995*.

Offence	Tax evasion
Customer	Business
Industry	Banking (ADIs)
Channel	Electronic Physical
Report type	SCTR SMR SUSTR
Jurisdiction	Domestic
Designated service	Account and deposit-taking services
Indicators	Customer offers incentives to representatives of a financial institution to assist bypassing AML/CTF procedures Repeated requests for quick cheque clearances by customer Same day cheque deposits, followed by cash withdrawals of an equivalent value to the cheque deposits, across multiple branches Significant value and volume of cash withdrawals Significant value and volume of cheque deposits into bank accounts

Case 11 – Police thwarted 500 kilogram cannabis shipment from Papua New Guinea

Australian law enforcement agencies worked with counterparts in Papua New Guinea (PNG) to dismantle an international drug syndicate conspiring to import more than 500 kilograms of cannabis to Australia. The street value of the cannabis could have exceeded AUD10 million had the importation reached Australia and not been disrupted by law enforcement.

Two suspects (A and B) in Australia inadvertently informed an undercover law enforcement officer of their plans to import the cannabis from PNG to Australia. One of the suspects, a PNG national, indicated they had relatives in PNG who could deliver the cannabis to a port in PNG. An associate in PNG would then transport the cannabis to Australia using small boats.

A New Zealand national, suspect C, was also involved. Suspect B, also from New Zealand, contacted suspect C and sought assistance with the funding, importation and subsequent distribution of the cannabis. It was agreed suspect C would receive 10 per cent of the actual imported cannabis. Suspect C transferred AUD1,000 into suspect B's account to assist with funding the importation.

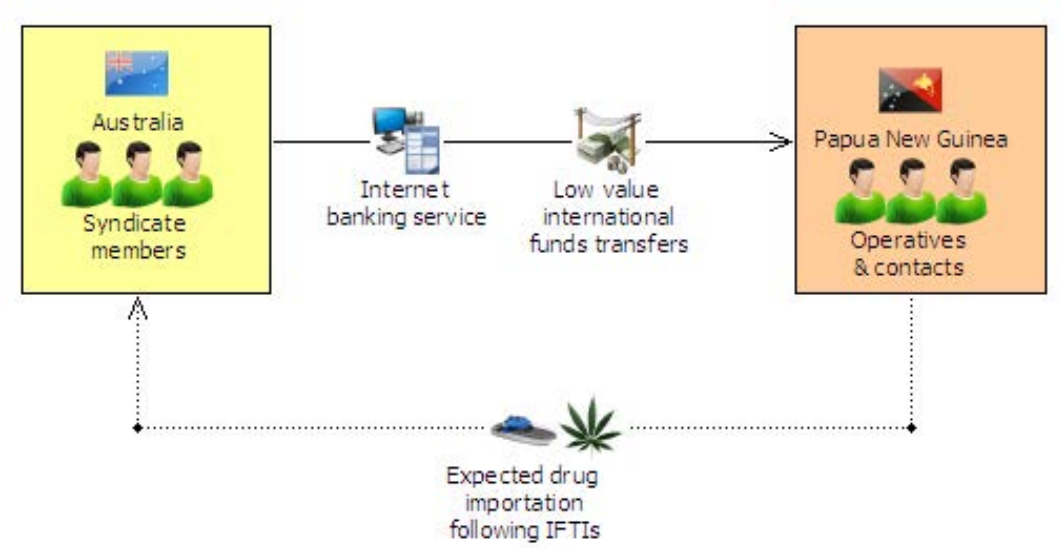
A fourth syndicate member, suspect D (a relative of suspect A), arranged with the PNG operative to collect and store the cannabis in PNG. Over a three-month period, suspect D conducted five outgoing international funds transfers totalling more than AUD1,500 from their Australian account to their PNG account and their PNG associate's account, to finance the importation.

As a result of international cooperation between Australian law enforcement agencies and their PNG counterparts, PNG authorities became aware of the planned drug importation operation and raided a warehouse, finding 19 kilograms of cannabis. The PNG-based operative was arrested as a result. Simultaneously, an Australian law enforcement agency raided an Australian property and seized equipment for cultivating cannabis.

AUSTRAC information was used as a primary source of intelligence to draw links between targets that had not previously been known to be associated. A number of international funds transfer instructions (IFTIs) were recorded on AUSTRAC's database, identifying transactions between syndicate members in Australia and operatives overseas. These IFTIs were usually conducted via internet banking through an account held with a major bank.

One IFTI of more than AUD800 was sent from suspect D to a beneficiary in PNG – authorities identified this payment as likely to have been for the transportation and shipment of the cannabis to Australia.

All syndicate members pleaded guilty on charges of conspiring to import drugs. Three were sentenced to imprisonment for three years and six months. Suspect B was sentenced to imprisonment for four years.



Case 11 – Police thwarted 500 kilogram cannabis shipment from Papua New Guinea

Offence	Drug importation
Customer	Individual
Industry	Banking (ADIs)
Channel	Electronic
Report type	IFTI
Jurisdiction	Domestic International – Papua New Guinea
Designated service	Account and deposit-taking services
Indicators	Multiple low-value international funds transfers International funds transfers to a high-risk jurisdiction

Case 12 – Ten thousand fake credit cards seized from money laundering syndicate

A suspicious matter report (SMR) was the catalyst for a law enforcement operation which resulted in the arrest of three foreign nationals. The operation revealed a multi-million dollar money laundering syndicate which was laundering illicit proceeds derived from producing fraudulent credit cards.

As a result of the SMR referral authorities seized more than 10,000 fake credit cards, which they believed had the potential to fund AUD25 million worth of fraudulent transactions.

The initial SMR related to the main suspect making an outgoing international funds transfer instruction (IFTI) to China, funded with AUD500,000 in cash from an unknown source. Two foreign nationals were also recruited by the main suspect to conduct similar financial transactions for the syndicate.

The lodgement of the SMR triggered AUSTRAC's automated monitoring systems and initiated enquiries by AUSTRAC of related financial transactions. The enquiries revealed that the syndicate used remitters who primarily sent funds to Chinese beneficiaries and also identified other high-value transactions made by the main suspect. The other transactions included cash deposits of values more than AUD10,000 that were reported to AUSTRAC via threshold transaction reports (TTRs).

Over a two-week period the main suspect deposited cash into the remitter's account, totalling AUD1.75 million, which funded international funds transfers to two beneficiaries in China. The suspect also made a foreign exchange purchase of AUD300,000, meaning that, over a two-week period, the main suspect had exchanged or deposited more than AUD2 million cash.

A further seven SMRs were submitted to AUSTRAC from reporting entities over the next four months, detailing further transactions worth AUD2 million, including cash deposits and IFTIs.

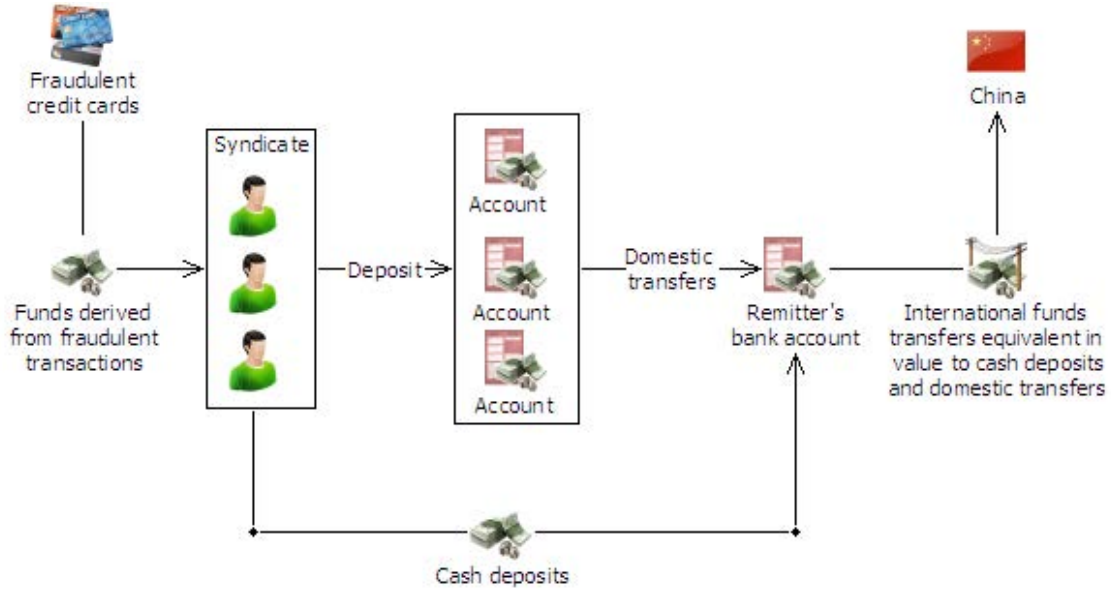
The SMRs identified that the syndicate was:

- depositing large values of cash into the account of a remittance business to fund IFTIs which were sent immediately after the deposit
- conducting multiple domestic transfers from several bank accounts into the same remitter's bank account, to fund IFTIs equal in value to the domestic transfers.

AUSTRAC assisted authorities with further searches on related financial transaction reports and found that the syndicate had, over this same four-month period, deposited more than AUD5 million in cash and conducted AUD6.5 million worth of outgoing international funds transfers to China and Hong Kong.

Authorities arrested the main suspect and two other foreign nationals, and seized fraudulent credit cards, sophisticated card-making equipment and AUD60,000 cash.

Two of the syndicate members pleaded guilty to dealing with cash reasonably suspected of being the proceeds of crime, and were sentenced to seven months and 12 months imprisonment. The main suspect was charged with offences relating to the manufacture of counterfeit credit cards, possessing proceeds of crime, money laundering offences and having a false passport. The suspect was sentenced to a maximum of five years and nine months.



Case 12 – Ten thousand fake credit cards seized from money laundering syndicate

Offence	Fraud Money laundering
Customer	Individual
Industry	Banking (ADIs) Remittance services
Channel	Physical Electronic
Report type	IFTI SMR TTR
Jurisdiction	Domestic International – China, Hong Kong
Designated service	Account and deposit-taking services Remittance services (money transfers)
Indicators	Financial transactions inconsistent with established profile Frequent and large-value cash deposits into a remitter's bank account to fund an international funds transfer Multiple domestic transfers, from several accounts, into a remitter's bank account to fund an international funds transfer Unexplained wealth

Case 13 – Vietnamese heroin importation syndicates dismantled

The following two cases, detailed in Part A and B, describe the activities of two suspects who worked with other criminal syndicates to import heroin from Vietnam into Australia. AUSTRAC information allowed law enforcement agencies to trace the various syndicates' financial activity, identify syndicate members and establish links between them and a wider network of syndicates.

Part A describes how AUSTRAC information revealed to authorities one syndicate's money laundering methodology through an Australian casino. Part B demonstrates how AUSTRAC analysis revealed links among a network of drug trafficking crime syndicates.

Part A and B are separate law enforcement investigations. The two cases are presented together to demonstrate how the use of AUSTRAC information was able to establish previously unknown links between suspects and crime syndicates.

Part A

AUSTRAC provided financial transaction reporting and associated analysis to law enforcement agencies which was instrumental in dismantling an international drug importation syndicate operating in Australia.

For a number of years, the syndicate had been importing heroin of the highest purity from Vietnam. Drug couriers brought the heroin into Australia by concealing it internally.

The syndicate used a consistent methodology for recruiting drug couriers and smuggling the drugs into Australia:

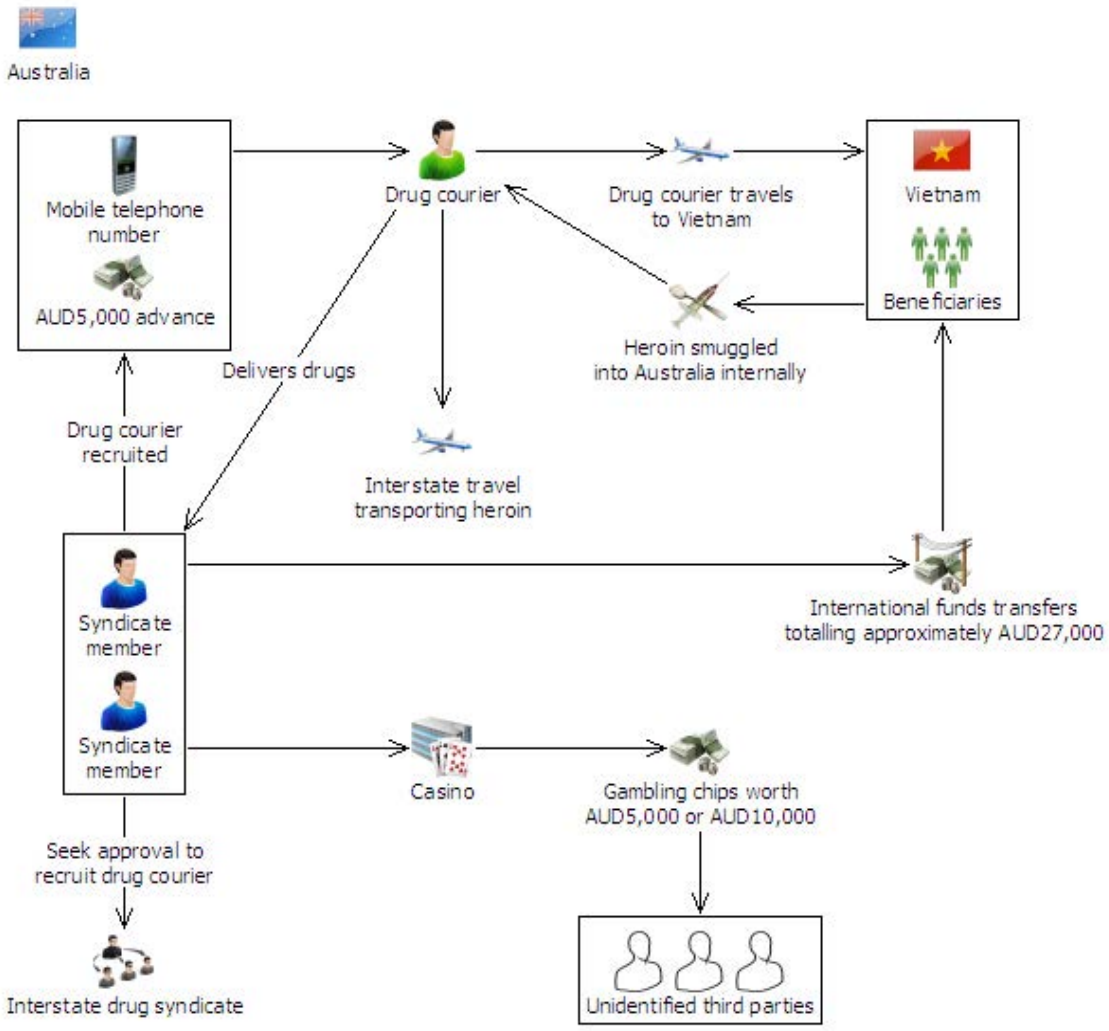
- The syndicate generally recruited individuals of Vietnamese descent who were in some form of gambling-related financial difficulty.
- The syndicate coerced these individuals into becoming couriers by providing them with loans until, eventually, they owed so much money to the syndicate they were forced to act as drug couriers to pay off their debts.
- When a courier was recruited, the syndicate would seek approval from members of another interstate drug syndicate to undertake a drug importation.
- Once the interstate syndicate approved, the main syndicate would give the newly recruited drug courier an advance of AUD5,000.
- Before the couriers flew out of Australia, the syndicate would provide them with a Vietnamese mobile telephone number and instructions on how to contact individuals on arrival in Vietnam.
- Once the courier had obtained the drugs, they would smuggle the drugs internally back into Australia where they were met by the main suspects who would assist with the removal of the drugs and then arrange distribution.
- Couriers were also used to smuggle drugs within Australia, by transporting the drugs internally on domestic flights for delivery to syndicate members and other syndicates located interstate.

AUSTRAC received suspect transaction reports (SUSTRs) relating to the syndicate's activities at a casino. The SUSTRs showed the main suspects regularly provided gambling chips to the value of AUD5,000 or AUD10,000 to unidentified third parties. These third parties would then cash the chips after limited gambling activity. This activity was an indication that the main suspects were using the third parties to launder illicit funds through the casino on their behalf, or were using the casino as a venue to covertly pay members of the syndicate.

AUSTRAC found that no cash threshold transaction reports (TTRs) had been submitted to it in relation to the syndicate's activities at the casino, despite the high volume of funds the suspects had been moving through the venue. This suggested to authorities that the syndicate had been 'structuring' its cash transactions into amounts of less than AUD10,000 to avoid the threshold transaction reporting regime.

AUSTRAC information also included reports of a number of international funds transfer instructions (IFTIs) conducted by the main suspects to beneficiaries in Vietnam, totalling approximately AUD27,000.

The investigation led to four suspects being arrested and charged with various drug offences and the seizure of an estimated AUD5 million worth of drugs. The suspects were convicted and sentenced to terms of imprisonment ranging from three to 11 years.



Case 13 – Vietnamese heroin importation syndicates dismantled - Part A

Offence	Drug trafficking
Customer	Individual
Industry	Banking (ADIs) Gambling services
Channel	Electronic Physical
Report type	IFTI SUSTR
Jurisdiction	International – Vietnam
Designated service	Account and deposit-taking services Gambling services
Indicators	Gaming chips given to unidentified third parties who cash the chips following minimal gambling activity High volumes of cash moving through accounts belonging to persons of interest at gaming venues Individuals structuring funds when cashing chips to avoid reporting requirements International funds transfers to high-risk jurisdictions and individuals of interest to authorities Unusual gaming activity

Part B

AUSTRAC information assisted an investigation by identifying previously unknown entities and links between a crime syndicate and a network of other drug syndicates operating in Australia, including the syndicate described in Part A. As a result, Australian law enforcement agencies were able to dismantle a number of the syndicates within the network.

Similar to the activity in Part A, the primary syndicate imported heroin from Vietnam to Australia using drug couriers concealing the drugs internally. This primary syndicate also sourced large amounts of heroin from a second drug syndicate, which operated in a different Australian state.

At the request of the investigating law enforcement agencies, AUSTRAC produced a number of intelligence assessments which analysed various aspects of the primary syndicate's financial activities. AUSTRAC information enabled law enforcement to identify and link Suspects A and B. Both these suspects were members of the second syndicate and major suppliers of drugs to the primary syndicate. Suspects A and B also had strong links to a third syndicate – the subject of Part A of this case study.

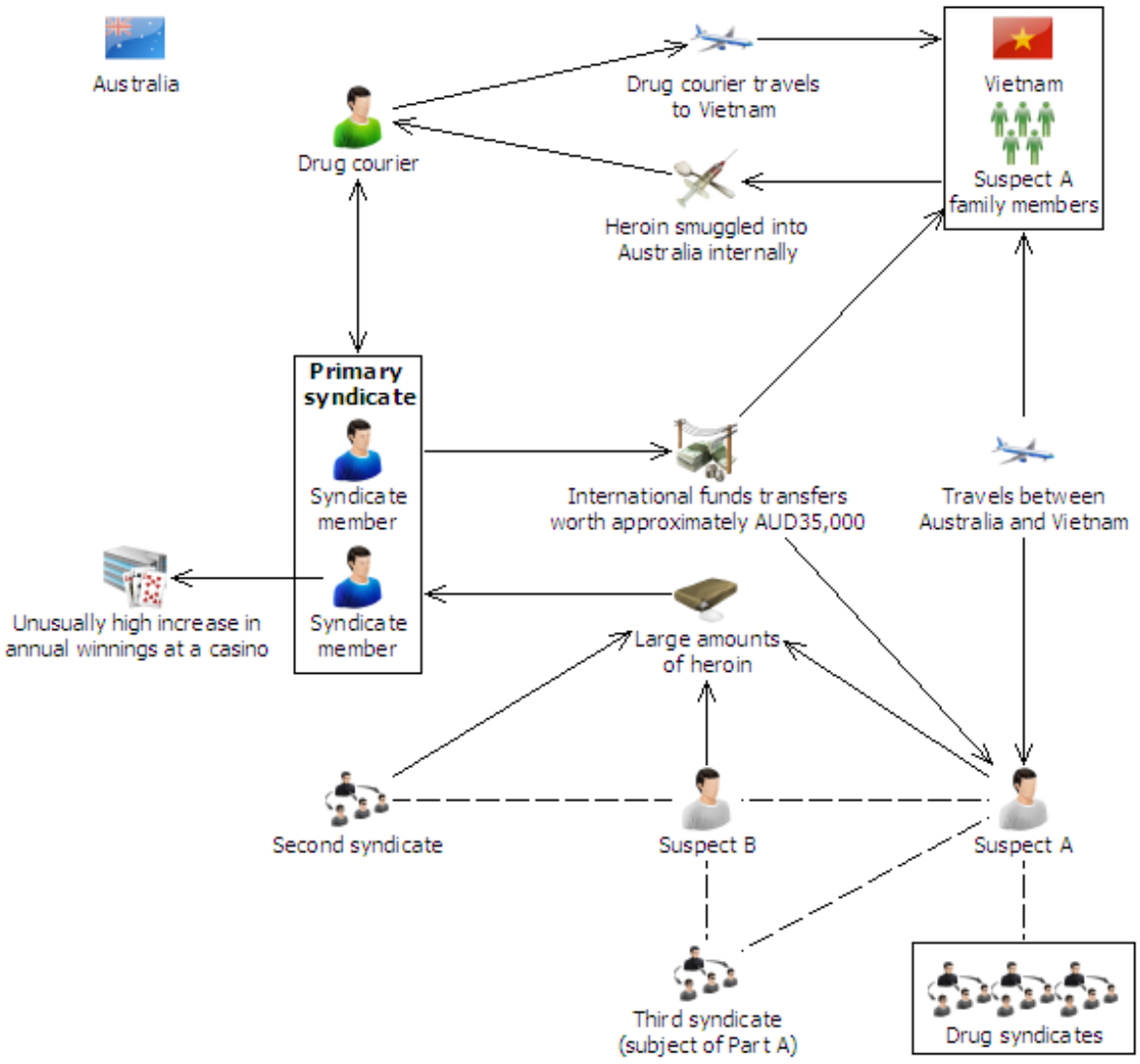
AUSTRAC information revealed that:

- members of the primary syndicate made five international funds transfers (IFTIs) to entities in Vietnam, worth approximately AUD35,000. The majority of funds were sent to Suspect A, who was also the beneficiary of several additional IFTIs sent from Australia to Vietnam by other individuals linked to the drug syndicates.

- AUSTRAC received a suspicious matter report (SMR) reporting an unusually high increase in the annual winnings at a casino by one of the main suspects of the primary syndicate. This unexplained wealth suggested that the suspect was receiving additional income from unknown sources.
- Suspect A appeared to be in control of a number of syndicates which were all part of an extensive drug trafficking network. This included the primary syndicate and the third syndicate (which was analysed in Part A).

Suspect A was known to travel between Australia and Vietnam, with family members in Vietnam who were part of the operation.

As a result of the law enforcement investigation, suspects A and B were arrested and charged with drug offences.



Case 13 – Vietnamese heroin importation syndicates dismantled - Part B

Offence	Drug importation
Customer	Individual
Industry	Banking (ADIs) International funds transfers
Channel	Electronic Physical
Report type	IFTI SMR
Jurisdiction	International – Vietnam
Designated service	Account and deposit-taking services
Indicators	Customer involved in high-value funds transfers, which are inconsistent with expected/established financial activity for the customer (i.e. unexplained wealth) Customer making regular international funds transfers of significant values to high-risk jurisdictions Multiple customers conducting international funds transfers to the same overseas beneficiary Unusually high increase in annual winnings from gaming activities

Case 14 – Hong Kong nationals avoided thousands in GST in jewellery import fraud

A suspicious matter report (SMR) informed a joint-agency investigation into a criminal syndicate which was undertaking significant tax evasion. The two suspects, one the director of an Australian jewellery business and the other an employee, were using the business to avoid paying the GST on imported jewellery.

The suspects were Hong Kong nationals. They would periodically enter Australia with jewellery, declaring the value of the goods significantly below their actual value. The suspects would sell the jewellery to clients based in Sydney, Melbourne, Adelaide and Brisbane and send the profits back to Hong Kong. The suspects had created a GST payment account with their financial institution. A GST payment account would usually be used to set aside funds to pay GST liabilities to the Australian government. AUSTRAC received an SMR from a reporting entity indicating that, over a six-month period, the GST payment account had received primarily cash deposits worth approximately AUD34,000. These deposits had been made by unknown third parties in New South Wales and Victoria. It was believed the cash deposits were from the proceeds of the jewellery sales.

The cash deposits were in amounts less than the AUD10,000 cash transaction reporting threshold and were therefore not reportable under the AML/CTF Act's transaction reporting requirements. The proceeds of these deposits were then withdrawn via cheques and made payable to the business account operated by the jewellery business.

Authorities identified large discrepancies between the declared value of the imported jewellery and the funds remitted to Hong Kong by the jewellery business. This was a strong indicator that the suspects were under-declaring the value of the imported jewellery and, thereby, evading paying the correct amount of tax. The proceeds of jewellery sales were remitted to Hong Kong and reported to AUSTRAC through international funds transfer instructions (IFTIs).

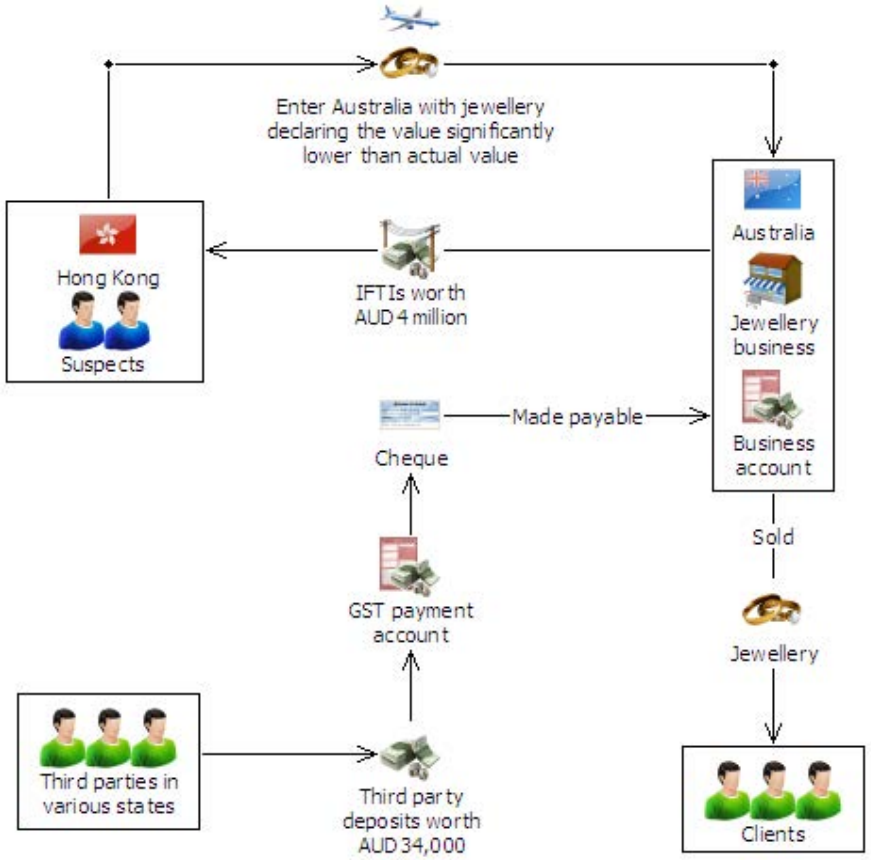
Over a five-year period, the suspects' jewellery business declared more than AUD120,000 worth of imported jewellery upon entry into Australia. AUSTRAC information identified that various individuals working for the jewellery business had sent IFTIs worth more than AUD4 million to Hong Kong in the same period – funds that authorities established were the proceeds of the jewellery sales.

When authorities became aware of the scheme, the suspects' passports and jewellery were seized upon their travel into Australia.

Both suspects were served with taxation notices of assessment and departure prohibition orders.

However, the two suspects fled Australia in contravention of the departure prohibition orders, using false documentation.

The jewellery seized by authorities was sold at auctions, raising almost AUD700,000. This amount was used to offset the loss of revenue for the Australian government.



Case 14 – Hong Kong nationals avoided thousands in GST in jewellery import fraud

Offence	Tax evasion Fraud
Customer	Business Individual
Industry	Banking (ADIs)
Channel	Electronic Physical
Report type	IFTI SMR
Jurisdiction	Domestic International – Hong Kong
Designated service	Account and deposit-taking services
Indicators	Account activity inconsistent with business profile Cheques from a GST payment account made payable to companies or individuals, rather than to the Australian Taxation Office (ATO) Third-party cash deposits into a GST payment account in various states Using the functions of a GST payment account as a normal business account

Case studies
Gambling services

3

Case studies – Gambling services

Case 15 – Asian crime syndicate recruited foreign students to steal and launder money

An Asian crime syndicate, which included an expert forgery artist, recruited foreign students to open bank accounts, steal mail and launder stolen cash. The students were among a number of third parties, also referred to as 'runners', enlisted to commit crimes for the syndicate.

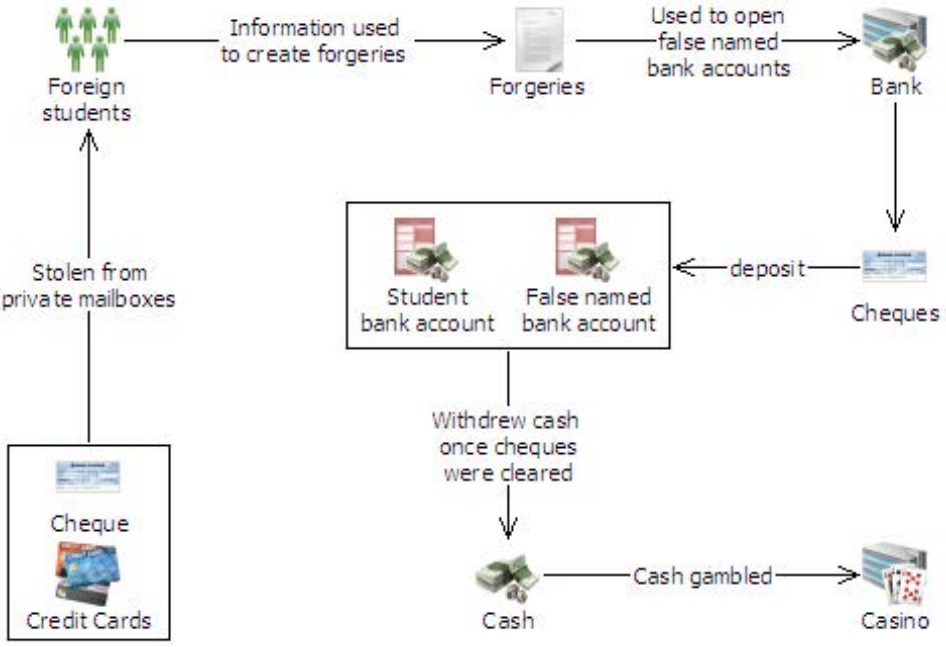
The scam began with the theft of cheques and credit cards from private mailboxes. The stolen documents were altered to create forgeries of sufficient quality to deceive bank tellers. The foreign students would deposit the cheques into their own bank accounts or accounts set up using false names.

When a cheque cleared, the money was withdrawn and gambled at casinos to mix or co-mingle it with legitimate cash – a common money laundering methodology.

An investigation uncovered more than 350 falsely named bank accounts that had more than AUD8 million laundered through them. Suspicious matter reports (SMRs) submitted by banks indicated that one member of the syndicate had made regular deposits below the AUD10,000 threshold for reporting cash transactions to AUSTRAC.

One suspect was arrested and charged with eight counts of dealing with the proceeds of theft. The individual had allegedly stolen a cheque for more than AUD500,000 from a deceased estate. The individual attempted to launder the proceeds of the fraudulently obtained cheque through a casino.

A second suspect was arrested and charged with six offences, including making a false document to obtain a financial advantage. A third suspect was also arrested and charged with identity fraud and money laundering offences.



Case 15 – Asian crime syndicate recruited foreign students to steal and launder money

Offence	Fraud Money laundering
Customer	Individual
Industry	Banking (ADIs) Gambling services
Channel	Electronic
Report type	SMR
Jurisdiction	Domestic
Designated service	Account and deposit-taking services Gambling services
Indicators	Customer making large cheque deposits despite having no known source of income Customer undertaking transactions that appear inconsistent with their profile and transaction history Large-value cheque deposits into newly opened, or student, bank accounts followed by immediate cash withdrawals once cleared Structuring of cash deposits to avoid reporting requirements Use of false identification to open bank accounts and conduct transactions

Case 16– Albanian crime syndicate used online betting service to launder drug proceeds

An Albanian organised crime syndicate operating in Australia used an online betting service and an internet payment system to launder illicit proceeds from the sale of cannabis. The syndicate used the two services together to receive international transfers and move funds offshore.

AUSTRAC identified an increase in international funds transfer instructions (IFTIs) to and from Albania which had originated from the same location in Australia. AUSTRAC analysed the IFTIs and identified a large network of entities.

AUSTRAC information revealed the two online services operating from the same physical address. A suspect transaction report (SUSTR) submitted to AUSTRAC identified a director of the internet payment system making domestic transfers to the online betting service. This link between the two services raised the possibility that the financial activity was an attempt to conceal the origin of illicit funds.

The network of entities used the internet payment system to:

- transfer value between members via online accounts
- act as a remittance service that used a domestic bank to conduct international funds transfers – since the resultant international funds transfer instruction recorded the 'remittance service' as the sending customer, this method camouflaged the identity of the actual ordering customer.

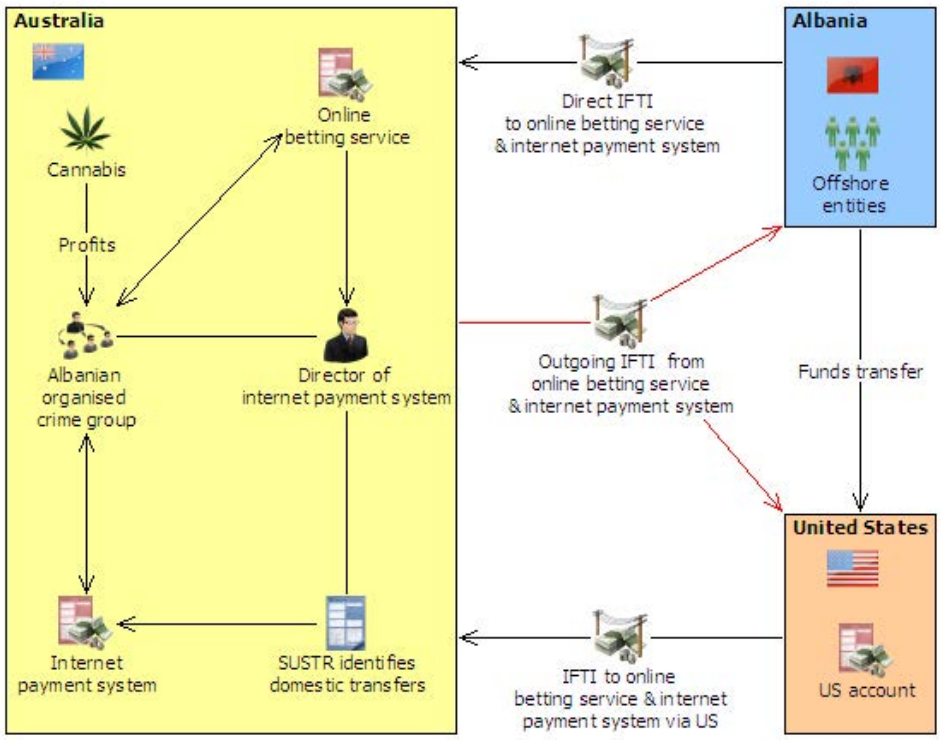
Similarly, the network used the online betting service to:

- store funds and make them accessible to other network members through sharing account passwords
- remit and receive international funds transfers
- create the illusion of paying 'gaming winnings' to members of the network and offshore entities, even though no inward transactions were recorded to justify an initial bet – analysis of this activity indicated the funds were not winnings but were for possibly illicit purposes.

The network also engaged in other suspicious transactions. The two online services transferred funds to customers in Sweden and the Philippines, but never received funds in return. The network also requested incoming international funds transfers of set, rounded-values (eg. AUD5,000) and in specific foreign currency amounts which were conducted over a single week. Large sums were transferred irrespective of any impact international foreign exchange rate changes may have had on these transactions.

Over an 18-month period the two online services received more than 600 incoming IFTIs valued at more than AUD26 million. Over the same period, they were recorded on AUSTRAC's database as having conducted more than 140 outgoing IFTIs worth more than AUD15 million. Funds were predominantly sent to and received from Albanian entities and were believed to be proceeds from the sale of cannabis. Analysis of the IFTIs revealed many of the customers of the two services had routed their payments via financial institutions in the United States in an attempt to further conceal the origin of the funds.

The 'Potential vulnerabilities' section of this report details the vulnerabilities of online gambling services and online methods of value transfer. The activities described in the case above demonstrate how different online platforms can be used in conjunction to manage criminal financial activity and conceal money trails.



Case 16– Albanian crime syndicate used online betting service to launder drug proceeds

Offence	Money laundering Drug trafficking
Customer	Business Individual
Industry	Remittance services Gambling services Banking (ADIs)
Channel	Electronic
Report type	IFTI SUSTR
Jurisdiction	International – Albania, the Philippines, Sweden, United States
Designated service	Remittance services (money transfers) Gambling services Account and deposit-taking services
Indicators	Company receiving and sending large value and volume of IFTIs inconsistent with their business profile Customer undertaking non-economic transaction Large value and volume of IFTIs to a high-risk jurisdiction Multiple incoming IFTIs at a set and/or rounded amount, transferee unconcerned about losing value due to foreign currency exchange rate changes

Case 17 – 'Bankrupt' suspect used casino to launder million dollar drug payments

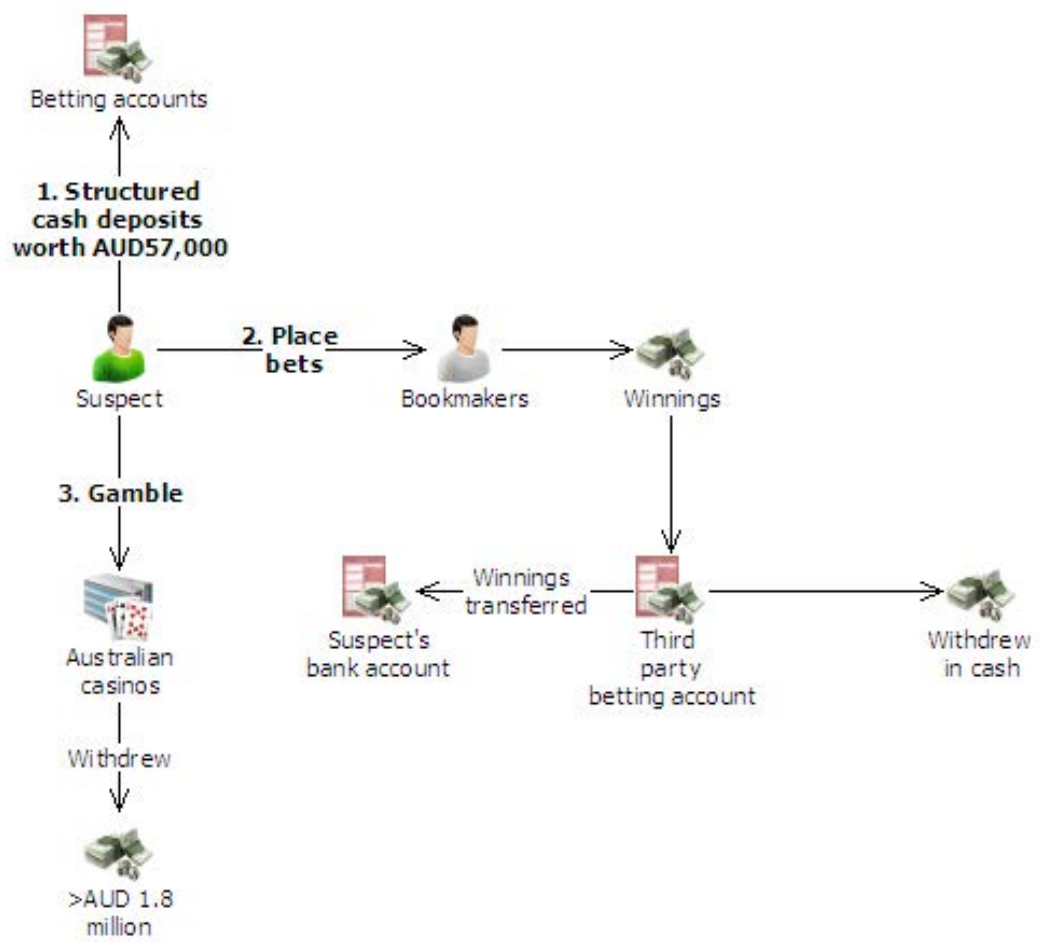
Law enforcement began an investigation into a known criminal identity who was suspected of being involved in numerous large-scale drug importations into Australia. The suspect was connected to criminal groups within Australia, including networks which provided specialised money laundering services. Analysis conducted by law enforcement authorities and AUSTRAC indicated that, despite being declared bankrupt, the suspect had deposited and withdrawn significant amounts of cash at Australian casinos and via betting accounts. These transactions in excess of AUD10,000 were reported to AUSTRAC. The suspect was also involved in the purchase and sale of race horses during the period of interest.

In 2007 AUSTRAC proactively disseminated a financial intelligence assessment to law enforcement agencies which detailed the suspect's gambling and betting activity at several casinos around Australia. AUSTRAC information identified:

- the suspect had conducted structured cash deposits worth approximately AUD57,000 into betting accounts
- minimal significant cash deposits made at Australian casinos, indicating that the suspect may have been structuring cash buy-ins at the casinos
- the suspect had begun using a betting account held in the name of a third party to layer illicit funds and place bets with registered bookmakers. The bookmakers returned any subsequent winnings to the third-party betting account, where the funds were withdrawn or transferred into the suspect's bank account
- suspect transaction reports (SUSTRs) submitted to AUSTRAC also provided further important information about the suspect. The suspect was the subject of an exclusion order prohibiting him from entering or remaining at a specific casino. The exclusion order related to one casino only. AUSTRAC information indicated the suspect withdrew more than AUD1.8 million in a series of large cash withdrawals at other Australian casinos. All of the withdrawals were gambling chip/token cash outs or payouts from electronic gaming machines.

Given the large amounts of cash the suspect was withdrawing from Australian casinos, authorities believed the suspect was moving illicit funds through Australian casinos in an attempt to disguise the withdrawn funds as legitimate winnings.

This matter became subject to a subsequent wider investigation into a major transnational network of drug trafficking syndicates.



Case 17 – 'Bankrupt' suspect used casino to launder million dollar drug payments

Offence	Drug trafficking Money laundering
Customer	Individual
Industry	Banking (ADIs) Gambling services
Channel	Physical
Report type	SUSTR
Jurisdiction	Domestic
Designated service	Account and deposit-taking services Gambling services
Indicators	Customer undertaking transactions which appear to be inconsistent with their profile and/or transaction history: Large casino chip cash-outs Large electronic gaming machine payouts Multiple cash deposits below AUD10,000 (i.e. 'structuring') Use of third-party gaming accounts

Case studies

Remittance services (money transfers)

4

Case studies – Remittance services (money transfers)

Case 18 – Suspicious overseas transfers helped unearth Colombian cocaine imports

AUSTRAC information alerted law enforcement authorities to the activities of a criminal syndicate involved in transferring large amounts of funds to South America. The law enforcement investigation led to three men being charged with drug-related offences for attempting to import cocaine to Australia.

The criminal syndicate came to the attention of AUSTRAC after a reporting entity submitted a suspect transaction report (SUSTR) detailing the financial activities of the group.

Within the SUSTR, the reporting entity staff detailed several grounds for their suspicions:

- The three suspects sent identical amounts of AUD2,000 in four transactions to four beneficiaries in the same city in Colombia, claiming the funds transfers were 'gifts'
- A fourth individual accompanied the three suspects as they made their international funds transfers, and they appeared to be acting under the guidance of that individual.
- Each of the three suspects gave their occupation as 'labourers', although this seemed inconsistent with their age and appearance.

AUSTRAC staff analysed financial transaction reports submitted by reporting entities that were linked to the criminal syndicate. AUSTRAC staff identified:

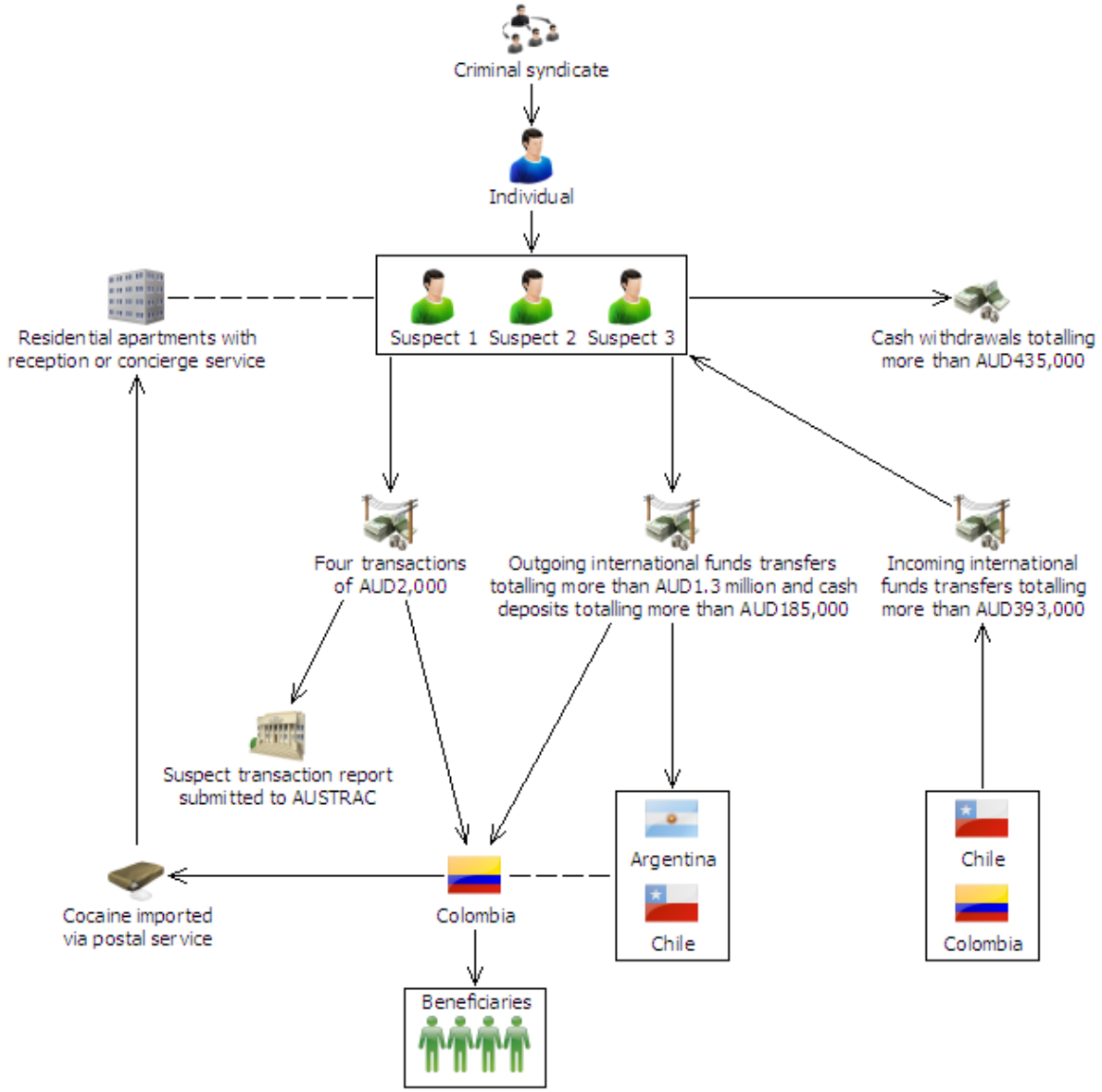
- 577 outgoing international funds transfer instructions (IFTIs) to Colombia, Argentina and Chile totalling more than AUD1.3 million
- 129 incoming IFTIs, including from Colombia and Chile, totalling more than AUD393,000
- 31 significant cash transaction reports (SCTRs) for withdrawals totalling more than AUD435,000
- 11 SCTRs for cash deposits totalling more than AUD185,000.

AUSTRAC information also identified the use of aliases by one of the suspects.

All IFTIs were made via remittance services. Authorities believe the funds sent to South America were used to purchase cocaine for import into Australia via the postal system.

Law enforcement authorities intercepted a package at an Australian mail centre. The package from South America contained cocaine hidden inside artwork. The cocaine had an estimated street value of AUD70,000.

The investigation traced the package to the three suspects. Following the execution of search warrants, the suspects were charged with possessing, trafficking and importing dangerous drugs. The suspects were convicted and sentenced to terms of imprisonment for seven years.



Case 18 – Suspicious overseas transfers helped unearth Colombian cocaine imports

Offence	Drug trafficking
Customer	Individual
Industry	Remittance services
Channel	Electronic
Report type	IFTI SCTR SUSTR
Jurisdiction	International – Argentina, Chile, Colombia
Designated service	Remittance services (money transfers)
Indicators	Customer explanation of 'reason for transfer' inconsistent with the particulars of the transaction and the customer's profile Customer undertaking transactions that appear inconsistent with their profile IFTIs being sent to individuals rather than an overseas business contact Multiple customers simultaneously conducting international funds transfers to the same destination city and country Multiple customers simultaneously conducting international funds transfers under the guidance or instruction of an individual Multiple international funds transfers to a high-risk jurisdiction

Case 19 – Money laundering remitter jailed after sending false reports to AUSTRAC

Law enforcement conducted an investigation into a remittance service provider suspected of falsifying customer information on transaction reports and submitting false information to AUSTRAC to facilitate money laundering.

AUSTRAC information was critical to the law enforcement investigation to help identify that the remitter and his remittance business had assisted a criminal syndicate with laundering the proceeds of identity fraud. The identity fraud involved money fraudulently withdrawn from the bank accounts of innocent third parties. A key element in the laundering of criminal proceeds involved the remitter disguising the funds and concealing the identity of members of the criminal syndicate.

The typical activity undertaken to launder the illicit funds involved:

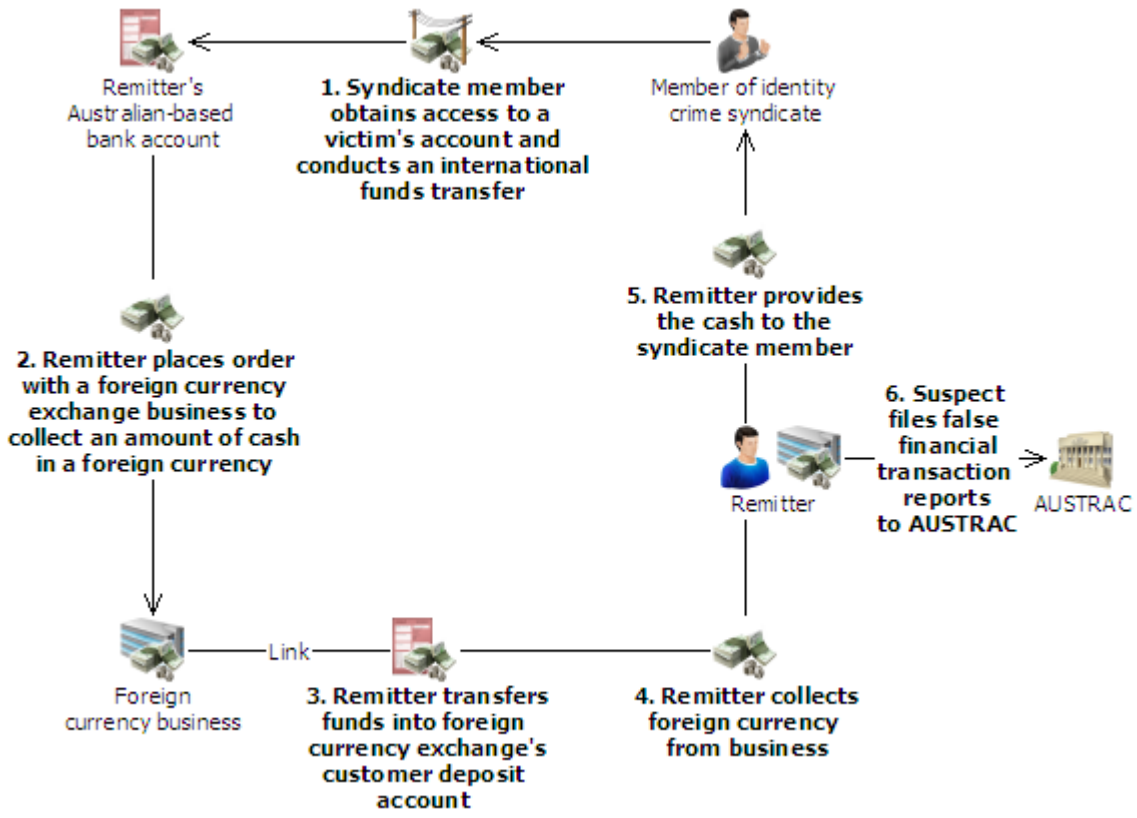
1. A member of the identity crime syndicate would obtain access to a victim's account and arrange for funds from the account to be sent as an international funds transfer instruction (IFTI) into an Australian account operated by the remitter.
2. The remitter would place an order with a foreign currency exchange business to collect an amount of cash in foreign currency equivalent to the value of the stolen funds.
3. Using the stolen money, the remitter would transfer funds into the foreign currency exchange's customer deposit account.
4. The remitter would visit the foreign currency exchange to collect the foreign currency.
5. With the original stolen funds now laundered into foreign currency, the remitter would provide the foreign currency, less a commission, to a member of the criminal syndicate.
6. As a last step in concealing the money trail, the remitter would file a significant cash transaction report (SCTR) with AUSTRAC detailing the payment to the syndicate member, but using false identification details to conceal the recipient's true identity from authorities.

Analysis of financial transaction activity by law enforcement, supported by AUSTRAC analysts, revealed the remitter had reported approximately AUD3.5 million in SCTRs over a two-year period. Further law enforcement investigation found that the majority of recipients recorded in these transaction reports could not be identified or did not exist. Over this same period, 15 foreign exchange transactions were reported to AUSTRAC totalling over AUD1.1 million. The value per transaction ranged between AUD10,000 and AUD 200,000.

AUSTRAC also received suspect transaction reports (SUSTRs) relating to the remitter's financial transactions with other reporting entities. Information within the SUSTRs, combined with further analysis of personal financial transactions undertaken by the remitter, revealed a range of suspicious activity, including:

- the remitter's reluctance to explain the source of funds to bank staff
- the depositing of large amounts of cash into an account followed by an international funds transfer on the same day
- the use of third parties to make international funds transfers on the remitter's behalf.

The law enforcement investigation collected evidence confirming the remitter was involved in money laundering on behalf of third parties. The remitter was charged and convicted on multiple counts of dealing with the proceeds of crime worth more than AUD100,000 contrary to section 400.4 of the *Criminal Code Act 1995*. The remitter was ultimately sentenced to five years and six months imprisonment, with a minimum of three years and seven months. The remitter was also charged and convicted of money laundering offences.



Case 19 – Money laundering remitter jailed after sending false reports to AUSTRAC

Offence	Fraud Money laundering
Customer	Business Individual
Industry	Banking (ADIs) Remittance services
Channel	Electronic Physical
Report type	IFTI SCTR SUSTR
Jurisdiction	Domestic International
Designated service	Account and deposit-taking services Remittance services (money transfers)
Indicators	International funds transfers sent directly to individuals rather than an overseas business contact Multiple entities, often linked via address or phone number, sending international funds transfers to the same overseas beneficiaries Significant increase in cash deposits received by the remitter Sudden increase in transactional activity inconsistent with the remitter's established business profile or transaction history Unauthorised account transfers Use of false identification

Case 20 – Australian and international law enforcement combined to dismantle ecstasy syndicate

Successful cooperation among state, federal and international law enforcement resulted in the dismantling of a major drug syndicate responsible for importing methylenedioxymethamphetamine (MDMA) – the powdered equivalent of ecstasy – into Australia. The international syndicate, coordinated by a suspect based in Montenegro, imported MDMA into Australia to manufacture ecstasy tablets.

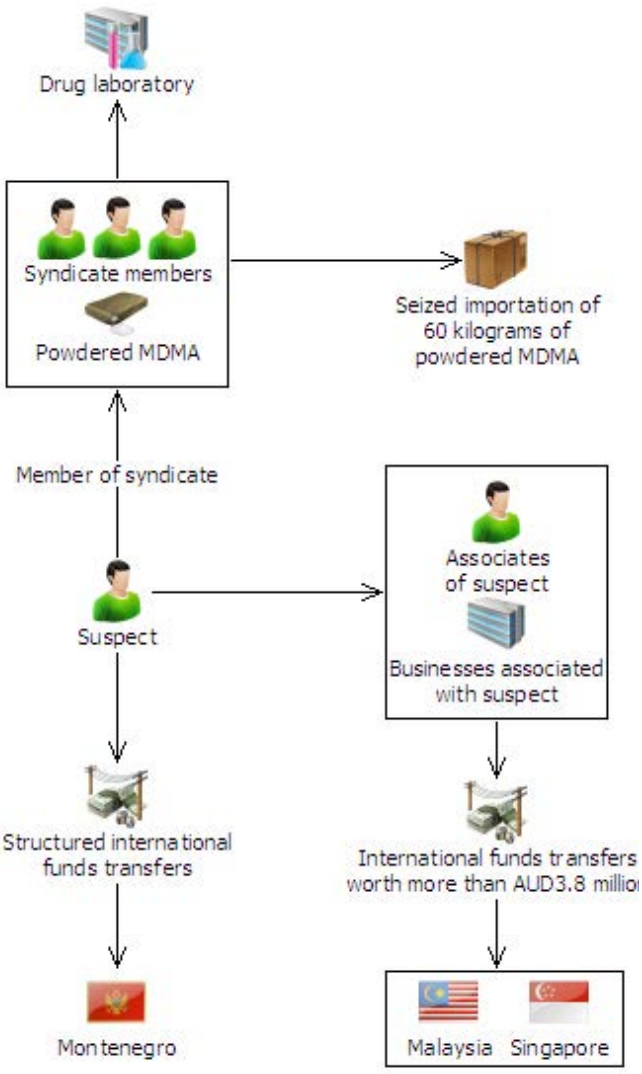
Four Australian suspects were arrested for their role in the operation, which led to the largest MDMA seizure recorded by a state police force in Australia. Following an investigation into a previous importation of 60 kilograms of powdered MDMA, a covert operation was set up by law enforcement to identify and disrupt the illicit activities of the perpetrators. Syndicate members were closely monitored and investigators uncovered an illegal drug lab with an estimated capacity of producing drugs worth AUD24 million. When authorities moved to arrest the syndicate members they seized a large quantity of powdered MDMA, with the potential to produce more than 350,000 ecstasy tablets.

AUSTRAC information revealed more information about the syndicate's activities:

- one of the suspects had undertaken two 'structured' international funds transfers to Montenegro. Both transfers were sent via remittance services within a five-day period
- individuals and businesses associated with the above suspect undertook outgoing international funds transfers (IFTIs) worth more than AUD3.8 million, predominately to Singapore and Malaysia.

The main suspect in the syndicate was charged with importing a commercial quantity of MDMA and conspiracy to traffic a commercial quantity of MDMA and was sentenced to 25 years on each charge, to be served concurrently.

The other three suspects were sentenced to between 14 and 17 years imprisonment for conspiracy to traffick a commercial quantity of MDMA.



Case 20 – Australian and international law enforcement combined to dismantle ecstasy syndicate

Offence	Drug Importation
Customer	Business Individual
Industry	Remittance Services
Channel	Electronic Physical
Report type	IFTI
Jurisdiction	Domestic International – Malaysia, Montenegro, Singapore
Designated service	Remittance services (money transfers)
Indicators	International funds transfers to a high-risk jurisdiction Structuring cash transactions (outgoing international funds transfers) to avoid reporting requirements

Case 21 – Australian terror suspects sent funds to Somalia to support terrorist group

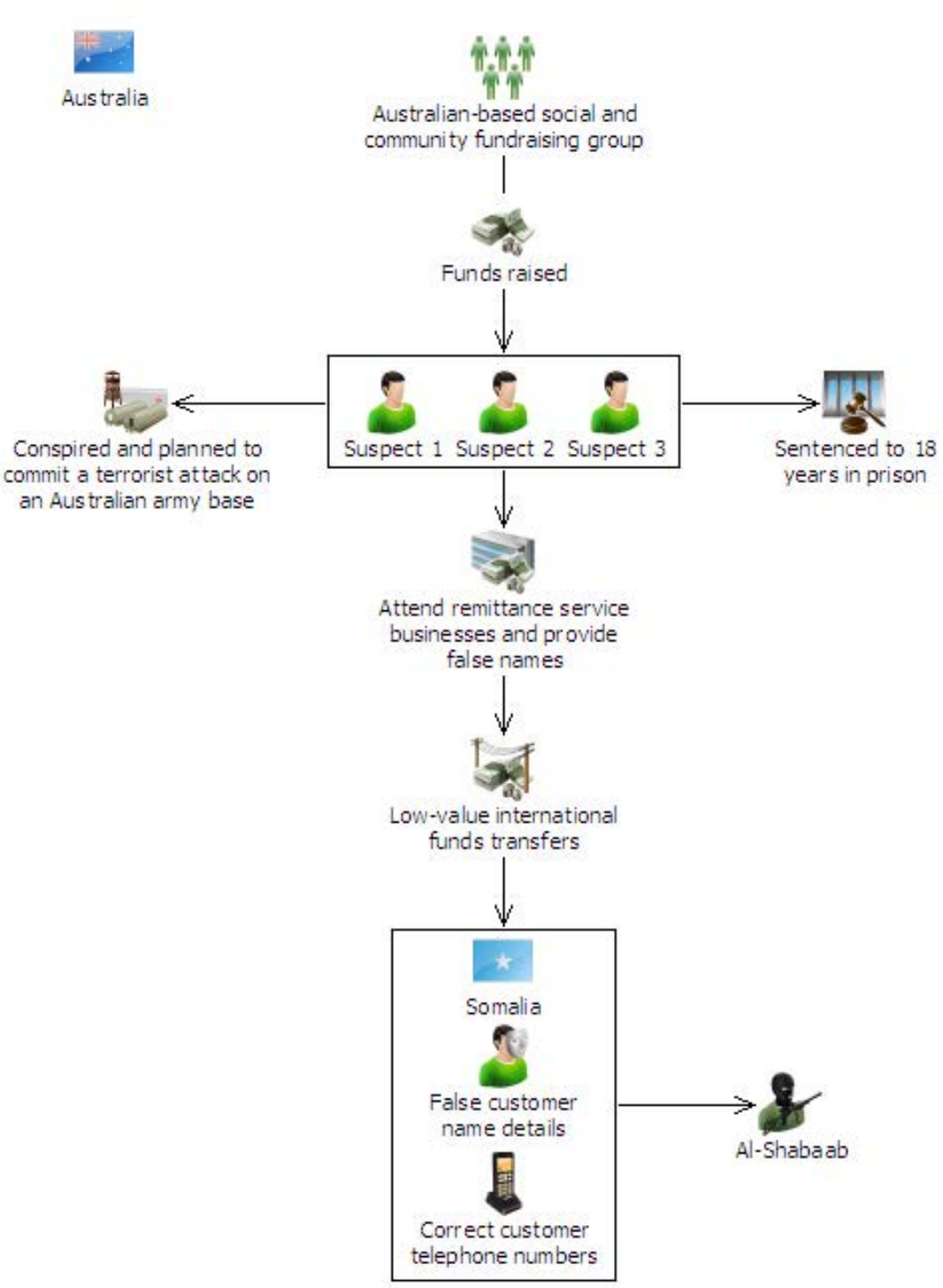
A joint-agency investigation led to the arrest of five suspects on charges of conspiring to commit a terrorist attack on an Australian army base. Investigations revealed the group had sent funds destined for use by the Somalia-based terrorist group, al-Shabaab. The group had also facilitated travel for Australian-based supporters to attend overseas military training camps. Funds remitted offshore by the suspects did not go directly to al-Shabaab but to entities linked to al-Shabaab's activities in Somalia.

Investigating officers, assisted by AUSTRAC information, discovered that the suspects had sent thousands of dollars in low-value IFTIs to Somalia. Authorities suspected these IFTIs were to support the aims of al-Shabaab and associated military training activities overseas.

The suspects sent the funds via remittance service businesses, often using false names for the overseas beneficiary customer to obscure the money trail. However, the telephone numbers recorded in the IFTIs for the overseas customers were correct. Investigating officers concluded that the suspects used the customers' correct phone numbers to ensure the funds arrived safely and were handed to the correct customer in Somalia. In this case, the information reported in the IFTIs was valuable intelligence for the investigation officers to use to corroborate other information or consider leads in the investigation.

In general, the group members paid for the remittances to Somalia using their own funds. The group also remitted funds that had been raised by Australian-based social and community fundraising groups – a common terrorism-financing method internationally. There was no evidence to suggest that members of the social and community groups involved were aware that the funds being raised were to be remitted to East Africa in support of al-Shabaab.

Three suspects were found guilty of conspiring to plan an Australian-based terrorist attack and sentenced to 18 years jail to serve 13 years and six months. Two of the suspects were found not guilty.



Case 21 – Australian terror suspects sent funds to Somalia to support terrorist group

Offence	Conspiring to plan a terrorist attack
Customer	Individual
Industry	Remittance services
Channel	Physical
Report type	IFTI
Jurisdiction	Domestic International – Somalia
Designated service	Remittance services (money transfers)
Indicators	Low-value international funds transfers to a high-risk jurisdiction Use of false identification when sending funds offshore

Appendix A & B
Case study index
Glossary & abbreviations

5

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 encourage further monitoring and examination. In most cases it is the existence of multiple indicators which raises a reporting entity's suspicion of potential criminal activity, and informs their response to the situation.

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

Money launderers and terrorism financiers will continuously 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 ensure their internal AML/CTF systems and training are effective.

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

- Account activity inconsistent with customer profile
- High-volume account activity involving significant amounts of cash funds
- Cash withdrawals conducted at various bank branches and/or ATMs on the same day
- Customer offering incentives to representatives of a financial institution to assist in bypassing AML/CTF procedures
- Customer receiving multiple large-value domestic transfers into their personal account from a company account, followed by an outgoing international funds transfer equivalent in value to the domestic transfers
- Customer submits an application to roll over funds from a superannuation account into a newly opened account and then conducts an international funds transfer shortly afterwards
- Significant value of funds rolled over into a recently opened self-managed superannuation fund (SMSF) account, followed by immediate cash withdrawals
- High-value cash deposits to pay for international funds transfers
- International funds transfers from an individual's account to several offshore accounts held in the same name
- Multiple customers conducting international funds transfers to the same overseas beneficiary
- Multiple low-value international funds transfers, possibly indicating a large amount of funds broken down into smaller amounts (scattering)
- International funds transfers to a high-risk jurisdiction
- Large value cheque deposits into newly opened bank accounts followed by immediate cash withdrawals once cleared
- Repeated requests for quick cheque clearances by customer
- Regular or multiple cash deposits just below the AUD10,000 cash transaction reporting threshold
- Regular or multiple purchasing and cashing of gaming chips just below the cash transaction reporting threshold
- Third parties involved in depositing and withdrawing funds at casino

Appendix B – References and websites

References

Attorney-General's Department, Canberra, 2011,
<www.nationalsecurity.gov.au>

Australian Taxation Office, 'Tax havens and tax administration' 2011, ATO,
<http://www.ato.gov.au/corporate/content.aspx?doc=/content/46908.htm&page=4&H4>

Financial Action Task Force (FATF), *Money Laundering using New Payment Methods*, FATF Paris, October 2010

Summary of websites

www.ag.gov.au

www.aic.gov.au

www.ato.gov.au

www.austrac.gov.au

www.crimecommission.gov.au

www.customs.gov.au

www.ema.gov.au

www.fatf-gafi.org

www.moneysmart.gov.au

www.nationalsecurity.gov.au

Case study index

	Case study no.
scams (inc. 'advance fee fraud', 'early access' superannuation scams)	5, 6, 8, 15
SCTRs (significant cash transaction reports)	2, 5, 7, 8, 10, 18, 19
securities market/investment services (designated service)	4
shell company	10
SMRs (suspicious matter reports)	8, 10, 12, 13, 14, 15
stolen funds	3
structuring (of transactions)	2, 5, 9, 13, 15, 17, 20
superannuation/SMSFs	4, 8
SUSTRs (suspect transaction reports)	2, 3, 5, 6, 8, 10, 13, 16, 17, 18, 19
taxation (evasion of, fraud)	2, 9, 10, 14
terrorism financing	21
third parties	2, 8, 13
TTRs (threshold transaction reports)	12, 13
unexplained income	5, 13, 17, 18, 19
weapons (explosives, firearms)	7, 9
wildlife smuggling	1

Glossary and abbreviations

Glossary

advance fee fraud	A scam, also commonly referred to as 'the Nigerian scam', in which victims are approached, usually by email, and deceived into forwarding 'advance fee' payments, or divulging financial information such as bank account details. These scams attract their victims with promises of overseas lottery wins, unexpected inheritances or government windfalls.
beneficiary (or beneficiary customer)	The person (or organisation) who is the ultimate recipient of funds being transferred.
black money scam	A scam in which criminals attempt to persuade victims to pay for 'special chemicals' which are required to wash cash that has been dyed to avoid detection by customs. The scammers claim that the victims can keep a portion of the tainted cash as long as they buy the required chemicals to clean it.
cash couriers	People who physically transport cash on their person or as part of their luggage between international jurisdictions. Couriers may be directly connected to the criminal activity and the proceeds of crime, or they may be third parties (or 'mules') recruited specifically for the task of moving the money offshore.
co-mingling	The process of combining the profits of illicit activities with the profits of a legitimate business to disguise the illicit funds and make them appear legitimate.

cross-border movement of physical currency (CBM-PC) reports	Under the AML/CTF Act, CBM-PC reports are submitted when currency (coin or paper money) worth AUD10,000 (or the foreign equivalent) or more is carried, mailed or shipped into or out of Australia: When a person carries currency of AUD10,000 or more into or out of Australia, a CBM-PC report must be completed at the first Customs examination area upon entry into Australia or before leaving Australia. When a person mails or ships currency of AUD10,000 or more 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.
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.
high-risk jurisdiction	'High-risk jurisdictions' are jurisdictions known to be a source 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
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.
layering	Layering is the second stage of the money laundering process, in which illegal funds or assets are moved, dispersed and disguised to conceal their origin. Funds can be hidden in the financial system through a web of complicated transactions.

methodology	The processes or methods used by criminals to conceal the origins of illicit funds or, in the case of terrorism financing, conceal the intended use of funds.
mules (third parties)	'Money mules' are third parties that are employed to transfer illicit funds between jurisdictions. They do this by either transporting physical cash or goods on their person or in their luggage; or undertaking transactions through a bank or remittance service or electronically. To avoid direct involvement in the money laundering process, criminals may use 'mules' to undertake certain high-risk transactions that might expose the criminals to law enforcement or regulatory bodies. The mules or third parties are recruited in a variety of ways and have varying levels of knowledge of illicit activity.
phishing	A type of internet-based scam in which criminals attempt to fraudulently obtain sensitive data from victims (for example, usernames and passwords for online banking) by posing as a trustworthy source (i.e. banks or government departments).
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 then used by the scheme's promoter to pay them 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.
predicate offence	Any offence which generates proceeds of crime.

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.
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.
shell company	A company that, at the time of incorporation, has no significant assets or operations. Shell companies can be set up domestically or offshore and the ownership structure of a shell company can take several forms. Shell companies have no physical presence, employees or products and may be owned by corporations, nominee owners and bearer shares, obscuring beneficial ownership.
significant cash transaction report (SCTR)	Under the FTR Act, a SCTR must be submitted to AUSTRAC in respect of a currency (coin or paper money) transaction involving AUD10,000 or more (or the foreign equivalent).
smurfing	'Smurfing' involves numerous third parties conducting transactions on behalf of criminals. Large cash amounts are broken into multiple smaller amounts and then given to third parties to deposit in accounts held in different financial institutions. These third parties may be complicit or unwittingly involved in this money laundering activity.

specialist 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.
structuring	This is 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.
suspicious matter report (SMR)	Under the AML/CTF Act, reporting entities must submit SMRs 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).
suspect transaction report (SUSTR)	Under the FTR Act, SUSTR must be submitted to AUSTRAC under the FTR Act when a cash dealer has reasonable grounds to suspect that a transaction may be relevant to investigation of an offence against an Australian law, including tax evasion and terrorism financing. For most reporting entities, SMRs (which fall under the AML/CTF Act) have replaced SUSTRs.
threshold transaction report (TTR)	Under the AML/CTF Act, if a reporting entity provides a designated service to a customer that involves the transfer of physical currency (or e-currency) of AUD10,000 or more (or the foreign currency equivalent), that entity must submit a TTR to AUSTRAC.

Abbreviations

ACC – Australian Crime Commission

ADIs – authorised deposit-taking institutions

AFP – Australian Federal Police

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

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

ATM – automatic teller machine

ATO – Australian Taxation Office

AUD – Australian dollars

AUSTRAC – Australian Transaction Reports and Analysis Centre

DCE – digital currency exchange

DHS – Department of Human Services

EUR – euro

FATF – the Financial Action Task Force

FIU – financial intelligence unit

FTR Act – *Financial Transaction Reports Act 1988*

GST – Goods and Services Tax

IFTI – international funds transfer instruction

MDMA – methylenedioxymethamphetamine, also known as 'ecstasy'

MLA 2011 – *Money laundering in Australia 2011*

NPM – new payment methods

NTA 2011 – *National Threat Assessment on money laundering 2011*

P2B – person-to-business

P2P – person-to-person

SCTR – significant cash transaction report

SMR – suspicious matter report

SMSF – self-managed superannuation fund

SUSTR – suspect transaction report

TTR – threshold transaction report

USD – United States dollar

How can I contact AUSTRAC?

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

For more information visit:

www.austrac.gov.au

07/12/CC