Australian Government

Australian Transaction Reports and Analysis Centre

AUSTRAC typologies and case studies report 2011

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 mission 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 that provide 'designated services' as outlined in section 6 of the AML/CTF Act. AUSTRAC also supervises 'cash dealers' and solicitors, 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 2011* 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.

Because of its transnational nature, serious organised crime is recognised as a national security threat that warrants a whole-of-government response. The 2009 Commonwealth Organised Crime Strategic Framework set the direction for a coordinated and cohesive approach to combating organised crime which guides AUSTRAC's work and the efforts of many of its partner agencies[1].

As an example, the Australian Crime Commission's Financial Intelligence Assessment Team (FIAT) facilitates a whole-of-government approach to financial information sharing and coordination, collaborative operational targeting and the development of strategies to respond to organised crime threats. As a member of FIAT, AUSTRAC directly contributes to law enforcement operations and provides ongoing support to its law enforcement partner agencies[2].

Launched in July 2010, the Australian Crime Commission's (ACC) Criminal Intelligence Fusion Capability builds on the successful FIAT model. AUSTRAC staff seconded to the ACC apply their expertise in analysing financial data to support operational outcomes.

---

1 AUSTRAC, *AUSTRAC Intelligence Strategy 2010–12*, <http://www.austrac.gov.au/is_2010_12_strategy.html>

2 FIAT member agencies are the Australian Customs and Border Protection Service, Australian Federal Police, Australian Securities and Investments Commission, AUSTRAC, Australian Taxation Office, Centrelink, the Department of Immigration and Citizenship (DIAC) and the Australian Crime Commission (ACC).

The Fusion Capability maximises the use of the full range of data held across a range of government agencies and boosts the ability of law enforcement agencies to identify 'high-risk' cash flows, patterns of crime, and the individual, business and corporate structures that may be involved in serious and organised criminal enterprises in Australia and overseas[3].

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 law enforcement agencies working together and sharing information about criminal groups.

Industry's contribution to combating money laundering and terrorism financing

This report is designed 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. It contains case studies detailing investigations and operations by AUSTRAC's partner agencies. As with previous reports in this series, AUSTRAC acknowledges the valuable contribution made by partner agencies in the preparation of this publication.

AUSTRAC also encourages future contributions from industry to assist in developing overall knowledge of AML/CTF in Australia, and to demonstrate how a robust AML/CTF framework benefits industry by assisting reporting entities to manage their own money laundering and terrorism financing risks.

3 Australian Crime Commission, Canberra, 2011, viewed 29 June 2011, <http://www.crimecommission.gov.au/media/faq/fusion.htm>

Report methodology

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.

In preparing this report, AUSTRAC acknowledges its use of publicly available information such as the ACC report, *Organised Crime in Australia 2011*, the Department of the Prime Minister and Cabinet *Counter-Terrorism White Paper Securing Australia – Protecting our Community*, and the Australian Competition and Consumer Commission report, *Targeting Scams: Report of the ACCC on scam activity 2009*. A full list of sources used is included in Appendix B of this report.

AUSTRAC also acknowledges its use of information obtained from the Attorney-General's Department, Australian Institute of Criminology and the Queensland Police Service to complement research undertaken by AUSTRAC analysts into money laundering and terrorism financing risks and methodologies.

This report identifies some key methods that have been used in Australia to conceal the origins of illicit funds or, in the case of terrorism financing, conceal the intended use of funds.

The case studies presented in this report have been approved by our partner agencies for external use.

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

- **Offence** – the criminal or civil offence involved (these do not necessarily represent actual charges brought against the perpetrators).
- **Customer** – the type of customer/s involved in the offence (this can be an individual, business or foreign entity).
- **Industry** – the industry through which transactions were conducted (some cases involve multiple industries).
- **Report type** – where relevant, the types of financial transaction reports submitted by 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 offshore) where the transactions originated or were undertaken.
- **Designated service** – the category of 'designated service', 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 the indicators identified in this report can be found in Appendix A.

Typologies

Australia continues to see sophisticated and well-organised criminal syndicates exploiting weaknesses in business products and services to launder the proceeds of illicit activities and to commit financial and other serious crimes.

Advances in technology and increased globalisation, combined with the diversification, sophistication and transnational nature of organised crime, are some of the issues that shape current and emerging threats to the financial environment.

The first section of this report examines the particular typologies used to commit serious transnational crimes: fraud, terrorism financing, and people smuggling and human trafficking.

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 previous reports at www.austrac.gov.au/typologies.

Fraud

Criminals continue to exploit legitimate services offered by reporting entities to perpetrate scams and frauds.

There are many examples of the extent to which scammers are willing to go in order to attract potential victims. While the general public is becoming more aware of scams, the variety and level of sophistication of scams continues to create challenges. Frauds generally incorporate, run parallel to, or underpin criminal activities such as money laundering.[4]

Case studies 9 and 12 in the report demonstrate how AUSTRAC and law enforcement agencies work together and share information about scams and frauds.

'Boiler room' scams

The name 'boiler room' originates from the high-pressure, aggressive selling techniques employed by the perpetrators.

Boiler room scams involve the illegal and/or aggressive selling of worthless or overpriced shares, or shares traded in limited volumes or markets. Boiler room fraud is generally highly organised, spanning multiple jurisdictions and can involve the use of sophisticated technology and identity fraud.

The Australian Crime Commission report, *Organised Crime in Australia 2011*, estimates that millions of dollars have been lost in Australia to boiler room scams. In one case alone, featured in AUSTRAC's 2010 typologies and case studies report, Australian victims lost AUD21.5 million to such a scam. Other recent reports of such scams indicate that the intended victims were contacted by phone and referred to well-designed – but bogus – websites in an attempt to convince them that the proposed investment was genuine.

Australian businesses and the public can remain vigilant to the emergence of new boiler room scams by using publicly available information published by Australian regulators, including the names of overseas and Australian based-businesses known to have made unsolicited investment calls to Australians. For example, the Australian Securities and Investments Commission (ASIC) 'Money Smart' website includes a list of 'Companies you should not deal with': <www.moneysmart.gov.au/scams/companies-you-should-not-deal-with>.

4 Australian Crime Commission, *Crime Profile Series – Frauds*, ACC, Canberra, 2011, viewed 25 May 2011, <www.crimecommission.gov.au/publications/crime-profile-series/frauds.htm>

Indicators for industry

Industry should remain alert to patterns of financial transactions which may indicate a boiler room scam is in operation. Particular indicators reporting entities should look for include:

- multiple customers sending international funds transfers to the same overseas beneficiary
- multiple international funds transfers sent to the same beneficiary in one day
- high-value international funds transfers
- u-turn transactions, involving funds being transferred out of Australia and then part of those funds being transferred straight back into the country.[5]

Advance fee fraud

'Advance fee fraud' originated in Nigeria in the mid-1980s. When Nigerian authorities became aware of the extent of this fraud activity, and its negative impact on legitimate Nigerian businesses, the Nigerian government introduced section 419 of the Nigerian Penal Code to prohibit advance fee fraud. This type of fraud is now often referred to as '419' advance fee fraud[6].

A number of Australians have fallen victim to these scams. Despite its origins, advance fee fraud is not limited to Africa and is now conducted from a number of other regions, including South-East Asia, Central Asia and Europe.

How does advance fee fraud work?

Advance fee fraud involves an unsolicited invitation to potential victims to invest funds, usually with the promise of significant financial returns. The scams lure potential victims by offering them a range of benefits. These may include money, prizes, gifts or employment – none of which actually exist.

After responding to the initial contact from the scammer, which normally comes via email, victims of the scams enter into correspondence with the scammer. After a period of time, the scammer asks the victim to transfer funds offshore – the amount requested is often small at first, but usually increases over time. In return for the offshore transfers, the victim is promised a large financial return.

The scammers aim to single out the victim and make them feel as if they have been personally selected to take part in an exclusive, profitable deal. By providing falsified documents – often in the form of government or other official documents – the scammer gains the victim's confidence as to the legitimacy of the arrangement.

Once the victim is committed to the fraud, the scammer may indicate that a problem has occurred with the arrangement. At this stage the victim may be pressured into providing further funds in order to ensure the arrangement can continue as promised.

A typical advance fee fraud methodology

Advance fee frauds are evolving and the methodologies used by scammers reflect advances in technology and global communication. Increased computer ownership, internet use and cheap and effective worldwide communication have facilitated growth in global scams. Scammers can now contact victims worldwide while disguising their true locations and identities.

---

5 See the Glossary for a definition of 'u-turn transactions'

6 United States Department of State, *Nigerian Advance Fee Fraud*, United States Department of State, Washington, 1997, <www.state.gov/documents/organization/2189.pdf>

Below is an example of how a typical advance fee fraud may operate:

- The scammer contacts the intended victim – normally via email, often using a free email provider such as Gmail or Hotmail – claiming to be a representative of an overseas government agency or a solicitor. The email may be written in poor English and include grammatical errors.
- The scammer asks for the victim's assistance in moving a substantial amount of money out of the scammer's country, often claiming that the money is trapped in banks due to civil wars or government restrictions.
- The scammer advises that they intend to forward the money to the victim's bank account, and that the victim will be able to retain 10 to 20 per cent of the funds as payment for their assistance.
- However, the scammer also informs the victim that, before they can transfer the funds, the victim will first need to pay various 'transfer costs', such as the cost of anti-terrorist certificates, taxes or storage expenses.
- The victim pays the transaction costs as instructed by the scammers – the victim's money and the scammers disappear and the scam is complete.

In Australia, advance fee fraud continues to represent a vulnerability for industry and the broader community as individuals continue to fall victim to such scams and use international banking and remittance services to send funds to the scammers. Figures released by the Queensland Police Service suggest that fraud by computer rose by 26 per cent from 2008–09 to 2009–10[7]. In 2009 alone, more than AUD600,000 was sent offshore each month by Queensland residents who had fallen victim to advance fee frauds[8].

Recent developments in advance fee frauds include:

- After originating in Nigeria and other West African nations (such as Ghana and the Ivory Coast), advance fee fraud is increasingly being detected in other regions, including Asia (in particular, Hong Kong and Malaysia), the United Kingdom and the United Arab Emirates.
- Major world events, such as the global financial crisis or natural disasters, have seen a growth in advance fee frauds that target businesses. The 2011 Queensland floods, for example, provided an opportunity for scammers to employ advance fee fraud tactics to exploit the vulnerabilities of unsuspecting victims. They did this by claiming to be tradespersons offering to repair damaged buildings, but demanding payment for their services in advance.[9]
- Technological advances and transnational crime have prompted an increase in online advance fee fraud. Scammers use online classified websites to target online consumers worldwide by advertising cheap prices for products (such as electronic goods) to entice victims. When the victim orders the product, the scammer informs them that there are 'additional' costs, such as postage, which must be paid in advance. The scammers may also ask the victim to pay upfront costs, such as shipping, before the product is delivered.

---

7 Queensland Police Service, *2009–2010 Annual Statistical Review*, Queensland Police Service, Brisbane, 2010, <www.police.qld.gov.au/services/reportsPublications/statisticalReview/0910/default.htm>

8 Queensland Police Service, *Advance Fee Fraud project launched*, media release, Queensland Police Service, Brisbane, 28 August 2009, viewed 8 June 2011, <www.police.qld.gov.au/News+and+Alerts/Media+Releases/2009/08/28fraud.htm>

9 Murdoch, L, '"Vultures" descend on victims with scams', *Brisbane Times*, 17 January 2011, viewed 20 May 2011, <www.brisbanetimes.com.au/environment/weather/vultures-descend-on-victims-with-scams-20110116-19sm0.html>

Indicators for industry

Below are some indicators which may alert reporting entities to transactions associated with international advance fee fraud:

- International funds transfers sent to recipients in locations such as Africa, the United Arab Emirates, Malaysia and the United Kingdom, despite the recipients' names not being traditionally associated with that country. Rather, the recipients or scammers use a mix of native and Anglo-Saxon names in order to appear authentic.
- A series of recurring low-value international funds transfers conducted in amounts below AUD300 (totalling between AUD1–5,000). The aim of the fraud is to conduct recurring low value transactions in order to avoid detection. The transfers are usually made via remittance services, but may occasionally be made from an individual's personal bank account.

Scammers target individuals regardless of age, gender, education or income level and some scams have specifically targeted small businesses. Further information and advice regarding advance fee frauds and related scams can be obtained from the Australian Competition and Consumer Commission 'SCAMwatch' website (www.scamwatch.gov.au), and ASIC's MoneySmart website (www.moneysmart.gov.au).

Terrorism financing

The Australian Government's *Counter-Terrorism White Paper: Securing Australia – Protecting our Community* identifies terrorism as an ongoing threat which poses a serious security challenge to Australia[10].

Partner agency response to terrorism financing

Australia's response to the threat of terrorism involves every level of government. It entails the creation of effective laws and collection of intelligence, together with national defence, law enforcement, aviation, border control and maritime security activities[11].

Financial intelligence can play a significant role in identifying and prosecuting individuals involved in terrorism financing. Law enforcement agencies utilise AUSTRAC data to not only track financial transactions, but also to identify relationships between suspects. The more detailed and accurate the transaction information reported to AUSTRAC, the more value this information has to these agencies.

In addition, AUSTRAC has agreements in place with many overseas counterparts for sharing financial intelligence, and works cooperatively with these partners to share and develop expertise and contribute to global action against terrorism financing, as well as money laundering and other serious crime.

The *AUSTRAC typologies and case studies report 2010* detailed a number of possible methods of terrorism financing, including:

- the use of an individual's or a group's own income for logistical funding or to fund actual terrorist attacks
- the collection of donations from witting or unwitting donors, including through charitable organisations and/or community groups
- the use of formal bank transfers to move funds internationally
- undertaking international funds transfers through formal, non-bank remittance service providers (remittance service providers)
- undertaking international funds transfers through informal, cultural-based remittance arrangements (for example, 'hawala'[12])
- the use of cash couriers – passengers who physically carry cash when they travel abroad.

10 Department of the Prime Minister and Cabinet, *Counter-Terrorism White Paper: Securing Australia – Protecting our Community*, Department of the Prime Minister and Cabinet, Canberra, 2010, <www.dpmc.gov.au/publications/counter_terrorism>

11 Attorney-General's Department, Canberra, 2011, viewed 8 June 2011, <www.ag.gov.au/www/agd/agd.nsf/Page/National_security>

12 See the Glossary for a definition of 'hawala'.

AUSTRAC's role

Case study 1 within this report demonstrates how following the money trail can lead to successful outcomes in detecting and dismantling Australian terrorist cells.

Emerging methodologies of terrorism financing

Since the release of AUSTRAC's 2010 typologies and case studies report, law enforcement and intelligence agencies have observed further patterns and activities relating to terrorism financing, including:

- individuals, often sharing the same cultural background, using their personal bank accounts to transfer funds offshore to provide support for terrorism activities overseas
- individuals using false names to undertake international funds transfers, particularly to high-risk jurisdictions[13]. This may include an individual of one gender giving instructions that an international funds transfer be carried out in the name of an individual of the opposite gender
- foreign nationals coming to Australia for a specific time frame to raise funds to support overseas terrorist organisations. Typically, these individuals only stay in Australia for short period of time – usually no longer than one month
- offenders undertaking card 'skimming' on EFTPOS and automatic teller machines (ATMs) to generate funds to support terrorist organisations or activities.

Reporting entities must submit a suspicious matter report (SMR) to AUSTRAC detailing any financial activity they consider suspicious. Where the suspicion relates to the financing of terrorism, an SMR must be made to AUSTRAC within 24 hours of the suspicion being formed.

13 Refer to the Glossary for a definition of 'high-risk jurisdiction'.

People smuggling and human trafficking

The terms 'people smuggling' and 'human trafficking' are sometimes used interchangeably and both terms refer to irregular entries into a country or state. However, there are some notable differences between the two:

- Consent – In most instances of people smuggling, the individual being smuggled has consented to being transported across a national border. Conversely, victims of trafficking have either not given their consent, or, where that consent has been given, it has been given under coercion.
- Exploitation – The relationship between people smugglers and those being smuggled generally ends when irregular maritime arrivals reach their ultimate destination. In some instances irregular arrivals can not raise the entire fee to pay the cost of the smuggling operation in advance, and in these circumstances the they may have to work off debts after they arrive at their destination; this may involve them working for the people smuggling syndicate in some form.

  Victims of human trafficking are generally subject to ongoing exploitation (often through sexual servitude or bonded labour) by the trafficker or associated parties after reaching their destination.
- Transnational movement – People smuggling involves the movement of people across international borders, whereas human trafficking may involve the movement of victims within a country's borders, as well as across them.
- Source of profit – People smugglers profit from the payments they receive for providing the service of smuggling people into another country. Perpetrators of human trafficking derive their profits from the continuing exploitation of the victims.

Partner agency response to people smuggling and human trafficking

As part of their response to these threats, Australia's national intelligence and law enforcement agencies investigate the financial activity of individuals and groups suspected to be involved in people smuggling and human trafficking.

The establishment of national people smuggling strike teams and ACC Criminal Intelligence Fusion Capability has further enabled AUSTRAC's partner agencies to investigate people smuggling and human trafficking syndicates. These agencies use AUSTRAC information, including financial transaction reports and SMRs, to inform their enquiries and investigations.

AUSTRAC works as part of a whole-of-government approach in tackling people smuggling and human trafficking activities. Key terminology associated with these crime types includes:

- Source country – the country from which an irregular maritime arrival originally departed
- Transit country – an intermediary country, from which irregular arrivals begin their passage to Australia.

AUSTRAC provides financial intelligence to assist authorities to detect, monitor and disrupt people smuggling and human trafficking syndicates, as highlighted by cases 5 and 15 in this report. Partner agencies also use this information to warn industry about vulnerabilities that may expose reporting entities to the risk of being misused for people smuggling and human trafficking.

People smuggling

The United Nations Office on Drugs and Crime (UNODC) defines people smuggling (or 'migrant smuggling') as:

> 'a crime involving the procurement for financial or other material benefit of illegal entry of a person into a State of which that person is not a national or resident.'

The Australian Federal Police has identified people smuggling as a major threat to Australian borders.[14]

Indicators for industry

Australian law enforcement agencies have identified a number of indicators associated with people smuggling. In isolation, these indicators may not necessarily indicate illicit activities. However, where multiple indicators exist, it may suggest the misuse of the Australian financial system to facilitate people smuggling:

- People smuggling ventures may be funded through several low-value international funds transfers, often to a common overseas beneficiary. These transfers may be sent by (apparently) unrelated customers, who may share the same ethnic background.
- Funds transfers related to people smuggling may be sent to countries with no apparent commercial connection to the activities of the customer transferring the funds.
- People smuggling facilitators may insist that the identification documents of those being smuggled are destroyed to prevent them being used to trace their source country. Consequently, identification documentation used by these individuals to establish accounts or transfer funds offshore after their arrival in Australia may be fraudulent or not represent their true identity. Reporting entities should be vigilant when individuals who have recently arrived in Australia report that their identification documentation has been destroyed or lost.

Human trafficking

Internationally, human trafficking represents a lucrative trade for criminal organisations and syndicates. Australia is not immune from human trafficking and is a destination country for victims of trafficking from at least Thailand, Malaysia, and the Republic of Korea[15].

The UNODC defines 'human trafficking' as:

> an act of recruiting, transporting, transferring, harbouring or receiving a person through a use of force, coercion or other means, for the purpose of exploiting them.

UNODC warns that 'human trafficking is one of the fastest growing transnational organised crimes', and notes that the exploitation of trafficking victims can include prostitution or other forms of sexual exploitation, and the forced provision of labour or services[16].

---

14 Australian Federal Police, Canberra, 2011, viewed 29 June 2011, <www.afp.gov.au/policing/human-trafficking/people-smuggling.aspx>

15 Attorney-General's Department, Canberra, 2011, viewed 3 May 2011, <www.ag.gov.au/www/agd/agd.nsf/page/PeopleTrafficking_PeopleTrafficking>

16 United Nations Office on Drugs and Crime, Vienna, 2011, viewed 3 May 2011, <www.unodc.org/unodc/en/human-trafficking/what-is-human-trafficking.html?ref=menuside>

Although human trafficking is difficult to detect, Australian law enforcement and intelligence agencies have made a number of observations about the methodologies used by human trafficking syndicates domestically and offshore, including those used to recruit victims:

- Victims trafficked into Australia often incur a 'bond' or 'contract' (known as 'debt bondage')with the offshore or Australian-based facilitator. The victim is compelled to stay in servitude until they have 'paid off' their debt, in accordance with the terms of the debt bondage contract.
- Human traffickers may use high-quality false documentation and passports to facilitate a victim's arrival into Australia.

Indicators for industry

AUSTRAC and its partner agencies have identified indicators which may suggest to reporting entities the misuse of their services to fund human trafficking operations and launder the profits of these operations:

- Individuals in Australia may send low-value international transfers via remittance and formal banking services to offshore human trafficking facilitators, including to a number of different offshore beneficiaries. These facilitators are often located in source countries, and receive the low-value transfers as partial payments for their services.
- An individual may act as a signatory on newly established bank accounts opened by victims based in Australia. These syndicate members generally act as a signatory on multiple accounts opened by different victims of trafficking.
- Victims may be accompanied by a third party when attending a bank or remittance service to facilitate the transfer of profits out of Australia to members of the trafficking network overseas.
- Cash-based businesses may be used to 'co-mingle'[17] illicit funds with the legitimate funds generated by the businesses. In a number of human trafficking cases, the victims have been 'employed' in apparently legitimate businesses.
- Those involved in human trafficking may deposit their illicit funds into bank accounts as 'structured'[18] cash deposits, to ensure the deposits fall below the cash transaction reporting threshold.

17 See Glossary for a definition of 'co-mingling'

18 See Glossary for a definition of 'structuring'.

Case studies – Account and deposit-taking services

Case 1 – Suspects raised funds in preparation for acts of terrorism

Funds associated with the financing of terrorism can be derived from legitimate sources, including the incomes of individuals or community donations, or through the proceeds of non-terrorism related crimes (including fraud or robbery). By using a diversity of funding sources, those planning acts of terrorism may attempt to distance themselves from the origin of the funds generated to finance those acts.

The following two related cases illustrate the challenge of identifying terrorism financing, given that it may model normal patterns of financial behaviour, be undertaken through low-value transactions, or not involve the financial sector at all.

Part A – Sydney

A joint investigation led to the arrest in November 2005 of nine Sydney suspects who authorities suspected were planning an act of terrorism in conjunction with thirteen Melbourne suspects. The group's activities included military-style training and purchasing materials they planned to use to manufacture explosives.

The investigation revealed that the Sydney-based suspects relied mainly on their own incomes and efforts to fund their training activities and purchases, using their own bank accounts. Members of the group were caught shoplifting batteries, maps and electronic timers. Investigating officers also located stolen railway detonators during the execution of search warrants.

The Sydney suspects regularly used false names to register mobile phones when purchasing supplies and materials for their activities. For example, members of the group established companies in false names and used these companies to avoid suspicion when ordering and purchasing chemicals.

Four members of the Sydney group pleaded guilty to various terrorism offences, while the remaining five members were found guilty by a jury of conspiring to commit an act in preparation for a terrorist attack under the *Criminal Code Act 1995*.

Offence	Terrorism
Customer	Individual
Industry	Banking (ADIs)
Report type	SCTR
Channel	Physical
Jurisdiction	Domestic
Designated service	Account and deposit-taking services
Indicators	Low-value payments undertaken through accounts and low-value cash withdrawals (below the AUD10,000 threshold) Use of false identification to establish Australian companies

Part B – Melbourne

The same joint investigation also led to the arrest of thirteen Melbourne suspects who, in conjunction with the Sydney suspects, were planning an act of terrorism. The Melbourne group also undertook military-style training and purchased materials to manufacture explosives.

Investigations revealed that the Melbourne-based group funded their planned activities primarily through a series of small cash donations made by the group members to a central fund, known as the 'sandooq' (traditionally a box where all financial contributions were held). The majority of the Melbourne group were employed as electricians, tilers or panel beaters.

One individual was alleged to have been the treasurer and holder of the sandooq. Another group member approved group members to use funds from the sandooq. All members contributed to the sandooq, with some contributing AUD100 per month. The fund was worth approximately AUD19,000 at the time the group was arrested.

The suspects were also engaged in systematic credit card fraud, whereby they paid taxi drivers to provide them with the credit card numbers of unsuspecting taxi passengers. In addition, third parties provided the group with extra funds raised from a car re-birthing racket.

The group undertook the fundraising activities for the purpose of purchasing weapons and materials for a planned terrorist attack.

Nine members of the Melbourne group were found guilty of being members of a terrorist organisation. Four members were acquitted. Seven group members were also found guilty of committing acts in preparation for a terrorist attack under the *Criminal Code Act 1995*.

Offence	Terrorism
Customer	Individual
Industry	Banking (ADIs)
Report type	SCTR
Channel	Physical
Jurisdiction	Domestic
Designated service	Account and deposit-taking services
Indicators	Multiple individuals contributing cash to a central fund (sandooq) Frequent contributions made to the sandooq by members of the group and through proceeds of business activities Individual members contributed up to AUD100 per month

Case 2 – Suspects paid for Armenian cocaine shipments with international transfers

An investigation uncovered a major drug smuggling operation after law enforcement officers identified that a number of suspects under investigation had transferred more than AUD100,000 out of Australia.

One of the suspects was subsequently arrested while attempting to transfer AUD100,000 to Armenia through a bank. The suspect had attempted to pay for the international funds transfer with cash.

Following the suspect's arrest, the group's regular funds transfers to Armenia ceased for a period of time. When the group recommenced sending funds to Armenia, they employed a different method to transfer funds in an attempt to avoid detection by authorities. The method included:

- funds being transferred overseas in the last week of each month
- international funds transfers being conducted through banks and paid for with cash. However, the cash payments for these transfers were seemingly structured into amounts of less than AUD10,000 to avoid the cash transaction reporting threshold
- four individuals from the group sending funds overseas at the same time. The group would travel to one suburb and transfer the funds through various branches of different banks within that suburb
- funds always being sent to the same branch of the same Armenian bank.

Over a four-year period the group transferred nearly AUD1.8 million to Armenia.

Authorities believe the transferred funds were subsequently sent to the United States, where they were used to purchase cocaine for importation into Australia.

The group owned a number of auto body repair shops in Sydney, and the cocaine was shipped into Australia hidden inside automobile brake drums. Authorities also believe that the group used brake drums to smuggle cash out of Australia.

Ultimately, two members of the group were arrested and sentenced to six years imprisonment for possession of a marketable quantity of imported cocaine.

Offence	Drug trafficking
Customer	Individual
Industry	Banking (ADIs)
Channel	Electronic Physical
Report type	SUSTR IFTI SCTR
Jurisdiction	International – Armenia, United States
Designated service	Account and deposit-taking services
Indicators	High-value cash deposits to pay for international funds transfers International funds transfers conducted at the same time each month International funds transfers conducted through banks and paid for in cash Cash deposits structured to fall beneath reporting threshold Third-party individuals making large cash deposits into accounts Multiple high-value international funds transfers to a country of interest to authorities Multiple customers conducting international funds transfers to the same overseas beneficiary

Case 3 – Jail for suspects who extorted victim for three years

A law enforcement investigation into blackmail and extortion attempts resulted in the arrest of two suspects, who were both later found guilty of multiple charges.

Suspect A and Suspect B extorted money and other assets from a victim over a period of three years by threatening the victim, the victim's family, and their property. The extortionists' demands against the victim were initially small, but grew over time to include cash, company shares and luxury motor vehicles.

The victim made cash payments to the suspects and electronically transferred funds directly into the suspects' accounts, which were held in their own names. These payments totalled approximately AUD150,000. The victim was also forced to take out loans to purchase two luxury vehicles for the suspects. In addition, the suspects attempted to obtain shares in the victim's company.

AUSTRAC information revealed that:

- Suspect A was identified in a number of suspect transaction reports (SUSTRs) and significant cash transaction reports (SCTRs) detailing their apparent structuring of cash transactions to avoid cash reporting requirements. Additionally, while there was no record of Suspect A being employed, they regularly made large cash deposits into an account. Known associates of Suspect A were thought to have deposited and then transferred funds on Suspect A's behalf. A number of these associates were linked to Suspect A's accounts through funds they had received or transferred. One associate also held a joint account with Suspect A.
- Suspect B conducted numerous large cash withdrawals which were detailed in SCTRs submitted to AUSTRAC. Suspect B was also linked to a suspected criminal network. It was also found that associates of Suspect B had been the subject of numerous SUSTRs due to changes in their gambling behaviour, which involved significant cash amounts.

The resulting law enforcement investigation into the pair's activities led authorities to restrain two luxury vehicles, two properties and numerous other items, with a total value of more than AUD1 million.

Suspect A was charged with 36 counts relating to blackmail and extortion, and sentenced to a minimum of six-and-a-half years jail. Suspect B was charged with 13 counts of blackmail and extortion, and sentenced to a minimum of three-and-a-half years jail.

Offence	Extortion Blackmail
Customer	Individual Business
Industry	Banking (ADIs) Remittance services Gambling services
Channel	Electronic Physical
Report type	SUSTR SCTR
Jurisdiction	Domestic
Designated service	Account and deposit-taking services Remittance services Gambling services
Indicators	Significant cash deposits and withdrawals at a financial institution Structuring of deposits and withdrawals to avoid reporting requirements Customer making large cash deposits despite having no known source of income Use of third parties to deposit and withdraw funds

Case 4 – Suspects jailed after using offshore scheme to avoid $4 million tax

Authorities investigated three suspects for their involvement in the use of an offshore scheme to defraud the Commonwealth and avoid paying almost AUD4 million in tax.

The suspects allegedly used an offshore scheme promoted by an overseas accounting firm to avoid paying the tax:

- A fictitious intermediary company was set up by the overseas accounting firm, which charged the main company, owned by the suspects, for inflated business expenses on 44 separate occasions.
- By artificially inflating their business expenses, the suspects reduced their company's taxable income and therefore the amount of income tax they were required to pay.
- After the main company paid the inflated invoices issued by the intermediary company, the funds used to pay the invoices were diverted into offshore trust funds held in each of the suspects' names.
- These undeclared company profits were subsequently channeled through the trust funds and bank accounts, and finally withdrawn by the suspects as cash from automatic teller machines in Australia.

Ultimately, two of the suspects were found guilty of conspiring to dishonestly cause a loss to the Commonwealth and sentenced to six-and-a-half years imprisonment.

Offence	Fraud
Customer	Individual
Industry	Banking (ADIs)
Report type	IFTI
Channel	Electronic
Jurisdiction	International
Designated service	Account and deposit-taking services
Indicators	Multiple high-value international funds transfers to a high-risk jurisdiction

Case 5 – Human trafficking victims forced to work in Melbourne brothel

Authorities received an allegation that three foreign nationals were being forced to work in sexual servitude at a registered brothel in Melbourne. Law enforcement officers executed a search warrant of the premises and found that a number of foreign women were working at the brothel.

Following further investigations, one individual was arrested and charged with three counts of possessing a slave and three counts of exercising the rights of ownership over a slave. A second individual was arrested and charged with three counts of possessing a slave and three counts of exercising the rights of ownership over a slave.

Charges against the two accused were subsequently dropped, with one of them then being deported from Australia.

While full details of payments and transactions made in association with the three women remain unknown, AUSTRAC financial transaction data indicated that the manager of the brothel had made a number of low-value international funds transfer instructions (IFTIs) to Hong Kong and Malaysia. These international transfers were made through banks and authorities suspected they were made in connection with the three victims.

In addition, AUSTRAC information assisted authorities to identify a number of women linked to common addresses. These addresses were also linked to the manager. The women made a number of structured international transfers to Hong Kong and Malaysia, which authorities suspect may have been for the purposes of facilitating the movement of trafficked individuals to Australia.

Offence	Human trafficking
Customer	Individual
Industry	Banking (ADIs)
Report type	IFTI
Channel	Electronic
Jurisdiction	International – Hong Kong, Malaysia
Designated service	Account and deposit-taking services
Indicators	Structuring transactions (outgoing international funds transfers) to avoid reporting requirements Employing foreign nationals Customer undertaking transactions that appear inconsistent with their profile and/or transaction history: Multiple international funds transfers

Case 6 – Information from industry helped expose suspect funds transfers to China

AUSTRAC information alerted a law enforcement agency to the activities of a suspect who was apparently structuring larger international funds transfers into smaller amounts, seemingly to avoid reporting requirements.

The person came to the attention of AUSTRAC after reporting entities submitted a series of suspicious matter reports (SMRs) detailing the suspect's activities. Further investigations revealed that:

- The suspect had been making regular cash deposits into a personal bank account. The source of these cash deposits could not be established and there was no evidence of the suspect receiving salary payments into the bank account from any employer.
- On occasions, the suspect would present cash in amounts of about AUD9,900 to pay for international funds transfers to individuals who were assessed to be the suspect's relatives in China. The amounts involved in the transfers strongly suggested to reporting entity staff that the suspect was deliberately structuring the cash payments to fall just below the AUD10,000 reporting threshold for cash transactions.

The suspect conducted 28 international funds transfers totalling approximately AUD295,000. Most of the transfers were for the amount of AUD9,900.

The suspect was ultimately charged under section 142 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* with conducting transactions to avoid reporting requirements and was sentenced to four months imprisonment.

Offence	Structuring
Customer	Individual
Industry	Banking (ADIs)
Channel	Electronic Physical
Report type	IFTI SMR
Jurisdiction	International – China
Designated service	Account and deposit-taking services
Indicators	Multiple international funds transfers in amounts just below the reporting threshold (i.e. structured transactions) Structured cash payments just below the cash reporting threshold used to pay for international funds transfers Only funds being deposited into an account are via cash deposits by account holder High-volume account activity involving significant amounts of funds, despite no evidence of employment income Customer undertaking transactions that appear inconsistent with their profile Multiple international funds transfers to country of interest to authorities

Case 7 – Internet banking fraudsters stole thousands from customer accounts

A law enforcement agency conducted an investigation into a criminal syndicate suspected of various offences, including account and internet-banking fraud, money laundering and using false identity documentation.

Banks alerted law enforcement after it was discovered that members of the syndicate had fraudulently transferred funds from the accounts of legitimate customers into accounts they had opened using false identity documents.

The criminal investigation revealed that the syndicate had used internet banking sites to access legitimate customer accounts, using fraudulently obtained customer information. Once they had access to a customer's account, the suspects transferred AUD50,000 out of the account to another account they had previously opened using a false name. Using this method, the syndicate fraudulently obtained approximately AUD500,000. The syndicate also attempted additional transfers worth AUD350,000, but these were identified and stopped prior to payment.

On the same day as making a fraudulent AUD50,000 transfer into their account, two members of the syndicate attended various bank branches and automatic teller machines (ATMs) in Sydney and systematically withdrew the funds from their account. Of these funds, AUD28,000 was given to a third syndicate member.

AUSTRAC information identified that over a four-year period individuals linked to the syndicate sent international funds transfers worth more than AUD250,000 to various countries, with the primary destinations being countries in central and eastern Europe.

Three members of the syndicate were arrested and charged with serious money laundering offences, involving conspiring to deal in proceeds of crime valued at AUD50,000 or more. The suspects were convicted and sentenced to more than six months imprisonment for their role in the money laundering activities.

Offence	Money laundering
Customer	Individual
Industry	Banking (ADIs)
Channel	Electronic Physical
Report type	IFTI
Jurisdiction	International – central and eastern Europe
Designated service	Account and deposit-taking services
Indicators	International funds transfer to a country of interest Use of false identification documentation Use of internet banking to access legitimate customer accounts Multiple cash withdrawals from accounts Multiple ATM withdrawals Cash withdrawals conducted at various bank branches and ATMs on the same day

Case 8 – Company avoided $200,000 GST in import/export fraud

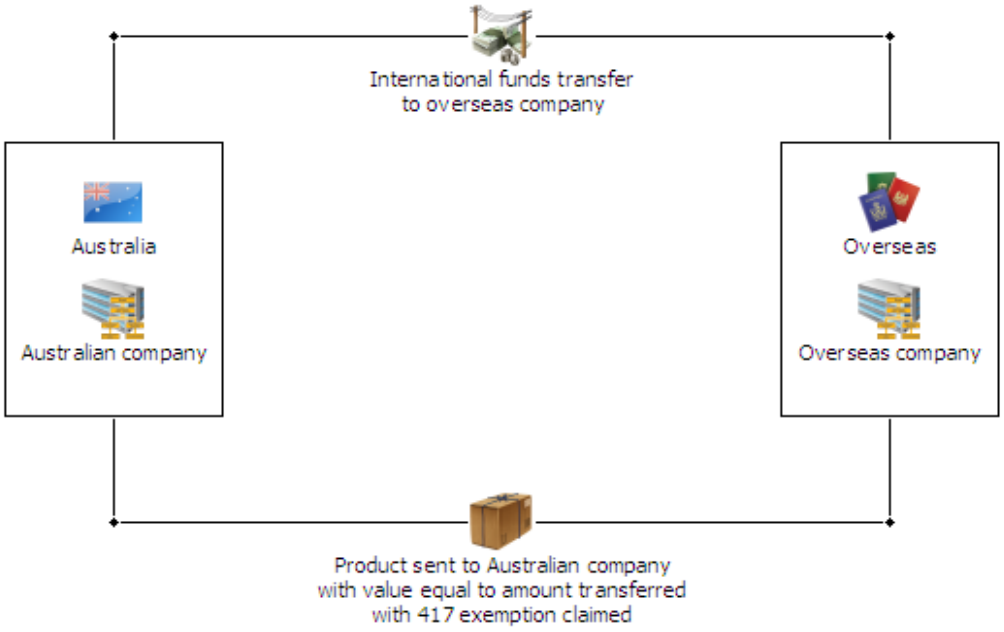
AUSTRAC assisted authorities in identifying an Australian company that was importing goods without paying the correct amount of Goods and Services Tax (GST).

The Australian company regularly purchased high-value collectable artwork from overseas. When the artwork arrived in Australia, the company would claim that the imported artwork was actually 'returned Australian goods', and therefore exempt from GST.

Such returned goods are covered by Customs exemption code 417, which provides that 'goods, originally acquired in Australia that were exported by their owners and subsequently re-imported with unchanged ownership are a non taxable importation.'[19] By claiming that the goods were goods previously exported from Australia, rather than new overseas purchases, the company avoided paying GST on the imports.

AUSTRAC information revealed that the company had regularly conducted international funds transfers to various overseas companies. These overseas companies would then send goods to the Australian company equal in value to the outgoing international funds transfers. This strongly indicated to authorities that the imports were overseas purchases being made by the company, rather than returned Australian goods.

After further investigation authorities took action against the company, which was found to owe more than AUD200,000 in GST.



19 Australian Customs and Border Protection Service 2011, Canberra, viewed 28 February 2011, <www.customs.gov.au/site/page5350.asp#e950>

Offence	Tax fraud
Customer	Business
Industry	Banking (ADIs)
Channel	Electronic
Report type	IFTI
Jurisdiction	International
Designated service	Account and deposit-taking services
Indicators	Outgoing international funds transfers match value of goods imported into country Consistent claims for exemption from GST on products

Case 9 – Fake carbon credits investment scam cost Australian investors millions

AUSTRAC information assisted investigators to identify an overseas-based investment scam that deceived Australian-based victims into sending more than AUD3.5 million to accounts in Taiwan and China. Many of the victims were small business operators, self-funded retirees or investors seeking ethical investment opportunities.

The company came to AUSTRAC's attention after three suspicious matter reports (SMRs) were submitted by an Australian bank over a two-day period. The reports outlined complaints by customers, living in different states, who had been cold-called about a carbon credits investment scam. Two of the customers had previously sent funds overseas to the company, but had since been contacted and asked to transfer more money for further 'investment opportunities'.

The scam operated as follows:

- Overseas-based telemarketers made unsolicited calls to individuals and businesses in Australia. During the calls, the telemarketers gauged the potential victim's views on current environmental concerns and whether they would consider investing in environmental projects.
- For those people who expressed an interest in such investments, the telemarketers arranged for them to be contacted by a representative from the Japanese-based investment scam business offering them the opportunity to invest in projects that generated carbon credits.
- The victims were then instructed to transfer money to accounts in Taiwan and China owned by the scam business.

The scam business used a genuine-looking website to convince investors of the legitimacy of the investment opportunity. The scammers also assured potential investors they could review their investment certificates online through an independent website. However, after investing their money investors subsequently reported they were unable to obtain their investment certificates. Victims also reported the scammers ignored their requests to sell the investments and/or to provide them with a refund.

AUSTRAC information indicated that Australian victims sent more than AUD3.5 million to accounts in Taiwan and China held by the scam investment company. The overwhelming majority of the transfers were conducted through major bank branches, with a small proportion conducted via remittance services.

Australian regulatory authorities have detailed this carbon credits investment scam on their websites and warned Australian consumers and businesses to avoid all dealings with the company.*

* Information and advice about current frauds and scams can be found the Australian Competition and Consumer Commission 'SCAMwatch' website (www.scamwatch.gov.au), and ASIC's MoneySmart website (www.moneysmart.gov.au).

Offence	Fraud
Customer	Business Individual
Industry	Banking (ADIs) Remittance services
Channel	Electronic
Report type	SMR SUSTR IFTI
Jurisdiction	International – Japan, China, Taiwan
Designated service	Account and deposit-taking services Remittance services
Indicators	Multiple customers conducting international funds transfers to the same overseas beneficiary Multiple international funds transfers sent to the same beneficiary in one day High-value international funds transfers

Case 10 – Joint law enforcement investigation uncovered million dollar drug importations

A joint law enforcement investigation led to the arrest of four men and the seizure of approximately 50 kilograms of methamphetamine ('ice') imported into Australia.

Law enforcement officers were investigating suspected large-scale importations of methamphetamine by Hong Kong and Sydney-based individuals who were linked to Asian organised crime syndicates.

During the investigation, it was established that a suspect based in Sydney was operating on behalf of a Hong Kong-based syndicate member and may have been in control of up to 100 kilograms of methamphetamine stored at a location in Sydney.

The suspect and his associates were observed using the services of a Sydney-based Chinese money remitter. Numerous cash 'hand-offs' were arranged, where an associate of the remitter would collect large amounts of cash (up to AUD500,000) at various locations across Sydney from the suspect or his associates. These funds were believed to be payments for the 'ice' importations.

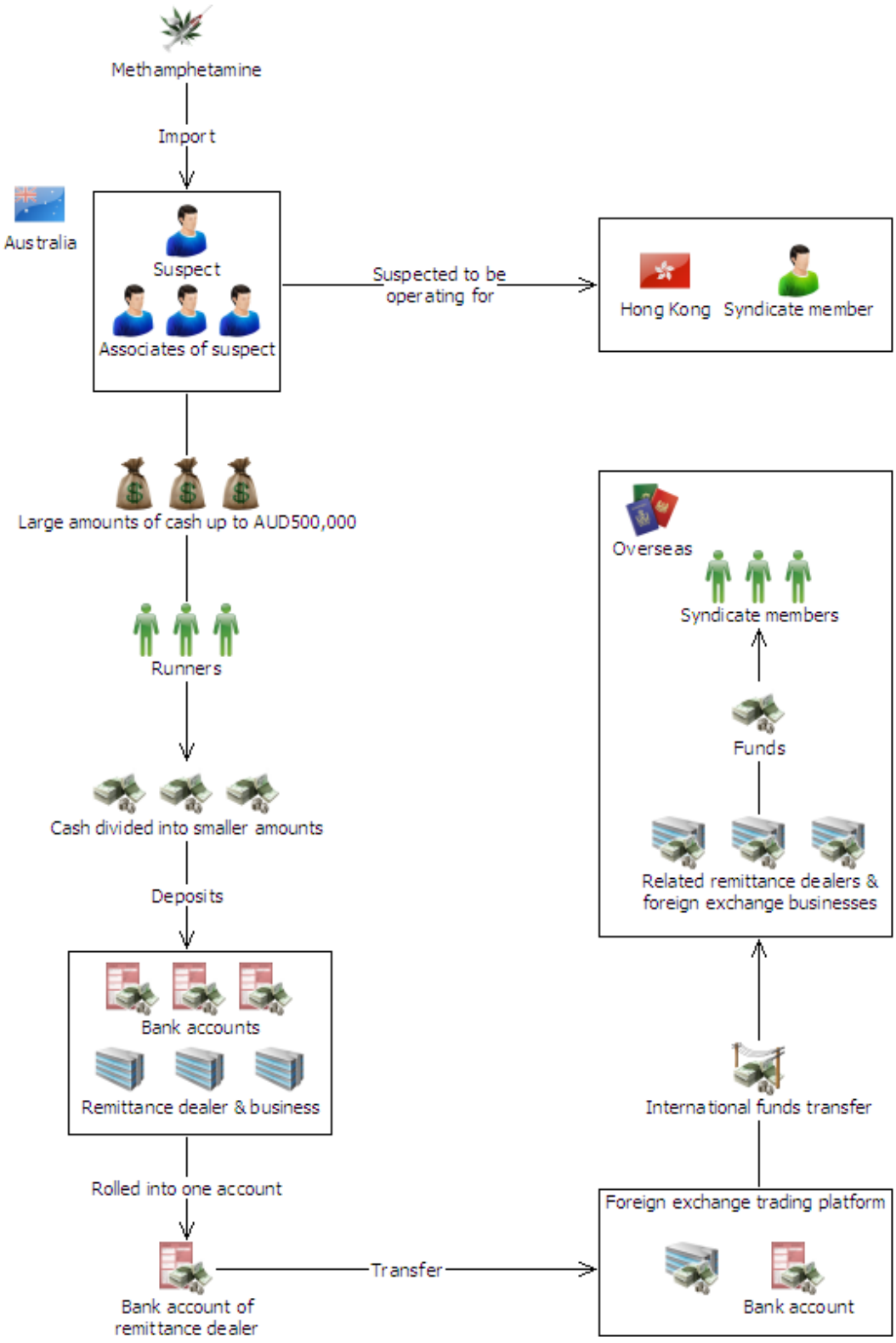
After the cash was collected by the associates, it was immediately broken up into smaller amounts and deposited into the bank accounts operated by the remitter and related businesses. The cash deposits were made via various banks and branches. The remitter made no attempt to structure the cash deposits below the AUD10,000 cash transaction reporting threshold, and the funds were simply rolled into the general cash deposits of the remittance business.

Once the funds were deposited into the remitter's accounts, the remitter then transferred the funds domestically to the account of a Chinese-based foreign exchange trading platform[20]. The remitter then used this trading platform to transfer the funds overseas to other related remittance and foreign exchange businesses, where the funds were available to overseas-based members of the syndicate.

Four men arrested were charged with trafficking a commercial quantity of controlled drugs contrary to the *Criminal Code Act 1995*. It was estimated that the 50 kilograms of methamphetamine seized by law enforcement had a street value of AUD20 million. At the time of writing, two individuals had been convicted and sentenced to 13 years and 11 years imprisonment, respectively.

Offence	Drug trafficking
Customer	Individual
Industry	Banking (ADIs) Remittance services
Channel	Physical Electronic
Report type	IFTI SCTR
Jurisdiction	International
Designated service	Account and deposit-taking services Remittance services
Indicators	Use of third parties to carry cash Large cash deposits Multiple cash deposits at various banks and branches International funds transfers to high-risk jurisdictions

20 A trading platform is software typically provided by a broker, to client, which the client uses to make trades through the broker's system and to manage their account.


Methamphetamine
Import
Australia
Suspect
Associates of suspect
Suspected to be operating for
Hong Kong
Syndicate member
Large amounts of cash up to AUD500,000
Runners
Cash divided into smaller amounts
Deposits
Bank accounts
Remittance dealer & business
Rolled into one account
Bank account of remittance dealer
Transfer
Overseas
Syndicate members
Funds
Related remittance dealers & foreign exchange businesses
International funds transfer
Foreign exchange trading platform
Bank account

Case 11 – Law enforcement agencies combined to foil major money laundering syndicate

The Australian Federal Police (AFP) commenced an investigation into a complex money laundering scheme following a referral from the Australian Crime Commission's 'high risk funds' strategy[21]. The investigation resulted in serious criminal charges being laid against multiple suspects, the largest cash seizure in the AFP's history, and the shutting down of a criminal network. The investigation is a prime example of the effectiveness of inter-agency cooperation in combating criminal organisations and bringing them to justice.

The investigation received significant analysis and intelligence assistance from AUSTRAC and an AUSTRAC analyst was embedded with the AFP investigations team. The investigation identified individuals who were part of a well-organised international money laundering scheme responsible for the laundering of millions of dollars through cash deposits and international funds transfers.

The investigation into the activities of a remittance business network and its agents in Sydney and other major Australian cities identified that large amounts of cash were being deposited into Australian bank accounts operated by the network.

AUSTRAC information assisted the investigation in identifying a number of suspect financial transactions between various bank accounts. The investigation found that the bank accounts had received multiple large cash deposits in denominations of AUD50 or AUD100 notes. Some of the deposits were worth AUD100,000 and, altogether, these cash deposits totalled millions of dollars. Investigators identified that the majority of the deposited funds were subsequently transferred overseas.

The investigation also revealed that previously unidentified individuals from Sydney had been depositing large amounts of cash into three Australian bank accounts linked to a remittance business network operating in Australia.

The investigation focused on the identified members of the Sydney-based network and two suspects responsible for the cash deposits. The identified members of the remittance network would take delivery of the cash in Sydney and then pass it on to the other suspects. These suspects would either deposit the money in Sydney into the bank accounts linked to the remittance network, or give the money to a courier for it to be physically transported interstate by road or air for depositing into the same, linked bank accounts.

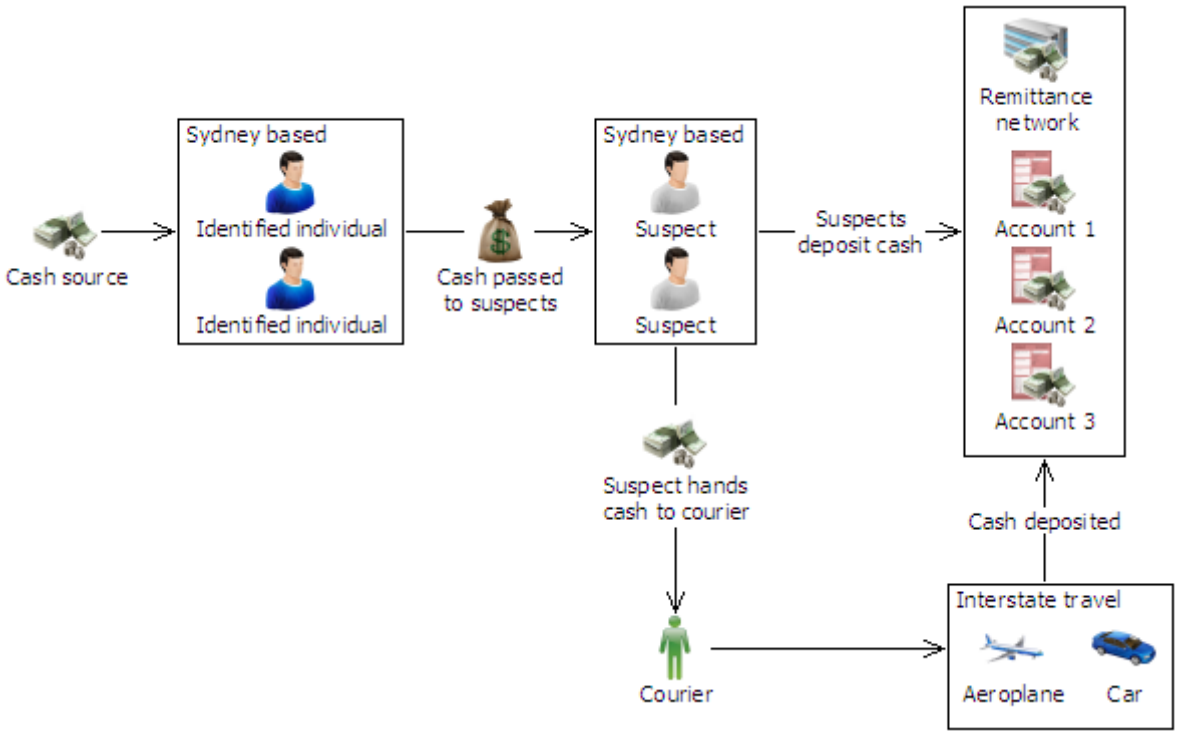
During the resolution of this matter, investigators searched vehicles, businesses and residential premises in Sydney and ultimately seized more than AUD9 million cash.

The investigation led to three people being charged with recklessly dealing in the proceeds of crime (that is, money or property) to the value of AUD1 million or more. A fourth person was charged with possession of money or property reasonably suspected of being proceeds of crime. One of the offenders received a sentence of 14 months imprisonment, while another received a sentence of seven years.

---

21 Australian Crime Commission, *Annual Report 08-09*, ACC, Canberra, 2009, <http://www.crimecommission.gov.au/publications/annual_report/_files/0809/ACC_AR_0809%20COMPLETE.pdf>

Offence	Money laundering
Customer	Business Individual
Industry	Banking (ADIs) Remittance services
Channel	Electronic Physical
Report type	SMR SCTR
Jurisdiction	International
Designated service	Account and deposit-taking services Remittance services (money transfers)
Indicators	Multiple high-value cash deposits in rounded amounts and using only high denominations Third-party individuals making large cash deposits into accounts Multiple high-value international funds transfers Multiple customers conducting international funds transfers to the same overseas beneficiary



Case 12 – Australian investors fell victim to offshore investment 'opportunity'

An AUSTRAC partner agency received a number of complaints from consumers about a suspected 'cold calling' investment scam. An investigation revealed that a number of Australian victims had been deceived into sending money overseas after responding to phone calls offering offshore investment opportunities – representing a similar method to that used in boiler room scams.

AUSTRAC information was used to identify suspected Australian victims who had sent international funds transfers to beneficiaries overseas. AUSTRAC information also established the method of payment and the value of funds transferred by each victim. Amounts varied from AUD3,000 to AUD30,000 per transaction.

Over two-months, Australian victims lost a total of over AUD1 million to these two overseas-based scammers.

AUSTRAC financial information enabled the Australian regulator to alert the reporting entities being used by the victims to transfer money to the overseas scammers.

Offence	Fraud
Customer	Business Individual
Industry	Banking (ADIs) Remittance services
Channel	Electronic
Report type	IFTI
Jurisdiction	International
Designated service	Remittance services (money transfers) Account and deposit-taking services
Indicators	Multiple customers conducting international funds transfers to the same overseas beneficiary Multiple international funds transfers sent to the same beneficiary in one day High-value international funds transfers

Case studies – Gambling services

Case 13 – Lost wallet led to arrest of identity fraudster

The discovery of a lost wallet at a fast food outlet led to a law enforcement operation that uncovered several cases of identity fraud. The wallet contained several different forms of identification, all featuring different names but bearing a photograph of the same individual.

Investigating officers established that the suspect maintained several false identities, while the suspect's wife possessed a false drivers licence.

It was established that the suspect had been using the names of real people to create some of his false identities, although it was never established if these people were complicit in the suspect's fraudulent activities.

AUSTRAC information included seven suspicious matter reports (SMRs) linked to the suspect, although it was impossible to differentiate between transactions undertaken by a suspect while using false identification and legitimate transactions undertaken by the actual identity holders. Six of the SMRs detailed the suspect's suspicious behaviour at gambling venues, including:

- cashing out gambling chips worth a total of AUD89,000 in structured amounts below the AUD10,000 cash transaction threshold
- a reluctance to provide identification at gambling venues.

The SMRs also suggested that the suspect had used some of his various aliases to conduct these gambling activities.

AUSTRAC information also showed that, over a one-year period, the suspect had made a number of significant cash withdrawals from a bank account, totalling AUD620,000.

During the same period, the suspect sent a number of international funds transfer instructions (IFTIs), primarily to India and China, totalling AUD103,000.

The suspect was ultimately charged with identity fraud and with using accounts made out in false names.

Offence	Fraud
Customer	Individual
Industry	Banking (ADIs) Gambling
Report type	IFTI SCTR SMR
Channel	Physical
Jurisdiction	International – China, India
Designated service	Account and deposit-taking services Gambling services
Indicators	High-value international funds transfers to/from Australia with no apparent logical reason Use of false identification to conduct transactions Structuring of cash transactions Unusual customer behaviour at a casino Refusal to show identification

Case 14 – Japanese nationals failed to declare $30,000 cash at airport

Australian casino staff lodged two suspicious matter reports (SMRs) with AUSTRAC detailing suspicious deposits of foreign currency into casino gambling accounts. These reports assisted border protection authorities to detect and apprehend two Japanese nationals who were attempting to leave Australia without declaring physical currency worth more than AUD10,000.

Over a seven-year period the pair had made a number of trips to Australia, bringing with them substantial amounts of Japanese Yen, which they deposited into casino gaming accounts. The source of these funds is unknown.

Throughout this period, the pair had regularly submitted cross-border movement of physical currency (CBM-PC) reports indicating they were carrying physical currency worth AUD10,000 or more. CBM-PC reports must be submitted by travellers arriving in and departing from Australia when carrying physical currency worth AUD10,000 or more (or the foreign currency equivalent).

However, during more recent visits to Australia, the pair had not submitted any CBM-PC reports, even though they were undertaking similar levels of casino gaming activity, involving large amounts of cash. This was assessed as an indication that the pair may still have been carrying, but not declaring, significant amounts of cash during more recent visits.

Analysis of AUSTRAC information over a seven-year period revealed that the pair had deposited more than AUD11 million cash into gaming accounts in Australia. However, over that same period the pair had only reported bringing into Australia the equivalent of AUD7 million cash.

AUSTRAC alerted border protection authorities about the discrepancy and authorities stopped the pair as they attempted to leave Australia. It was discovered that they were carrying foreign currency worth almost AUD30,000 – none of which had been declared. The pair were each issued with an infringement notice and fined for failing to report movements of physical currency valued at AUD10,000 or more.

Offence	Undeclared currency
Customer	Individual
Industry	Gambling services
Channel	Physical
Report type	SMR SCTR CBM–PC
Jurisdiction	International – Japan
Designated service	Gambling services
Indicators	Large cash deposits and withdrawals through gaming account Change in currency declaration behaviour with no change in gaming activity

Case studies – Remittance services (money transfers)

Case 15 – Use of remitters to facilitate people smuggling

Law enforcement partners successfully cooperated with foreign law enforcement counterparts during an investigation into offshore people smuggling networks. The investigation discovered a financial methodology involving remittance dealers enabling the financing of people smuggling. The investigation resulted in the foreign law enforcement agency bringing charges against remitters in their jurisdiction. The charges related to: people smuggling; money laundering; and providing financial services without appropriate licensing.

The financial methodology facilitates people smuggling through the use of funds held by Middle East-based remitters for staged transfer to people smuggling facilitators. The stages of funds transfers were linked to the progress of individuals being smuggled through transit countries.

The methodology has a number of benefits for those involved in the people smuggling:

- The people *smuggler* can be confident that the funds exist to pay for the individual's passage to Australia.
- The *Middle East-based remitter*, located in the source country, has access to funds to use in the operation of their business. Their business cash flow is assisted through the staged release of funds to the people smuggling facilitators.
- The *individuals being smuggled* make payments to the Middle East-based remitter and effectively have their funds held in trust. The funds are safe-guarded while they progress through transit countries, avoiding the need for them to carry cash, with its associated risks.

The methodology uses a three-part process which relies upon international funds transfer instructions and funds deposited with Middle East and Australian-based remitters:

Part 1: Funds transfer instructions from Australia

(i) An Australian-based remittance dealer accepts instructions from customers to send money to beneficiaries in the Middle East.

(ii) The Australian-based customers provide funds to the remitter by:

- depositing funds directly into the remitter's bank account; or
- providing funds directly to the remitter.

Where funds are provided directly to the Australian-based remitter it results in limited information being available for authorities to identify the original owner of the funds, because:

- the deposit made directly to the remitter's bank account may be less than the AUD10,000 threshold transaction reporting limit; or
- the remitter may accumulate cash payments from numerous customers and then deposit the funds into their bank account in one amount.

The Australian-based remitter maintains a record of individual payments made by Australian customers intended for beneficiaries in the Middle East. The remitter uses these records to balance transactions with their counterpart remitter in the Middle East.

Part 2: Imports from Asia by entrepreneurs in the Middle East

(i) The counterpart remitter in the Middle East receives payments from local businesses to pay for imported goods from suppliers in Asia.

(ii) The remittance dealer facilitates funds transfers to the Asian suppliers by instructing an associated Australian-based remitter to transfer funds from Australia using the deposits from Australian-based customers (refer Part 1), avoiding official reporting of the transaction in relation to import tax and excise duty payable in the Middle Eastern country.

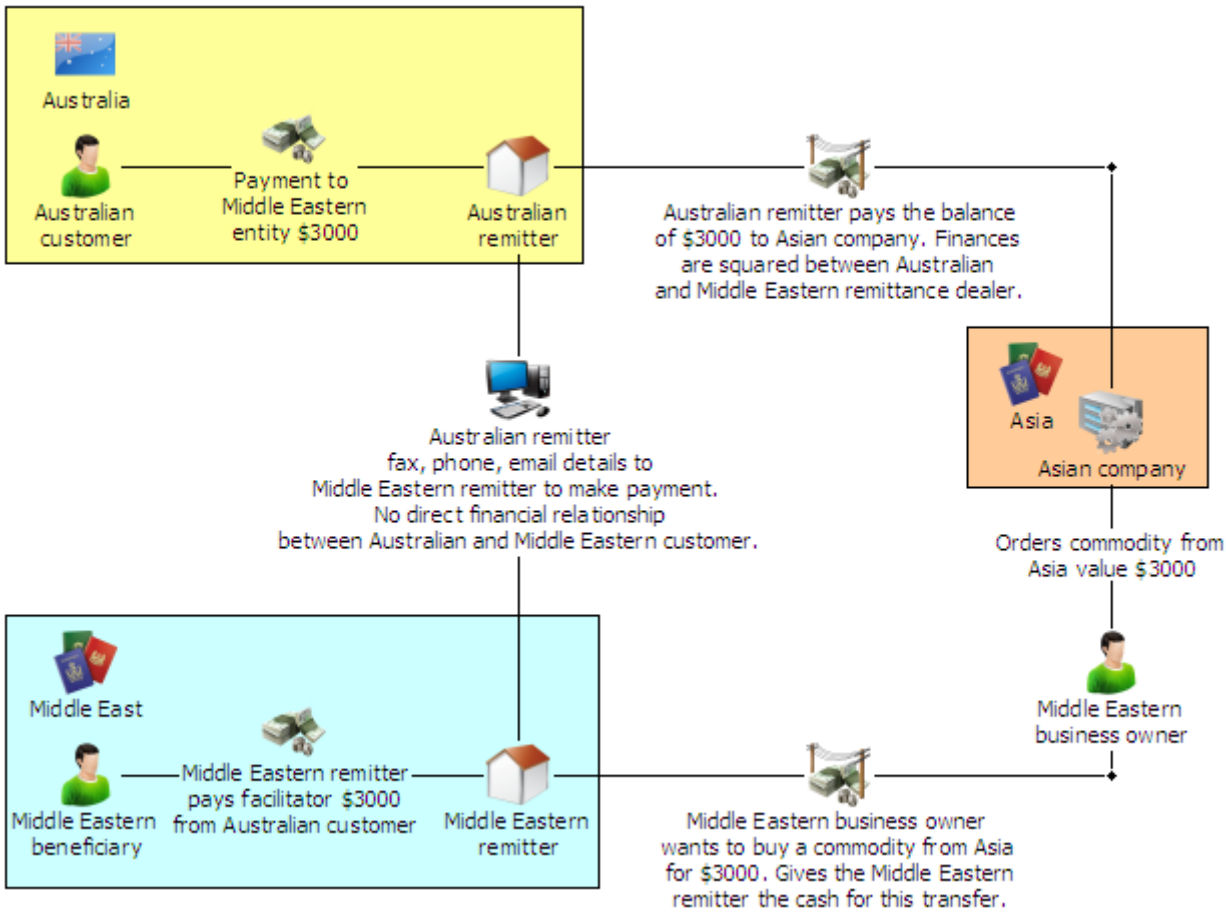
At this stage, funds provided by the local businesses can be used by the Middle East-based remitter to facilitate people smuggling by making payments to people smuggling syndicates at specific points in a person's passage from their country of origin.

To confirm payment has been effected for the goods being imported from Asia, the Australia-based remitter sends a copy of the funds transfer instruction to their counterpart.

Part 3: Payments to effect funds transfer instructions from Australia

(i) The Middle East-based remitter will arrange for payments to be made to the intended recipients as per the instructions from the Australian-based customers (refer Part 1).

The financial methodology is complete when the export company in Asia has received its payment and the funds have been released to the intended recipients in the Middle East.



This example is a simplified version of the methodology. In practice, it is likely that the methodology would involve an even more complex series of payments which could vary in value and take place over a longer timeframe before all parties involved are 'in balance' and all funds are with their intended beneficiaries.

Of significance to this methodology is the fact that where funds are transferred overseas:

- international funds transfer instructions may not identify the sender or the ultimate beneficiary
- some international funds transfers may not be reported at all.

AUSTRAC collaborates with law enforcement to identify incomplete or non-reporting to assist in unravelling the complicated financial trails involved in this methodology

This example demonstrates how financial activity involving people smuggling source and transit countries could result in the misuse of the Australian financial system to enable people smuggling.

Offence	People Smuggling
Customer	Business Individual
Industry	Banking (ADIs) Remittance services
Report type	IFTI
Channel	Electronic
Jurisdiction	International
Designated service	Remittance services (money transfers) Account and deposit-taking services
Indicators	Multiple low-value international value transfers Trade-linked payments to third party countries

Case 16 – Canadian drug importations hidden in foot spas

A law enforcement investigation foiled efforts by an Asian organised crime group to import hundreds of kilograms of drugs – cocaine, ecstasy and crystal methamphetamine ('ice') – into Australia. Law enforcement officers intercepted several shipping containers from Canada and seized the drugs, worth more than AUD31 million, which had been hidden in foot spas.

Authorities suspected that the crime syndicate responsible for the shipments had also been responsible for multiple previous importations of illegal drugs.

AUSTRAC information assisted authorities to identify various suspects and entities involved in the importations:

- Financial transaction information helped identify the Canadian company believed to have supplied the foot spas used to conceal the drugs.
- AUSTRAC information also helped identify the Australian companies that were to receive the importations. The Australian companies had sent a number of international funds transfers to the Canadian company. These transfers were sent through major banks and were worth approximately AUD20,000 each.
- A Canadian national suspected of being the main organiser of the importations made a number of low-value international funds transfers from Australia to Vietnam while he was visiting Australia. Details of these international funds transfers revealed that the suspect had provided a mobile phone number when undertaking the transactions.
- This same phone number was also provided by a second suspect when sending low-value transfers to beneficiaries in Vietnam through a remittance dealer based in Australia. This second suspect was subsequently arrested for overseeing one of the drug importations.
- Other information contained in international funds transfer instruction (IFTI) reports confirmed the connection between the drug importations and the Canadian national suspected of being the main organiser behind the importations.
- AUSTRAC received a large number of significant cash transaction reports (SCTRs) from reporting entities detailing a large number of high-value cash deposits made into bank accounts belonging or connected to the suspects

As result of the investigation, one suspect was sentenced to five-and-half years jail for attempting to possess a commercial quantity of an imported border-controlled drug. The main suspect pleaded guilty to three counts of importing a commercial quantity of a border-controlled substance and was imprisoned for 19 years. A third suspect pleaded guilty to three counts of attempting to possess a commercial quantity of an imported border-controlled drug and was also sentenced to 19 years imprisonment.

Offence	Drug importation
Customer	Business Individual
Industry	Banking (ADIs) Remittance services
Report type	IFTI SCTR
Channel	Electronic
Jurisdiction	International – Canada, Vietnam
Designated service	Remittance services (money transfers) Account and deposit-taking services
Indicators	Multiple low-value international funds transfers to a country of interest to authorities Same ordering customer sending international funds transfers to multiple beneficiaries Significant volume of international funds transfers conducted in a short period of time Significant value and volume of cash deposits into bank accounts

Case 17 – Eastern European 'card skimming' operation spanned several states

Case A

Law enforcement agencies jointly conducted investigations into a criminal group operating a credit card skimming scheme that targeted automatic teller machines (ATMs). The investigations resulted in the arrest of multiple suspects across several states.

The suspects travelled to various states throughout Australia committing offences associated with card skimming and ATM fraud. The suspects attached skimming equipment to the card readers on ATMs, which electronically recorded and stored the details of the cards as they were inserted into the ATM. The suspects also attached pinhole cameras to the ATMs, which were used to record the customers as they entered their personal identification numbers (PINs). After skimming the victims' cards, the suspects created fraudulent cards using the victims' details and accessed their accounts using the captured PINs.

AUSTRAC information was used to detect false identity documents used by the syndicate. This information was crucial in tracking the movement of the suspects as they travelled through various states:

- International funds transfer instruction (IFTI) reports and suspect transaction reports (SUSTRs) submitted to AUSTRAC detailed how the suspects had frequently transferred amounts of less than AUD10,000 via remittance dealers to common beneficiary customers in Romania and Bulgaria.
- AUSTRAC information also identified that the suspects had used different remittance agents to transfer money overseas on the same day.
- Authorities suspected that the remitted funds were sourced through the group's criminal card skimming activities.

Law enforcement officers ultimately arrested numerous suspects, including Romanian and Bulgarian nationals. A suspect arrested in Victoria pleaded guilty to six charges, including dishonestly obtaining or dealing in personal financial information, obtaining property by deception and dealing with property suspected of being the proceeds of crime. The suspect was sentenced to six months imprisonment.

Case B

An additional and related investigation into another card skimming group ultimately resulted in the arrest of a further two suspects. The investigation was initiated when a package addressed to Suspect A was intercepted and found to contain a fake passport carrying a photo of Suspect A and several miniature cameras which could be used to record the PINs of ATM customers.

Suspect A was identified on closed-circuit television (CCTV) footage with Suspect B fitting cameras and skimming devices to ATMs at several locations in Sydney. Having been identified from the CCTV footage, Suspect A was arrested when he attended a local police station following a minor traffic incident. A warrant was issued for the arrest of Suspect B, who was subsequently arrested interstate – just days before his planned departure from Australia.

AUSTRAC information identified that over a three-week period Suspect A sent approximately AUD22,000 via IFTIs to Romania and the United Kingdom. In addition, AUSTRAC information identified that over a further three-month period Suspect B sent an additional AUD121,000 via IFTIs, also to Romania and the United Kingdom. This money is suspected to have been sourced through the pair's card skimming activities.

AUSTRAC received three SUSTRs submitted by reporting entities about the suspicious activities of Suspects A and B, including:

- the high volume of money transfers undertaken by the pair
- the structuring of transactions, apparently undertaken to avoid transaction threshold reporting requirements
- the undertaking of funds transfers to countries of interest to authorities.

Suspect B pleaded guilty in court to three counts of possessing implements to create fake bank cards and credit cards. He was sentenced to two years imprisonment.

Offence	Fraud
Customer	Individual
Industry	Remittance services
Channel	Electronic
Report type	IFTI SUSTR
Jurisdiction	International – Romania, Bulgaria and United Kingdom
Designated service	Remittance services (money transfers)
Indicators	International funds transfer to a country of interest to authorities Cash payments for international funds transfers Multiple low-value international funds transfers Multiple international funds transfers below AUD10,000 Multiple customers conducting international funds transfers to the same overseas beneficiary

Case 18 – AUSTRAC information sparked law enforcement investigation into money remitter

AUSTRAC's monitoring systems identified a substantial increase in cash activity undertaken by a remittance dealer. Further analysis identified significant inconsistencies between the information the remitter had reported to AUSTRAC, and the information reported by the financial institutions where the remitter was a customer.

This information was referred to the Australian Crime Commission's (ACC) FIAT. After the AUSTRAC referral, the FIAT undertook further investigations and disseminated the intelligence to the Australian Federal Police (AFP), who conducted the investigation.

As a result of the investigation two suspects were charged with money laundering offences under the *Criminal Code Act 1995*. One of the suspects was the remittance dealer, while the second suspect, an associate of the first suspect, allegedly acted on behalf of third parties to deposit large amounts of cash into accounts owned by the remittance dealer.

This investigation was triggered by recognised money laundering indicators. AUSTRAC data revealed significant discrepancies between the transactions reported by the remittance dealer from its own 'business' perspective, and the transactions reported to AUSTRAC by the financial institutions which dealt with the suspect remittance dealer as a customer (that is, transactions reported from a 'customer' perspective).

In a typical remittance business, authorities would reasonably expect that, over time, a high proportion of the cash paid by customers to the remittance dealer to pay for international funds transfers would eventually be deposited into a bank account held by the remitter. This 'balancing' of money received by the remitter against money ultimately deposited with financial institutions should be recorded in various AUSTRAC transaction reports, as per the below example:

Step 1

A remittance dealer receives a total of AUD100,000 cash from various customers as payments for international funds transfer instructions. The remitter, reporting from a 'business' perspective, should submit to AUSTRAC:

- threshold transaction reports (TTRs) recording any cash payments of AUD10,000 or more they have received from their customers; and
- international funds transfer instruction (IFTI) reports detailing all international transactions.

Step 2

Over time, the remitter would normally be expected to deposit some, if not all, of the AUD100,000 cash with a financial institution. The financial institution would in turn report these cash deposits to AUSTRAC in TTRs – in these reports, the remitter would be recorded as a 'customer' of the financial institution.

If the remittance dealer operates in the manner described above, it is comparatively straightforward for AUSTRAC to follow the flow and volume of money through its business. This is because the amounts reported from both 'business' and 'customer' perspectives are relatively consistent with each other.

However, certain business practices by the remittance dealer may lead to discrepancies between the transaction amounts reported by the remitter and the deposit amounts reported by financial institutions.

For example, the remitter may decide not to deposit the entire AUD100,000 cash into a bank account to pay for the outgoing international transfers, instead using some of the cash to pay for incoming funds transfers sent to Australian-based customers. This is consistent with the 'hawala'[22] method of transferring funds. The remitter may also utilise hawala for international transfers by arranging for an overseas associate to pay an overseas beneficiary directly.

22 See the glossary for a definition of 'hawala'.

Authorities recognise that the use of hawala by remitters may lead to some discrepancies between a remitter's turnover as reported from the 'business' and 'customer' perspectives. However, the effect of hawala alone seldom explains larger discrepancies. Where significant discrepancies do occur, AUSTRAC is more likely to suspect a remittance business to be handling and moving proceeds of crime, and escalate such matters to law enforcement.

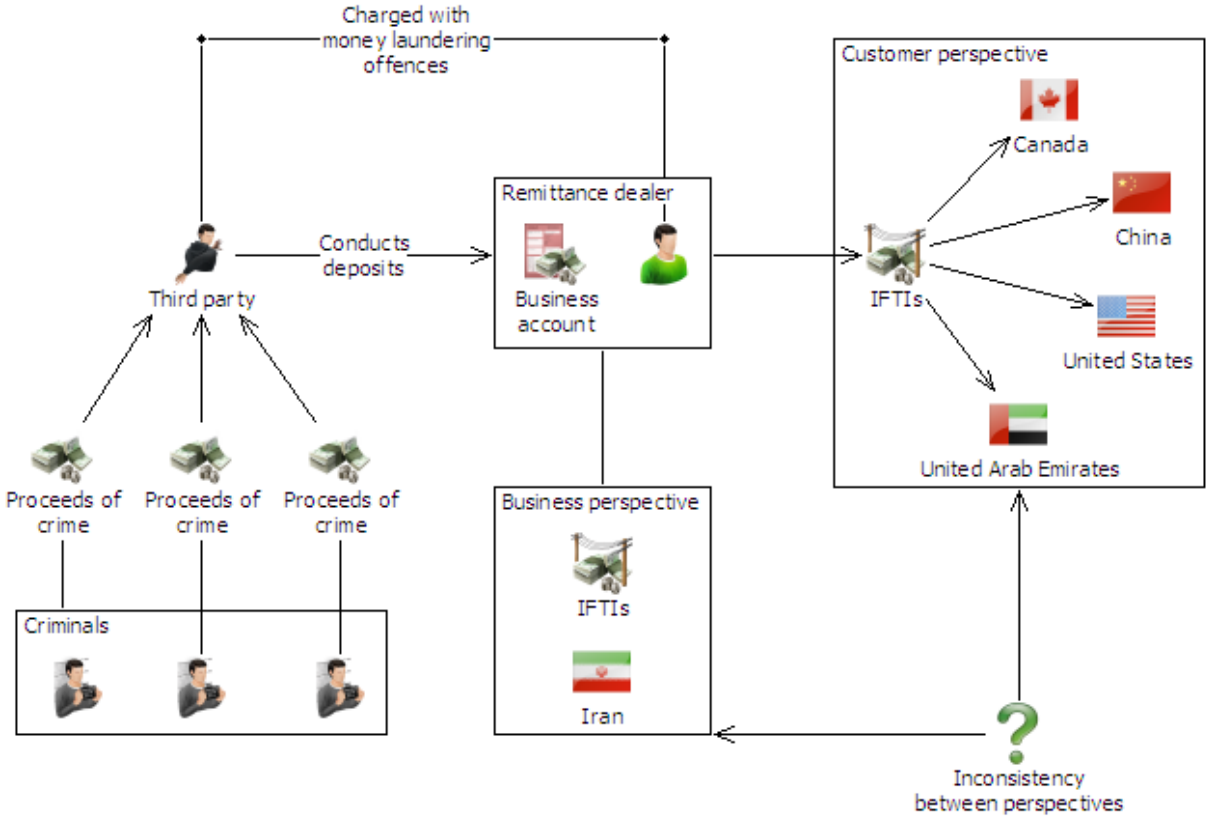
This major AFP investigation, which included significant contributions from the ACC and AUSTRAC, foiled a major money laundering operation. Transaction reporting information received by AUSTRAC revealed a number of significant and suspicious changes in the financial transaction patterns of the remittance dealer involved:

- The remittance dealer's activities changed from facilitating small outgoing international funds transfer instructions (IFTIs), to accepting large cash deposits and facilitating large IFTIs. This spike in financial transaction activity was clearly inconsistent with the remitter's previous profile and history.
- Shortly after this increase in the size of IFTIs, business bank accounts held by the remittance business stopped receiving deposits. However, AUSTRAC analysts identified additional accounts operated by the remittance business, which had been opened under a new company name. Under this new company name, the remitter's business practices appeared to change. While the remitter continued to report to AUSTRAC that the majority of its remittances were being sent to Iran, information received from institutions dealing with the remitter as a customer reported that a significant proportion of the business's outgoing IFTIs were now being sent to the United Arab Emirates (UAE).
- The remitter's transaction activity continued to escalate while operating under the new company name. Over a three-month period the remitter recorded cash deposits totalling AUD34 million and outgoing IFTIs totalling AUD33 million. At the peak of activity, the remitter was receiving cash deposits into its bank account of AUD1 million each day, and on one occasion received almost AUD4 million in two days. The third party making these large cash deposits made no attempt to conceal them, and they were conducted at the same bank branch.
- Information provided by reporting entities was also invaluable in highlighting discrepancies in the remitter's activities. The value of the remittance dealer's business activity as reported to AUSTRAC was significantly less than that reported by the financial institutions that dealt with the remitter as a customer. This discrepancy in reporting strongly suggested to authorities that the remittance dealer was dealing with proceeds of crime, rather than funds generated by legitimate business activities.

The following table highlights the discrepancies in the remitter's transaction activities as reported from customer and business perspectives, over a 10-month period:

Transaction types	**Value as reported by the remittance business (i.e. from the 'business perspective')**	**Value as reported by reporting entities dealing with the remittance business (i.e. from the 'customer perspective')**	**Difference**
Cash deposits recorded in TTRs	AUD48 million	AUD92 million	AUD44 million
Outgoing IFTIs	AUD55 million	AUD95 million	AUD40 million

As the remitter's cash activity escalated, law enforcement agencies executed warrants against the syndicate and stopped its operations. The AFP arrested two individuals, and restrained AUD1.2 million. While the original source of the funds could not be established, the large amount of cash involved led authorities to suspect that the funds were the proceeds of crime.



Offence	Money laundering
Customer	Business Individual
Industry	Banking (ADIs) Remittance services
Channel	Electronic Physical
Report type	SUSTR SMR SCTR IFTI
Jurisdiction	International
Designated service	Remittance services (money transfers) Account and deposit-taking services
Indicators	Multiple high-value cash deposits in rounded amounts and using only high denominations Multiple high-value international funds transfers Sudden increase in transactional activity inconsistent with the remitter's established business profile or transaction history Significant increase in cash deposits received by the remitter Regular large cash deposits made into the remitter's accounts by the same third party, who does not appear to be directly linked to the remittance business IFTIs being sent by a small remittance business to a wide range of different countries, especially when the destination countries are inconsistent with the business's established remitter profile and/or transaction history IFTIs being sent directly to individuals rather than an overseas business contacts A business that appears to provide a remittance service despite not identifying itself as remittance service provider in its dealings with the reporting entity and/or not being enrolled with AUSTRAC

Case 19 – Australian suspect laundered thousands through Turkish bank account

Information provided by an international law enforcement agency initiated an Australian investigation into a money laundering syndicate. The investigation identified that a main suspect was providing an international money laundering service for Australian criminal syndicates.

It was alleged the suspect met with members of the criminal groups and took possession of cash, which authorities suspected was the proceeds of crimes. The suspect allegedly laundered the proceeds of crime offshore on behalf of the criminal syndicates and received a commission in return. AUSTRAC information assisted authorities to identify the money laundering methods used by the main suspect:

- The suspect used a number of associates to assist in the process. The main suspect would pass the cash on to his associates, who would transfer the funds overseas on his behalf. The cash was transferred in amounts of approximately AUD9,000, an activity consistent with the standard pattern of 'structuring'. The associates used their real identities when conducting the international funds transfers through banks and remittance dealers.
- On each occasion, the money was sent to one of four associates based in Turkey. The main suspect then contacted a trusted associate in Turkey and provided him with details of the funds transfers from Australia to Turkey, including the amounts sent, the sender's name, the name of the associates in Turkey who received the transfers, and a reference number for the transactions. The associate in Turkey then collected the money, combined it and deposited it into a Turkish bank account, to which the main suspect in Sydney had access. Authorities identified that a total of AUD125,950 was laundered in this way over two months.

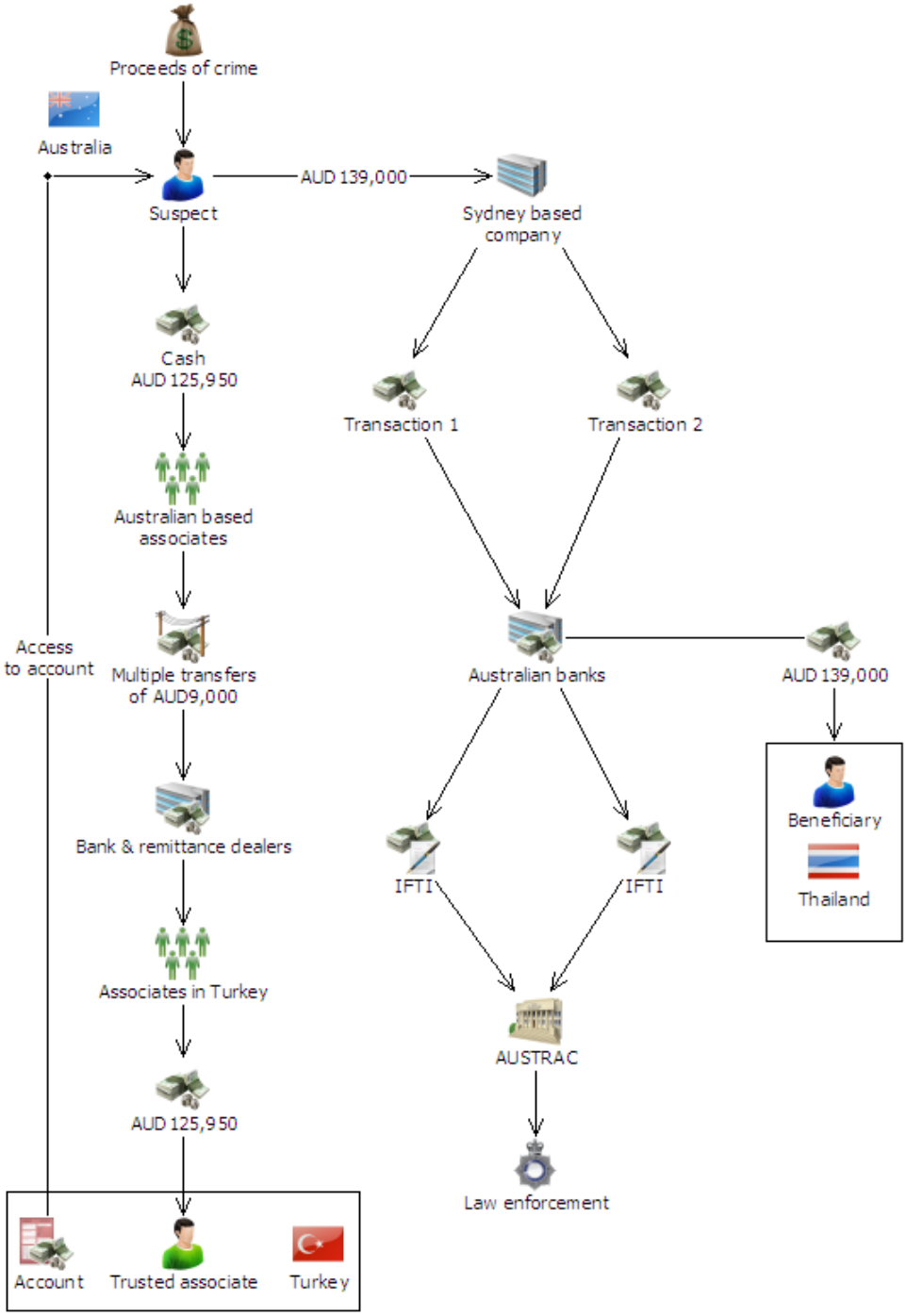
AUSTRAC information also assisted authorities to identify two large international funds transfer instructions (IFTIs) the main suspect had facilitated as part of his laundering activity. The suspect used a Sydney-based company to remit a total of AUD139,000 in two transactions through Australian banks to a beneficiary in Thailand. The main suspect used third parties to deposit and transfer funds in an effort to avoid being directly associated with the money transferred out of Australia.

The suspect was charged and convicted of money laundering under section 400.4 of the *Criminal Code Act 1995* (which covers offences in which a person deals with money or other property worth more than AUD100,000, where there is a risk that it will become an instrument of crime[23]). He was sentenced to four years and three months imprisonment.

Offence	Money laundering
Customer	Individual
Industry	Banking (ADIs) Remittance services
Channel	Electronic Physical
Report type	IFTI
Jurisdiction	International – Turkey and Thailand
Designated service	Account and deposit-taking services Remittance services

23 An 'instrument of crime' is money or other property used (or intended to be used) in, or in connection with, the commission of a Commonwealth, State, Territory or foreign indictable offence.

Indicators	International funds transfers to a country of interest to authorities Multiple customers conducting international funds transfers to the same overseas beneficiaries Cash payments for international funds transfers Use of third parties to conduct funds transfers Use of overseas bank accounts Structuring transactions to avoid reporting requirements Use of a front company



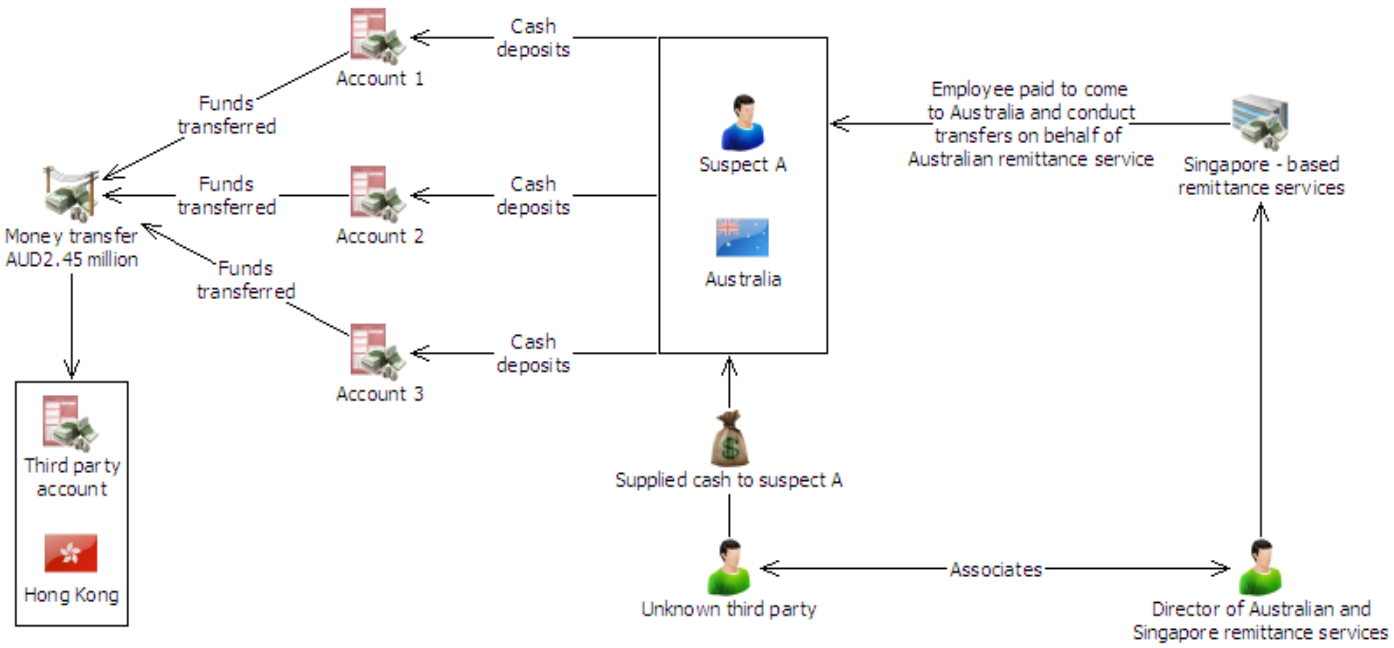
Case 20 – Money remitter sent millions of dollars in illicit cash to Hong Kong

Law enforcement officers commenced an investigation into an Australian money remittance service provider who was suspected of laundering illicit funds. Authorities alleged that, before he left Australia, the director of the money remittance business sent more than AUD7 million of suspected illicit funds to overseas accounts, some held in his own name. Authorities established that the director also operated a remittance business in Singapore.

Authorities subsequently began investigating the activities of Suspect A, a Malaysian national. Suspect A arrived in Australia from Singapore on a temporary visa, claiming to be visiting friends and family. It was established that Suspect A had previously been employed by the director to work at his remittance business in Singapore. Authorities believed that the director paid for Suspect A to come to Australia for approximately one month to conduct international funds transfers on behalf of the Australian remittance business. Further investigations revealed the following:

- Upon arriving in Australia, Suspect A established three accounts at three separate leading financial institutions. All three accounts were established in Suspect A's own name.
- Over an 11-day period, Suspect A made cash deposits worth AUD2.45 million into the three accounts. On each occasion the deposited funds were subsequently remitted to third-party accounts in Hong Kong on the same day the deposit was made.
- Prior to attending the branches to make the deposits, Suspect A collected the cash and instructions for transferring the cash from a third party. Authorities established that this third party was also linked to the Australian money remittance business.
- During the period in which these cash deposits were being made, AUSTRAC received two suspect matter reports (SMRs) from reporting entities. The SMRs detailed the substantial amounts of money involved in the deposits and subsequent international funds transfers.

Suspect A was arrested and charged under Section 400.9 of the *Criminal Code Act 1995* (Cwlth) with two counts of money laundering, and sentenced to one year's imprisonment with a non-parole period of seven months. After serving this sentence, Suspect A was also deported from Australia.



Offence	Money laundering
Customer	Business
Industry	Banking (ADIs) Remittance services
Channel	Electronic Physical
Report type	IFTI SCTR
Jurisdiction	International
Designated service	Remittance services (money transfers) Account and deposit taking services
Indicators	Multiple high-value international funds transfers to an overseas beneficiary within a short time frame Customer undertaking large cash deposits inconsistent with their established customer profile Significant volume of international funds transfers conducted in a short period of time Significant value and volume of cash deposits into bank accounts

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 that 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 suspect transaction or 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 indicators which appear within the case studies of this report, and should be treated as a non-exhaustive guide.

- Business that appears to provide a remittance service despite not identifying itself as remittance service provider in its dealings with the reporting entity and/or not being enrolled with AUSTRAC
- Cash deposits structured to fall beneath reporting threshold
- Cash payments for international funds transfers
- Cash withdrawals conducted at various bank branches and ATMs on the same day
- Change in currency declaration behaviour with no change in gaming activity
- Consistent claims for exemption from GST on products
- Customer making large cash deposits despite having no known source of income
- Customer undertaking large cash deposits inconsistent with their established customer profile
- Customer undertaking transactions that appear inconsistent with their profile and/or transaction history
- Employing foreign nationals
- High-value cash deposits to pay for international funds transfers
- High-value international funds transfers to/from Australia with no apparent logical reason
- High-volume account activity involving significant amounts of funds, despite no evidence of employment income
- IFTIs being sent by a small remittance business to a wide range of different countries, especially when the destination countries are inconsistent with the business's established remitter profile and/or transaction history
- IFTIs being sent directly to individuals rather than an overseas business contacts
- International funds transfers conducted at the same time each month
- International funds transfers conducted through banks and paid for in cash
- International funds transfers to a country of interest to authorities
- International funds transfers to high-risk jurisdictions
- Large cash deposits
- Large cash deposits and withdrawals through gaming account

- Low-value payments undertaken through accounts and low-value cash withdrawals (below the AUD10,000 threshold)
- Multiple ATM withdrawals
- Multiple cash deposits at various banks and branches
- Multiple cash withdrawals from accounts
- Multiple customers conducting international funds transfers to the same overseas beneficiary
- Multiple high-value cash deposits in rounded amounts and using only high denominations
- Multiple high-value international funds transfers
- Multiple high-value international funds transfers to a country of interest to authorities
- Multiple high-value international funds transfers to a high-risk jurisdiction
- Multiple high-value international funds transfers to an overseas beneficiary within a short time frame
- Multiple individuals contributing cash to a central fund (or 'sandooq')
- Multiple international funds transfers below AUD10,000
- Multiple international funds transfers in amounts just below the reporting threshold (i.e. structured transactions)
- Multiple international funds transfers sent to the same beneficiary in one day
- Multiple international funds transfers to country of interest to authorities
- Multiple low-value international funds transfers
- Multiple low-value international funds transfers to a country of interest to authorities
- Only funds being deposited into an account are via cash deposits by account holder
- Outgoing international funds transfers match value of goods imported into country
- Refusal to show identification
- Regular large cash deposits made into a remitter's accounts by the same third party, who does not appear to be directly linked to the remittance business
- Same ordering customer sending international funds transfers to multiple beneficiaries
- Significant increase in cash deposits received by the remitter
- Significant value and volume of cash deposits into bank accounts
- Significant volume of international funds transfers conducted in a short period of time
- Structured cash payments just below the cash reporting threshold used to pay for international funds transfers
- Structuring of deposits and withdrawals to avoid reporting requirements
- Structuring transactions (outgoing international funds transfers) to avoid reporting requirements
- Sudden increase in transactional activity inconsistent with a remitter's established business profile or transaction history
- Third-party individuals making large cash deposits into accounts
- Trade-linked payments to third party countries
- Unusual customer behaviour at a casino
- Use of a front company
- Use of false identification to conduct transactions
- Use of false identification to establish Australian companies
- Use of internet banking to access legitimate customer accounts
- Use of overseas bank accounts
- Use of third parties to carry cash
- Use of third parties to deposit and withdraw funds

Appendix B

References and websites

References

Attorney-General's Department, Canberra, 2011, viewed 8 June 2011, <www.ag.gov.au/www/agd/agd.nsf/Page/National_security>

Attorney-General's Department, Canberra, 2011, <www.ag.gov.au/www/agd/agd.nsf/page/PeopleTrafficking_PeopleTrafficking>

Australian Competition and Consumer Commission, *Targeting Scams: Report of the ACCC on scam activity 2009*, ACCC, Canberra, 2010, <www.accc.gov.au/content/index.phtml/itemId/916075>

Australian Crime Commission, *Annual Report 08-09*, ACC, Canberra, <www.crimecommission.gov.au/publications/annual_report/_files/0809/ACC_AR_0809%20COMPLETE.pdf>

Australian Crime Commission, *Crime Profile Series – Frauds*, ACC, Canberra, 2011, viewed 25 May 2011, <www.crimecommission.gov.au/publications/crime-profile-series/frauds.htm>

Australian Crime Commission, *Organised Crime in Australia 2011*, ACC, Canberra, 2011, <www.crimecommission.gov.au>

Australian Institute of Criminology, *Labour trafficking: key concepts and issues – Transnational crime brief no. 3*, Canberra, 2009, <www.aic.gov.au/en/publications/current%20series/tcb/1-20/tcb003.aspx>

Department of the Prime Minister and Cabinet, *Counter-Terrorism White Paper: Securing Australia – Protecting our Community*, Department of the Prime Minister and Cabinet, Canberra, 2010, <www.dpmc.gov.au/publications/counter_terrorism/>

Financial Action Task Force, *Money Laundering & Terrorist Financing Typologies: 2004–2005*, FATF, Paris, 2005, <www.fatf-gafi.org/dataoecd/16/8/35003256.pdf>

Queensland Police Service, *2009–2010 Annual Statistical Review*, Queensland Police Service, Brisbane, 2010, <www.police.qld.gov.au/services/reportsPublications/statisticalReview/0910/default.htm>

Queensland Police Service, *Advance Fee Fraud project launched*, media release, Queensland Police Service, Brisbane, 28 August 2009, viewed 8 June 2011, <www.police.qld.gov.au/News+and+Alerts/Media+Releases/2009/08/28fraud.htm>

Murdoch, L, '"Vultures" descend on victims with scams', *Brisbane Times*, 17 January 2011, viewed 20 May 2011, <www.brisbanetimes.com.au/environment/weather/vultures-descend-on-victims-with-scams-20110116-19sm0.html>

Rice, S, 'Vigil urged by police on boiler room scams', *The Advertiser*, 10 March 2011, viewed 25 May 2011, <www.adelaidenow.com.au/news/south-australia/vigil-urged-by-police-on-boiler-room-scams/story-e6frea83-1226019293328>

United Nations Office on Drugs and Crime, Vienna, 2011, viewed 3 May 2011, <www.unodc.org/unodc/en/human-trafficking/what-is-human-trafficking.html?ref=menuside>

United States Department of State, *Nigerian Advance Fee Fraud*, United States Department of State, Washington, 1997, <www.state.gov/documents/organization/2189.pdf>

Websites

www.accc.gov.au

www.ag.gov.au

www.aic.gov.au

www.asic.gov.au

www.crimecommission.gov.au

www.customs.gov.au

www.dpmc.gov.au

www.fatf-gafi.org

www.immi.gov.au

www.moneysmart.gov.au

www.police.qld.gov.au

www.scamwatch.gov.au

www.state.gov

www.unodc.org

Case study index

	Case study
account and deposit-taking services	1–13, 15, 16 18–20
alternative (hawala/informal) remittance	18
automatic teller machine (ATM)	7, 17
card skimming	17
cash courier/smuggler/undeclared currency	2, 11, 14
cash deposit	2, 3, 6, 10, 11, 14–16, 18–20
cash withdrawal	1, 3, 4, 7, 13, 14
casino	13, 14
company accounts	1, 4, 8, 9, 15, 16, 18, 19
country of interest to authorities	2, 6, 7, 16, 17, 19
credit card	1, 17
cross-border movement (physical currency) (CBM-PC) reports	14
director (company director)	20
drugs/narcotics	2, 10, 16
extortion/blackmail	3
false identification	1, 7, 13, 17
family members/relatives	6
foreign exchange	10
foreign nationals	5, 14–17, 20
fraud (see also scams)	1, 4, 7–9, 12, 13, 17
gambling services	3, 13, 14
Goods and Services Tax (GST)	8
illegal immigration/human trafficking	5, 15
import/export goods	2, 8, 15, 16
international funds transfers (inc. IFTIs)	2, 4–13, 15–20
internet banking	7
loans	3
money laundering	7, 11, 15, 18–20
motor vehicles	3
organised crime/syndicates	7, 10, 11, 15–19
remittance services (money transfers)	3, 9–12, 15–20

	Case study
sandooq	1
scams (inc. investment scams, fake carbon credits)	9, 12
SCTRs (significant cash transaction reports)	1–3, 10, 13, 14, 16, 18, 20
sexual servitude/exploitation	5
shares/investments	3, 9, 12
structuring	2, 3, 5, 6, 10, 13, 17, 19
SMRs (suspicious matter reports)	6, 9, 11, 13, 14, 18, 20
SUSTRs (suspect transaction reports)	2, 3, 9, 17, 18
taxation fraud	4, 8
terrorism financing	1
third parties	1–3, 10, 15, 18–20
trust funds	4
weapons/explosives	1

Glossary and abbreviations

Glossary

beneficiary (or beneficiary customer)	The person (or organisation) who is the ultimate recipient of funds being transferred.
cash couriers	People who physically transport cash on their person, internally or as part of their luggage between international jurisdictions. Couriers may be directly connected to the criminal activity and proceeds of crime, or they may be third parties (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. In December 2006, CBM-PC reports replaced international currency transfer reports (ICTRs), which were submitted under the FTR Act.
hawala	Hawala is an informal money transfer system which operates around the world, primarily in the Middle East and South Asia. The system operates outside traditional banking and financial channels, and typically involves little or no government regulation and operates with minimal documentation. In Australia, it is an offence for a person to provide a registrable designated remittance service if the person's name and registrable details are not entered on the Register of Designated Remittance Service Providers in accordance with the AML/CTF Act.

high-risk jurisdictions	Jurisdictions which are known to be a source of narcotics[24] or other significant criminal activity, any jurisdiction subject to trade sanctions, jurisdictions known to be a tax haven[25], or jurisdictions linked to proscribed terrorist organisations.[26]
instrument of crime	Money or other property used (or intended to be used) in, or in connection with, the commission of a Commonwealth, state, territory or foreign indictable offence
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. Prior to 12 December 2008, IFTI reports were required to be submitted under the FTR Act.
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.
organised crime group	A criminal network engaged in serious and organised crime as defined by the *Australian Crime Commission Act 2002*.
proceeds of crime	Any money or other property that is wholly or partly derived or realised, directly or indirectly, by any person from the commission of an offence against a law of the Commonwealth, a state, a territory or a foreign country.
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.

24 United States Department of State, 2011, Washington, viewed 29 June 2011, <www.state.gov/p/inl/rls/nrcrpt/index.htm>

25 Australian Taxation Office, 'Tax havens and tax administration', 2011, ATO, viewed 29 June 2011, <http://www.ato.gov.au/corporate/content.aspx?doc=/content/46908.htm&page=4&H4>

26 Attorney-General's Department, Canberra, 2011, viewed 29 June 2011, <www.nationalsecurity.gov.au>

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). For many reporting entities, TTRs (which are submitted under the AML/CTF Act) have replaced SCTRs.
skimming (i.e. card skimming)	Card skimming is the illegal copying of information from the magnetic strip of a credit or debit card, to create a fake or 'cloned' card which allows access to a victim's financial accounts. A common method of card skimming involves attaching small, hidden skimming devices to automatic teller machines (ATMs). The devices electronically record and store the details of the cards as they are inserted into the ATM. The devices are often used in conjunction with pinhole cameras mounted on the ATM, which record customers as they enter their PIN (Personal Identification Number).
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.
suspect transaction report (SUSTR)	Under the FTR Act, a SUSTR must be submitted to AUSTRAC 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 many reporting entities, SMRs (which fall under the AML/CTF Act) have replaced SUSTRs.
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).

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.
'u-turn' transaction	An international transaction where money transferred out of a country is immediately followed by an incoming transfer back into the country, without any obvious business rationale or logical explanation.

Abbreviations

ACC – Australian Crime Commission

ACCC – Australian Competition and Consumer 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*

ASIC – Australian Securities and Investments Commission

ATM – automatic teller machine

AUD – Australian dollars

AUSTRAC – Australian Transaction Reports and Analysis Centre

CBM–PC report – cross-border movement of physical currency report

CCTV – closed-circuit television

EFT – electronic funds transfer

EFTPOS – electronic funds transfer at point of sale

FATF – the Financial Action Task Force

FIAT – Financial Intelligence Assessment Team (hosted by the Australian Crime Commission)

FIU – financial intelligence unit

FTR Act – *Financial Transaction Reports Act 1988*

GST – Goods and Services Tax

IFTI – international funds transfer instruction

PIN – personal identification number

RSA – retirement savings accounts

SCTR – significant cash transaction report [1]

SWIFT – Society for Worldwide Interbank Financial Telecommunication

SMR – suspicious matter report

SUSTR – suspect transaction report [2]

TTR – threshold transaction report

UAE – United Arab Emirates

UNODC – United Nations Office on Drugs and Crime

---

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

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

AUSTRAC typologies and case studies report 2011 feedback form

AUSTRAC is interested in including real-life cases contributed by reporting entities in its future typologies and case studies reports. If you are able to provide details of cases in which your AML/CTF processes identified attempts by criminals to misuse your services for money laundering or other serious crimes, please email AUSTRAC's Typologies and Feedback Unit: typologies_&_feedback@austrac.gov.au.

An online version of this form is available via the AUSTRAC website: www.austrac.gov.au/typologies_2011.html

1. What designated services do you offer (if relevant)?

_____

_____

_____

_____

2. Please indicate how useful you found each section of this typologies and case studies report.

(1 = Not Useful, 5 = Very Useful)

	1	2	3	4	5
Report methodology (p6)					
Typologies (p7)					
Case studies (pp16–51)					
Case study narratives					
Indicators listed for each case					
Link diagrams for cases studies (where applicable)					
Appendix A – Indicators of potential money laundering/terrorism financing activity (p52)					
Appendix B – References and websites (p54)					
Case study index (p56)					

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

4. What information did you find least helpful or interesting? Please explain why (again, please indicate by section title/page number):

5. What new issues, trends, or patterns in money laundering/terrorism financing would you like to see addressed in future typologies and case studies reports (or in other AUSTRAC resources)?

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

Please return this completed feedback form to:

By post

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

By fax

(02) 9950 0071

By email

TYPOLOGIES_&_FEEDBACK@austrac.gov.au

Online form

Alternatively, an online version of this form is available via the AUSTRAC website:
www.austrac.gov.au/typologies_2011.html

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

ISSN 1838-0026

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