Australian Government

Australian Transaction Reports and Analysis Centre

AUSTRAC *typologies and case studies report 2014*

ISSN 1838-0026

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

Foreword

I am very pleased to present the latest *AUSTRAC typologies and case studies report,* the eighth in the series.

These reports are a valuable resource for industry and AUSTRAC's partner agencies. They reveal the diversity and seriousness of the money laundering and terrorism financing threats facing industry and the wider community.

The 20 real-life case studies included in this report present a snapshot of how criminals are seeking to misuse Australia's financial system. They describe international drug smuggling operations, people smuggling and human trafficking syndicates and sophisticated overseas tax evasion schemes. In 16 of these cases, AUSTRAC information and analysis was instrumental in helping to identify additional criminal identities and suspects, bank accounts, phone numbers and aliases that were not previously known to law enforcement.

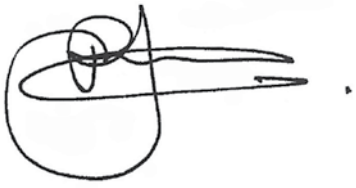
Notably, this report includes case studies where criminals have been caught using new technologies and criminal methods flagged in previous AUSTRAC reports as potential threats. These include a black market website and digital currencies being used to sell illegal drugs, and a cash courier who sent millions of dollars overseas on behalf of a professional money laundering syndicate.

This report examines AUSTRAC's involvement in two multi-agency government task forces – Project Wickenby and the Eligo National Task Force. It shows how AUSTRAC's financial intelligence is vital to their success and details the criminal typologies and suspicious customer behaviours that should trigger 'red flags' for Australian businesses.

AUSTRAC could not produce such detailed and informative resources without the valuable input of its federal, state and territory partners and the cooperation of its international counterparts.

The case studies in this report also demonstrate the enormous intelligence value of the financial transaction reports and reports of suspicious matters AUSTRAC receives from a wide range of reporting entities. I acknowledge the important role played by industry as partners in combating serious crimes, including money laundering.

I look forward to consulting with industry and partner agencies about future reports in this series. This input is crucial in ensuring our reports remain useful and relevant to our collective efforts to protect Australia against financial and other serious crimes.



Paul Jevtovic APM
Chief Executive Officer

Contents

Introduction **4**

AUSTRAC's role 4

Summary of case studies 8

Case studies – Account and deposit-taking services **12**

Case 1 – Suspect used black market website and digital currencies for drug trafficking 12

Case 2 – Mothballed cash stash led to drug trafficker's arrest 14

Case 3 – Suspect jailed after forcing trafficking victims to work in Australian brothels 16

Case 4 – People smuggling operation shut down by joint Australian–Indonesian investigation 18

Case 5 – AUSTRAC data helped capture international cybercriminal 20

Case 6 – Accountant jailed for laundering money via Hong Kong and New Zealand 25

Case 7 – Cash courier transferred millions of dollars to Hong Kong for money laundering syndicate 27

Case 8 – AUSTRAC information revealed extent of people smuggling operation 29

Case 9 – Suspicious funds transfers to Mexico unearthed million dollar drug trafficking syndicate 31

Case 10 – Accountant's overseas tax evasion scheme landed clients in jail 34

Case 11 – Complex tax avoidance scheme hid funds in Samoa and New Zealand 39

Case 12 – Street drugs smuggled into Australia inside stuffed toys and nappies 45

Case 13 – Crime syndicate recruited Malaysian nationals for major credit card fraud 47

Case 14 – Welfare recipients found with $75,000 cash and 15 kilograms of cannabis 50

Case studies – Remittance services (money transfers) **54**

Case 15 – Suspect stockpiled illegal firearms and explosives 54

Case 16 – International crime syndicate used underground banking to launder massive drug profits 55

Case 17 – AUSTRAC information identified Australian victim of $2 million overseas investment scam 58

Case 18 – Suspicious million dollar transfers undid major methamphetamine operation 60

Case 19 – Director of remittance business jailed for laundering cash for criminals 62

Case 20 – Suspect used casinos, remitters and airline pilots to launder proceeds of crime 63

AUSTRAC's work with multi-agency task forces **66**

Project Wickenby 66

Task Force Eligo 71

Money laundering typology – Third-party cash couriers misusing remitter accounts **76**

Appendix A – Indicators of potential money laundering/terrorism financing activity **80**

Appendix B – References and further reading **82**

Appendix C – Report types **83**

Appendix D – Information sources **85**

Case study index **86**

Glossary and abbreviations **88**

Introduction

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

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

AUSTRAC's role

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

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

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

Working with partner agencies to combat money laundering and terrorism financing

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.

AUSTRAC participates in a number of cross-agency task forces and operations. During 2013–14 these included:

- Project Wickenby, led by the Australian Taxation Office (ATO), which targets internationally promoted tax evasion schemes
- Eligo National Task Force, an Australian Crime Commission (ACC)-led task force to address criminal vulnerabilities within the remittance sector
- Taskforce Trident, a joint agency taskforce that was established to address serious and organised criminal activities relating to the maritime environment across Victoria
- Taskforce Galilee, an ACC-led task force investigating serious and organised investment fraud
- Project Tricord and Operation Polo, targeting organised crime syndicates operating in Western Australia
- Taskforce Attero, a national task force coordinated by the ACC targeting the Rebels outlaw motorcycle gang
- the Australian Federal Police (AFP)-hosted Terrorism Financing Investigations Unit and Criminal Asset Confiscation Task Force
- border security activities, including the Border Management Group of the Customs and Border Protection Service, the National Border Targeting Centre, and various multiagency waterfront task forces

Refer to the section *'AUSTRAC's work with multi-agency task forces'* for examples of AUSTRAC's contribution to Project Wickenby and the Eligo National Task Force.

AUSTRAC supports partner agencies through the analysis and dissemination of financial intelligence. AUSTRAC maintains a network of AUSTRAC senior liaison officers (ASLOs), who promote the effective and efficient use of AUSTRAC information and intelligence by partner agencies.

ASLOs are outposted to partner agencies in most capital cities, where they build and maintain relationships with partner agency personnel and provide on-site support, including financial intelligence analysis and training in using the AUSTRAC database. As at 1 December 2014, there are 20 ASLOs supporting various partner agencies.

AUSTRAC's production and dissemination of intelligence reports is informed by key partner agency and whole-of-government priorities. AUSTRAC produced 752 individual intelligence reports in 2013–14 and made 1,314 disseminations to partner agencies. As well as being disseminated to relevant partner agencies, these intelligence reports contribute to the repository of financial intelligence held by AUSTRAC. In addition, AUSTRAC disseminates a range of information and reports to partner agency staff, ranging from individual suspicious matter reports through to operational intelligence products. These products contributed to over 260 significant investigations undertaken by AUSTRAC's partner agencies as well as $358 million in tax assessments raised by the ATO.

AUSTRAC also undertakes research and produces strategic intelligence on money laundering and terrorism financing (ML/TF) risks threats and methods to inform industry and government partner agencies. AUSTRAC disseminates some of its intelligence products to its counterpart FIUs overseas.

In September, AUSTRAC released a public report, *Terrorism financing in Australia 2014*, to raise public and industry awareness of key Australian terrorism financing risks and methods. This has assisted reporting entities to detect suspicious matters that could relate to terrorism financing and to harden measures to deter terrorism financing through Australia's financial system. The report is based on AUSTRAC's classified *National risk assessment on terrorism financing 2014,* which was prepared in close collaboration with a number of other agencies, particularly the AFP.

Working with industry

Each year AUSTRAC receives millions of financial transaction reports and reports of suspicious matters from its regulated entities. The agency analyses this transaction data to identify potential money laundering, terrorism financing and other serious crime.

AUSTRAC then shares its financial intelligence with a wide range of domestic partner agencies and international counterparts for use in their criminal investigations and other operations. Financial transaction data assists authorities to identify relationships between individuals and networks, the movement of funds and patterns of financial activity.

Figure 1, below, illustrates how reporting by industry provides key intelligence to support law enforcement investigations and how AUSTRAC provides industry with information on criminal trends and methods, including through public reports such as this one.

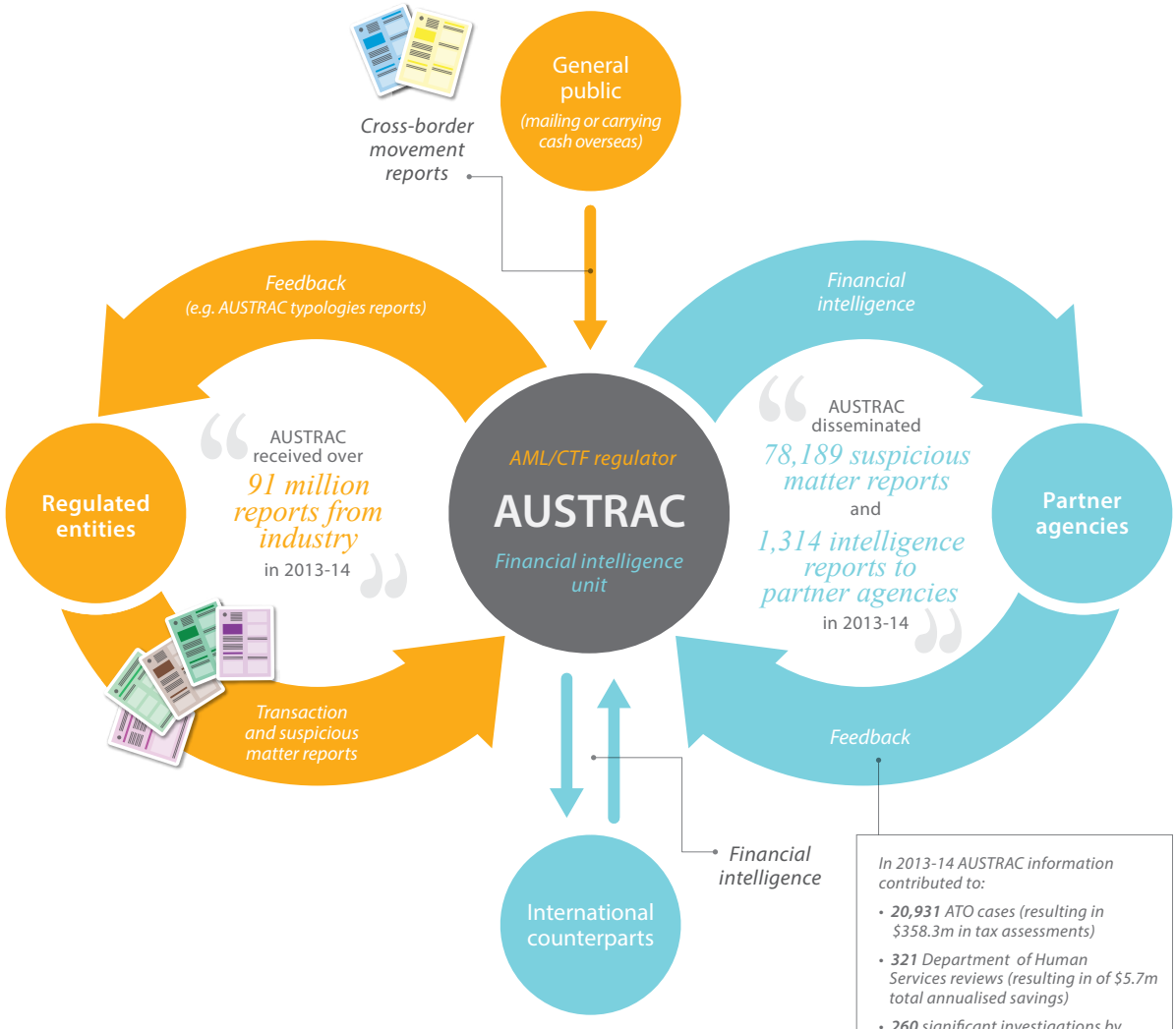


Figure 1 - AUSTRAC's feedback cycle

This report contains a range of case studies detailing investigations and operations undertaken by AUSTRAC's partner agencies. The case studies demonstrate the intelligence value of the transaction and suspicious matter reports submitted to AUSTRAC by reporting entities.

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

Regulated entities should use this report to:

- determine what ML/TF vulnerabilities are most relevant to their organisation
- inform the AML/CTF guidance material and training programs they provide to staff to raise awareness of ML/TF issues within the organisation
- inform their ML/TF risk assessments
- assist them in identifying and investigating unusual customer activity. Entities should use the risk 'indicators' in this report as a guide when describing unusual behaviour in suspicious matter reports
- add new and refine the existing detection scenarios and rules they use in their transaction monitoring programs
- highlight the benefits of maintaining a robust AML/CTF regime within their organisation.

Summary of case studies

The 20 case studies in this report feature partner agency investigations and operations to which AUSTRAC information has contributed. They detail successes achieved through AUSTRAC and its government partner agencies working together and sharing information about criminal activities.

The cases also highlight the value of industry's reporting of financial transactions and suspicious matters to AUSTRAC. They demonstrate how following the money trail is an effective way of detecting the activities of organised crime networks and the value of a whole-of-government approach to combating organised crime.

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

The sanitised case studies represent only a small sample of all partner agency investigations that use AUSTRAC information.

Case 1	AUSTRAC information assisted an investigation which led to the arrest of a suspect who used digital currency to import and sell illicit drugs through a black market website. The suspect was sentenced to three years and six months imprisonment and fined AUD1,000 for possessing controlled weapons.
Case 2	AUSTRAC information assisted law enforcement with an investigation into drug trafficking. The suspect was charged with attempting to traffic a controlled drug and sentenced to two-and-a-half years imprisonment.
Case 3	AUSTRAC information contributed to a law enforcement investigation into a syndicate involved in the trafficking of women from Thailand to Australia. The suspect pleaded guilty to conducting a business involving sexual servitude and making a false statement to an immigration official. The suspect was sentenced to two years and three months imprisonment.
Case 4	A joint investigation between Australian and Indonesian authorities identified two Australian suspects (a father and son) who were facilitating a people smuggling venture. AUSTRAC analysis of financial transaction reports assisted the investigation. Authorities restrained approximately AUD60,000 as the proceeds of crime. The main suspect was sentenced to a suspended nine-month jail sentence.
Case 5	Suspicious matter reports submitted to AUSTRAC led to the arrest of an international fugitive wanted for cybercrime and fraud offences. The suspect pleaded guilty to conspiracy to commit bank fraud, conspiracy to commit money laundering and computer fraud. The suspect was sentenced to five years and 10 months imprisonment and also agreed to assist United States authorities to recover the stolen funds.

Case 6	An Australian law enforcement agency conducted an investigation into a suspect believed to be involved in laundering money. AUSTRAC information linked the suspect to multiple companies and structured cash deposits. The suspect was charged with providing incomplete information in relation to a financial transaction. The suspect pleaded guilty and was sentenced to nine months imprisonment and received a two-year good behaviour bond.
Case 7	A law enforcement agency identified a suspect believed to be working as a cash courier for a suspected money laundering syndicate. AUSTRAC data revealed that the suspect and additional cash couriers were laundering millions of dollars internationally for the syndicate. Three suspects were arrested and received sentences ranging from 11 months imprisonment, a 12-month intensive corrections order and a 12-month good behaviour bond. Authorities also seized AUD543,000 cash.
Case 8	AUSTRAC information assisted authorities with an investigation which disrupted an international people smuggling operation, resulting in the arrest of two Australia-based facilitators. The two suspects received sentences of five years imprisonment and eleven-and-a-half years imprisonment respectively.
Case 9	A suspicious matter report contributed significantly to a law enforcement operation which dismantled an international drug importation syndicate operating in Australia. Authorities used AUSTRAC information to identify suspects, establish links between syndicate members, support existing intelligence and identify financial transactions of interest. Two suspects were convicted of attempting to possess commercial quantities of unlawfully imported border controlled drugs. One was sentenced to eight years and six months imprisonment, the other was sentenced to 17 years imprisonment.
Case 10	AUSTRAC information assisted authorities to investigate a tax evasion scheme promoted and facilitated by an accountant in Australia. The scheme used false invoices and loans to avoid tax. Authorities identified that a client of the accountant defrauded the Commonwealth of AUD2 million over a five-and-a-half year period. The accountant was sentenced to six years imprisonment. The accountant's clients were sentenced to prison terms ranging from two to four years.
Case 11	AUSTRAC information assisted authorities to identify offshore bank accounts and international funds transfers in relation to a complex tax avoidance scheme involving funds transfers between Australia, Samoa and New Zealand. The scheme involved the use of an offshore superannuation fund and a loan arrangement to avoid tax. Authorities ultimately issued amended tax assessments to the individuals involved, resulting in approximately AUD2 million in additional tax, penalties and interest.
Case 12	Suspicious matters reports assisted law enforcement with an investigation into a sophisticated drug importation criminal syndicate. AUSTRAC information assisted authorities to identify the scale of the syndicate's financial activity. A member of the syndicate was charged with attempting to import a marketable quantity of border-controlled drugs and precursors. He was sentenced to a maximum of six years and eight months imprisonment.

Case 13	AUSTRAC information was used to verify the identities of an organised crime syndicate undertaking credit card fraud. A number of suspicious matter reports also assisted authorities to unravel the group's illicit financial activities. Two members of the syndicate were charged with fraud-related offences. One was sentenced to two years and three months imprisonment and the other to 12 months imprisonment.
Case 14	AUSTRAC information helped initiate an investigation that resulted in the arrest of three suspects and the seizure of approximately 15 kilograms of cannabis. Authorities restrained a number of assets, including AUD100,000 cash suspected to be the proceeds of crime, a property and numerous vehicles. One suspect was sentenced to four years and 10 months imprisonment. The other suspect received a suspended sentence of two years and nine months imprisonment.
Case 15	Law enforcement identified a suspect who appeared to be importing components used to build or modify a prohibited type of assault rifle. Authorities used AUSTRAC information to identify the suspect's online payment account and other associated financial activity. The suspect was arrested and charged with various firearms offences.
Case 16	AUSTRAC assisted an investigation which disrupted a global crime syndicate involved in money laundering and the importation of more than 30 kilograms of methamphetamine into Australia. Three suspects were arrested and charged with importing a commercial quantity of a border controlled drug.
Case 17	AUSTRAC information was instrumental in identifying an Australian victim who sent approximately AUD2 million to a highly organised international crime syndicate committing 'advance fee' fraud.
Case 18	Multiple law enforcement agencies worked together to dismantle a major drug syndicate operating in Australia and Vietnam. The investigation uncovered one of the most elaborate methamphetamine operations in Victoria's history and led to the arrest of eight suspects. AUSTRAC information detailed international funds transfers undertaken by the syndicate.
Case 19	AUSTRAC provided financial intelligence to assist law enforcement with their investigation into a remitter suspected of laundering illicit funds for crime syndicates. AUSTRAC analysis identified additional entities, bank accounts and telephone numbers associated with the remitter. The remittance company director was charged and pleaded guilty to dealing with money reasonably suspected to be the proceeds of crime. He was sentenced to three months imprisonment and given an 18-month good behaviour bond.
Case 20	A law enforcement agency conducted an investigation into a suspect believed to be part of an international money laundering scheme. AUSTRAC information revealed the syndicate's financial activities and assisted authorities to identify the suspect. The suspect was charged with dealing with property reasonably suspected of being the proceeds of crime and received a 12-month good behaviour bond.

Case studies

Account and deposit-taking services

Case studies – Account and deposit-taking services

Case 1 – Suspect used black market website and digital currencies for drug trafficking

AUSTRAC assisted an investigation which led to the arrest of a suspect who used a digital currency to purchase, import and sell illicit drugs through a black market website.

The suspect was sentenced to three years and six months imprisonment and fined AUD1,000 for possessing controlled weapons.

Law enforcement intercepted a number of packages sent to Australia from Germany and the Netherlands via the postal system. The packages were addressed to the suspect. Authorities found that the packages contained cocaine and methylenedioxymethamphetamine (MDMA), with a combined weight of 60 grams.

AUSTRAC information identified that the suspect had sent funds to a digital currency exchange to purchase a digital currency. Analysis of AUSTRAC information showed that over a six-month period the suspect undertook 13 outgoing international funds transfer instructions (IFTIs) totalling approximately AUD28,000. The funds were transferred via banks to an online digital currency exchange based overseas.[1] The payments enabled the suspect to purchase an amount of digital currency.

AUSTRAC information showed that the suspect gradually increased the value of IFTIs sent to the digital currency exchange from approximately AUD600 to AUD3,500 per transaction over the six-month period. The suspect also received two incoming IFTIs totalling approximately AUD2,000 from the same online digital currency exchange.

Law enforcement executed a search warrant on the suspect's home and seized a quantity of illicit drugs including cannabis, MDMA, cocaine, amphetamine and methylamphetamine. Additionally, law enforcement seized a number of items associated with drug trafficking, namely digital scales, clip seal bags and a money counter. Authorities also seized approximately AUD2,300 cash, computers, mobile phones and a number of stun guns.

Computers and mobile phones revealed drug trafficking

Analysis of the suspect's mobile phones identified text messages that suggested the suspect was trafficking drugs. On one phone law enforcement identified 150 such messages sent during the week prior to the suspect's arrest.

Analysis of the suspect's computers revealed that he registered an online account with a black market website. The website allows users to purchase and sell illicit goods and conduct transactions using a digital currency. The use of digital currencies provides a degree of anonymity for users. The suspect used this online account to purchase, import and sell illicit drugs.

1 For information about digital currency exchanges see 'Digital currencies and virtual worlds', *AUSTRAC Typologies and case studies report 2012*, pp. 16–17, http://www.austrac.gov.au/typologies-and-case-studies-report-2012

The suspect was convicted of two charges of importing a marketable quantity of a border controlled drug and one charge of trafficking a controlled drug contrary to the *Criminal Code Act 1995*. He also pleaded guilty to possessing a controlled weapon contrary to the *Control of Weapons Act 1990*.

The suspect was sentenced to three years and six months imprisonment. He was also fined AUD1,000 for possessing controlled weapons.

Offence	Drug importation Drug trafficking
Customer	Individual Business
Industry	Banking (ADIs)
Channel	Electronic
Report type	IFTI
Jurisdiction	Domestic International
Designated service	Account and deposit-taking services
Indicators	Increase over time in the value of transactions with a digital currency exchange Multiple low-value international funds transfers

Digital currencies and the regulated AML/CTF sector

Financial activity relating to the use of digital currencies may be indirectly visible to AUSTRAC via the regulated sector. For example, when digital currency-related transactions intersect with the mainstream regulated AML/CTF sector they can generate reportable transactions such as:

- reports of IFTIs between Australian accounts and foreign accounts for the purchase/sale of digital currencies
- threshold transaction reports (TTRs) for cash deposits/withdrawals of AUD10,000 or more involving the bank accounts of digital currency exchange providers
- suspicious matter reports (SMRs) submitted where reporting entities consider financial activity involving a digital currency exchange to be suspicious.

Case 2 – Mothballed cash stash led to drug trafficker's arrest

AUSTRAC intelligence assisted law enforcement with an investigation into drug trafficking. The suspect was charged with attempting to traffic a controlled drug and sentenced to two-and-a-half years imprisonment.

AUSTRAC disseminated an intelligence assessment report to law enforcement regarding the financial activities of a suspect attempting to launder the proceeds of crime raised through drug-related activity. The suspect used bank and casino accounts to launder the funds.

The suspect was the subject of five suspicious matter reports (SMRs) submitted to AUSTRAC. Over a four-day period the suspect made five structured cash deposits of between AUD8,000 and AUD9,000 into his personal bank account.[2] The structured cash deposits totalled AUD41,500. Bank staff reported in the SMRs that the deposited cash smelled of mothballs. After the deposits, the suspect undertook a domestic electronic transfer to move AUD40,000 from his bank account into an account with an Australian casino. The suspect deposited an additional AUD40,000 cash directly into the casino account.

An additional SMR submitted by the bank reported that the suspect received a deposit via domestic electronic transfer of AUD131,000 from the casino. Following this deposit into his bank account, the suspect withdrew AUD9,000 in cash.

The casino submitted an SMR indicating that the suspect was known by two aliases and that he would become aggressive when casino staff requested identification as part of the casino's normal identification procedures for customers cashing out gaming chips. The casino also reported that the suspect was known to cash out chips in amounts under the AUD10,000 cash reporting threshold, presumably to avoid the requirement to present identification to staff.

The suspect was arrested at a domestic Australian airport after a drug detector dog reacted to his suitcase. The suitcase contained 10 vacuum-sealed plastic bags containing a total of 4.5 kilograms of cannabis. The suspect was charged with attempting to traffic a controlled drug, contrary to sections 11.1 and 302.4 of the *Criminal Code Act 1995* and was sentenced to two-and-half years imprisonment.

2 See the Glossary for a definition of 'structuring'.

Offence	Drug trafficking
Customer	Individual
Industry	Banking (ADIs) Gambling services
Channel	Electronic Physical
Report type	SMR
Jurisdiction	Domestic
Designated service	Account and deposit-taking services Gambling services
Indicators	Cash has a distinct or unusual odour Customer unwilling to produce identification when requested by reporting entity staff Structuring of multiple cash deposits below AUD10,000 to avoid reporting obligations Structuring of gaming chip cash outs to avoid reporting obligations Use of false identification

Case 3 – Suspect jailed after forcing trafficking victims to work in Australian brothels

AUSTRAC information contributed to a law enforcement investigation into a syndicate involved in the trafficking of women from Thailand to Australia. The suspect pleaded guilty to conducting a business involving sexual servitude and making a false statement to an immigration official.

The suspect was sentenced to two years and three months imprisonment.

The syndicate used a bank account to conduct a range of transactions to facilitate the trafficking. The investigation ultimately disrupted the Australia-based syndicate.

Australian law enforcement identified an Australia-based suspect who organised for foreign women to work in brothels in Australia. The suspect organised the placement of 11 women in brothels, where they were forced to work to pay off a large debt owed to the suspect. They incurred the debt in return for being brought to Australia.

A broker recruited the women in Thailand and organised passports, visas and other travel arrangements. Each of the women agreed to repay a 'debt' of approximately AUD53,000 after arriving in Australia. Some of the women were made aware that they would be working in the sex industry, while others were misled as to the nature of the work they would be required to perform.

Each Australian brothel deducted its fee and paid the remainder of the earnings to the women. The women used these funds to repay their debt to the suspect by transferring funds electronically into the suspect's bank account or by depositing cash into the suspect's account. In the case of one brothel, the repayments were made by giving cash directly to the suspect.

At the request of the law enforcement agency, AUSTRAC produced financial intelligence assessments which analysed various aspects of the suspect's financial activities.

AUSTRAC identified that:

- the suspect used aliases and variations of her address when conducting transactions
- significant cash transaction reports (SCTRs) revealed the suspect had withdrawn AUD53,000 cash from a bank account over a one-month period
- over an eight-year period the suspect, using her own name and a number of aliases, sent 90 international funds transfer instructions (IFTIs) to individuals in Thailand, totalling approximately AUD455,000.

Analysis of AUSTRAC information identified an individual in Thailand who was suspected of being a broker who arranged the trafficking of women from Thailand into Australia as part of the sexual servitude syndicate.

Over a 12-month period the suspect in Thailand received 37 IFTIs from Australia totalling approximately AUD320,000. The IFTIs were made through banks and were sent by Australia-based employees of the main suspect in Australia, as well as the 11 women. The IFTIs showed the women shared common addresses. Authorities suspect the cash payments were structured into amounts of less than AUD10,000 to avoid the cash transaction reporting threshold. AUSTRAC disseminated information to a Thai law enforcement agency to assist its investigations into the syndicate's operations in Thailand.

On average, it took approximately six months for each woman to pay off their debt to the suspect. Enquiries revealed that of the AUD53,000 each woman was required to pay back to the suspect, the broker in Thailand was paid AUD20,000. The main suspect made a profit of approximately AUD10,000 to AUD18,000 per woman.

As part of the arrangement, after the women arrived in Australia the suspect assisted them to apply for a protection visa. To substantiate a claim for refugee status the suspect provided the women with false information about the conditions they had each experienced in their home country. The suspect also coached the women on how to answer questions from Australian authorities about their visa application.

The suspect pleaded guilty to:

- conducting a business involving sexual servitude over a three-year period contrary to section 270.6(2) of the *Criminal Code Act 1995*
- making a false statement to an immigration official in connection with an application for a protection visa contrary to section 234(1)(b) of the *Migration Act 1958*.

The suspect was sentenced to two years and three months imprisonment.

Offence	People trafficking Sexual servitude
Customer	Individual
Industry	Banking (ADIs)
Channel	Electronic
Report type	IFTI
Jurisdiction	International – Thailand
Designated service	Account and deposit-taking services
Indicators	International funds transfers to a country of interest to authorities Large cash withdrawals within a short time frame Multiple customers linked by common addresses, conducting international funds transfers to the same overseas beneficiary Multiple international funds transfers below AUD10,000

Case 4 – People smuggling operation shut down by joint Australian–Indonesian investigation

A joint investigation between Australian and Indonesian authorities identified two Australian suspects (a father and son) who were facilitating a people smuggling venture. AUSTRAC analysis of financial transaction reports assisted the investigation. Authorities restrained approximately AUD60,000 as the proceeds of crime.

The main suspect was sentenced to a suspended nine-month jail sentence.

Australian authorities alleged that approximately 70 foreign nationals had paid the two suspects to facilitate their passage from Indonesia into Australia. The voyage was not undertaken due to intervention by Indonesian police. The father, suspect A, was identified as a people smuggler operating in Indonesia and Malaysia.

Suspect A originally arrived in Australia as an asylum seeker and was granted a visa. Suspect A was linked to numerous Afghan nationals who were detained in Indonesia and Christmas Island. Suspect A travelled to Pakistan, Malaysia and Indonesia and was approached by Afghan nationals to arrange their safe passage to Australia. The Afghan nationals were willing to pay between AUD8,000 and AUD10,000 each for the journey.

Suspect B assisted his father (suspect A) to transfer funds relating to the people smuggling operation. In Indonesia the foreign nationals paid cash up-front before being transported to Australia. Some of the funds were sent to Australia. Money was also sent from Australia to Indonesia to assist the suspects' people smuggling associates in Indonesia.

Over a two-month period, three suspicious matter reports (SMR) were submitted by reporting entities which identified the following:

- While in Australia, suspect B received multiple incoming international funds transfer instructions (IFTIs) from suspect A in Indonesia. The transfers appeared to be deliberately structured[3] into amounts below AUD10,000.
- Suspect A provided multiple, conflicting identification details when sending separate IFTIs from Indonesia to Australia.
- Suspect B received significant cash deposits into his personal account from multiple third parties in different Australian states.
- Suspect B transferred approximately AUD40,000 from his personal everyday account to his debit card account via internet banking. On the same day suspect B conducted three significant cash withdrawals from the debit card account in amounts of AUD10,000, AUD20,000 and AUD10,000. These cash withdrawals were made at three different bank branches in a major metropolitan area.
- On a separate occasion, suspect B attempted to withdraw a significant amount of cash. Upon being questioned by the branch manager regarding the purpose of the funds suspect B provided conflicting information and then became irate. Suspect B did not withdraw the funds and proceeded to close all accounts at this major bank.

3 See the Glossary for a definition of 'structuring'.

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

- Over a one-month period suspect B conducted one cash deposit of AUD11,000 and five cash withdrawals in amounts between AUD5,000 and AUD20,000. Suspect A also conducted one cash deposit of AUD13,000.
- Over a six-day period suspect A used remittance services in Indonesia to transfer approximately AUD40,000 to suspect B in Australia in amounts between AUD1,900 and AUD7,600.
- Over an eight-month period suspects A and B conducted 10 outgoing IFTIs from Australia to Indonesia. The suspects used the remittance services to transfer the funds to third-party accounts and accounts held in their names in amounts between AUD150 and AUD5,000.

Both suspects were charged with people smuggling and money laundering offences, and suspect B was charged with possessing a drug of dependence. Suspect A did not face trial. Authorities restrained as the proceeds of crime approximately AUD60,000 held in a bank account operated by suspect A's daughter. Suspect B was sentenced to a suspended nine-month jail sentence after pleading guilty to receiving and dealing with money from the proceeds of crime.

Offence	Money laundering Fraud People smuggling
Customer	Individual
Industry	Banking (ADIs) Remittance services
Channel	Electronic Physical
Report type	SCTR IFTI SMR
Jurisdiction	Domestic International – Indonesia
Designated service	Account and deposit-taking services Remittance service (money transfers)
Indicators	Conflicting or incomplete identification details provided for different transactions Customer becomes irate when questioned over financial transactions Customer undertaking transactions that appear to be inconsistent with their customer profile and transactional history International funds transfer from an individual account to several offshore accounts held in the names of third parties International funds transfer to high-risk jurisdictions Large cash withdrawals from multiple bank branches on the same day Structured international funds transfers within a short period of time Use of overseas bank accounts

Case 5 – AUSTRAC data helped capture international cybercriminal

Suspicious matter reports submitted to AUSTRAC led to the arrest of an international fugitive wanted for cybercrime and fraud offences. The suspect pleaded guilty to conspiracy to commit bank fraud, conspiracy to commit money laundering and computer fraud.

The suspect was sentenced to five years and 10 months imprisonment and also agreed to assist United States authorities to recover the stolen funds.

The suspect was an international fugitive who was wanted in the United States for cybercrime and fraud-related offences. United States authorities alleged that the suspect was part of an organised crime group that stole more than USD30 million from United States victims through an elaborate home equity line-of-credit fraud.[4] United States authorities seeking the suspect's arrest published information about him online to alert the public and international authorities.

Australian authorities analysed three SMRs submitted by reporting entities, which included detailed information about multiple aliases used by the suspect. The SMRs prompted AUSTRAC to conduct further analysis, which ultimately assisted Australian law enforcement to identify the suspect.

Initial analysis of AUSTRAC information identified that the suspect held multiple Australian bank accounts in a false name, a joint bank account with a third-party and a business account for a cafe he operated. The SMRs detailed a range of transactions, described below, which reporting entities considered to be suspicious.

International funds transfer instructions (IFTIs)

The SMRs detailed high-value incoming IFTIs sent to the suspect's Australian bank accounts. The suspect received incoming IFTIs in USD totalling approximately AUD1.5 million. These funds were sent from Hong Kong by different individuals and businesses over a one-month period. The suspect also received two incoming IFTIs for AUD90,000 and AUD95,000 from Canada.

Further analysis identified incoming IFTIs into the suspect's accounts totalling approximately AUD6.6 million over a one-year period. The IFTIs were sent from Canada, Hong Kong, Indonesia, Nigeria and the United Arab Emirates. The individual IFTIs were for amounts between AUD30,000 and AUD765,000.

Of the AUD6.6 million transferred into the suspect's accounts, AUD2.6 million was sent to the suspect's personal account, mostly from Hong Kong, Canada and Nigeria. The suspect's business account received approximately AUD4 million from Hong Kong, Indonesia, Nigeria and the United Arab Emirates. The high-value IFTI activity was inconsistent with the café's established customer profile.

The SMRs reported that the suspect withdrew the funds received via the incoming IFTIs shortly after receiving them, using a range of withdrawal types:

- cash withdrawals at different bank branches in two Australian states
- cash withdrawals from automatic teller machines (ATMs) at gaming venues

4 See the Glossary for a definition of 'home equity line-of-credit fraud'

- use of a debit card to purchase high-value goods including:
  - AUD50,000 purchase at a luxury car dealer
  - AUD95,000 purchase at a high-end jeweller
- withdrawal of a bank cheque for AUD195,000 made payable to a real estate agent.

Over the same period the suspect sent IFTIs totalled approximately AUD318,000. The IFTIs were sent to the United States, Canada, Germany, Luxembourg and Malaysia. The value per transaction ranged between AUD20 and AUD245,000. An outgoing IFTI to Canada for AUD245,000 was described by the suspect as 'pay out of mortgage'.

An SMR noted that the high-value incoming IFTIs and withdrawals were inconsistent with the customer's established profile, and therefore grounds for suspicion.

Cash withdrawals

The SMRs identified a large number of high-value cash withdrawals from accounts operated by the suspect:

- eight cash withdrawals totalling AUD94,000 conducted at multiple bank branches over a 10-month period in amounts ranging between AUD1,000 to AUD57,000
- cash withdrawals undertaken within a short time frame at multiple bank branches including:
  - three cash withdrawals totalling AUD25,000 over an eight-day period in amounts ranging between AUD6,500 and AUD9,500
  - more than 15 cash withdrawals undertaken at multiple bank branches totalling AUD128,000 over a two-month period in amounts ranging between AUD5,000 and AUD9,700.

  The above withdrawals appeared to be structured into amounts of less than AUD10,000 to avoid the threshold transaction reporting regime[5]
- eight cash withdrawals of AUD1,000 each on the same day at the same branch
- more than 100 cash withdrawals at ATMs totalling AUD105,000 over a three-month period in amounts of between AUD80 and AUD2,000

Cash deposits

The SMRs detailed a high volume of high-value cash deposits at multiple bank branches, including:

- two cash deposits of AUD8,500 and AUD32,000 made at two bank branches on different days
- cash deposits totalling AUD56,000 over a three-month period with each deposit ranging between AUD3,000 and AUD23,000
- cash deposits for amounts between AUD45 and AUD65,000 totalling AUD105,000 made at multiple bank branches over a 10-month period.

5 See the Glossary for a definition of 'structuring'.

Domestic electronic transfers

The SMRs also detailed high-volume and high-frequency domestic electronic transfers between the suspect's accounts:

- numerous transfers totalling AUD1.3 million over a two-month period between the suspect's accounts
- transfers from the joint bank account to the suspect's own accounts totalling AUD1.5 million over a three-month period
- transfers to and from unrelated third parties including:
  - approximately 75 transfers totalling AUD7.2 million ranging in value between AUD140 and AUD1.2 million over a three-month period from the suspect's accounts *to* unrelated third parties
  - transfers received *from* unrelated third parties totalling AUD7.2 million over a three-month period, ranging in value between AUD400 and AUD1.2 million.

Dissemination of SMRs to partner agencies

After analysing the SMRs, AUSTRAC disseminated them to law enforcement partner agencies, who used them to identify additional false names used by the suspect.

A further five SMRs submitted by reporting entities triggered AUSTRAC's monitoring system and were also disseminated to law enforcement. The financial transaction activity reported to AUSTRAC in the SMRs was consistent with the activity outlined above. Reporting entities detailed additional financial activity of the suspect including:

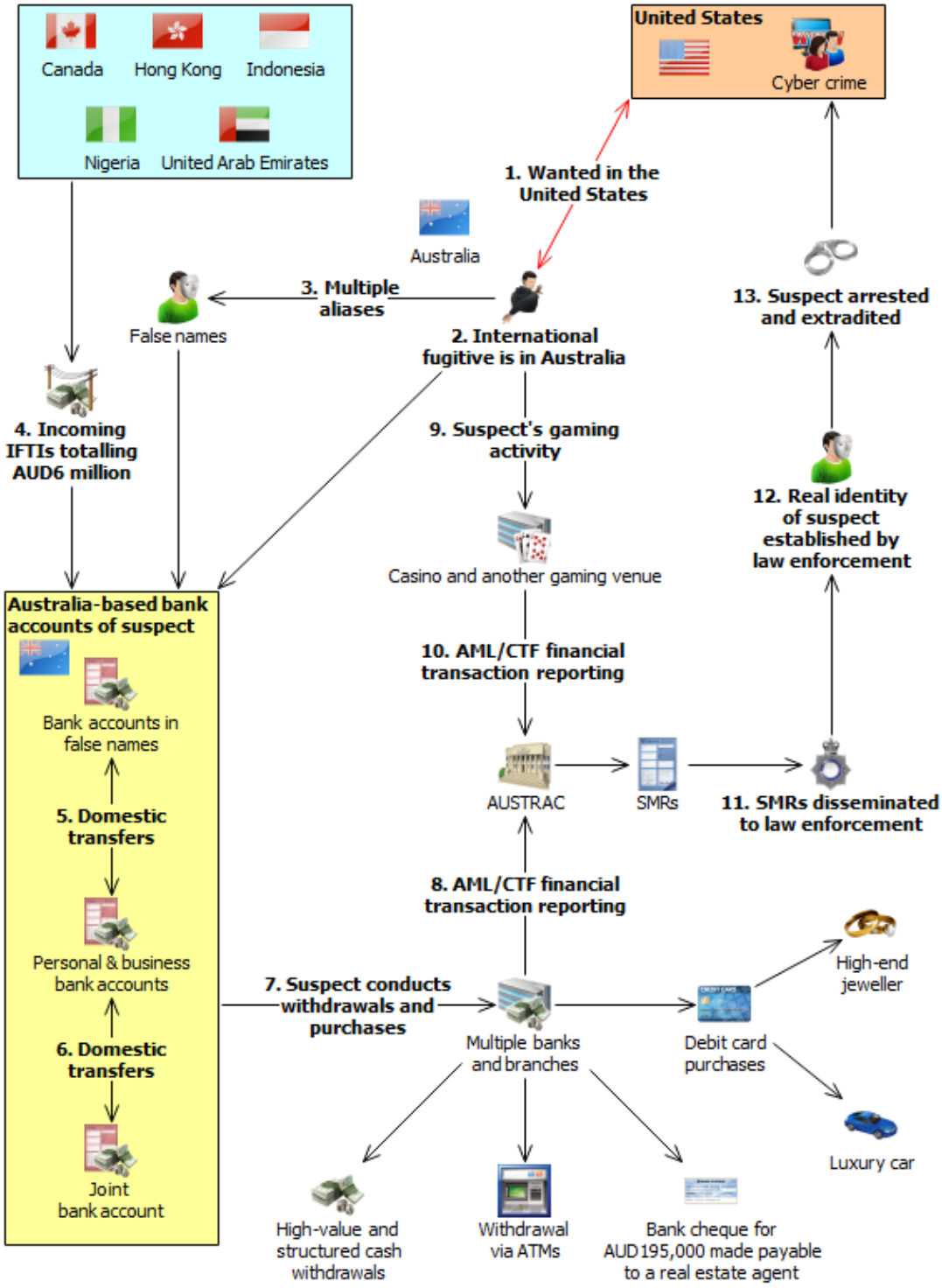
- two domestic electronic funds transfers conducted on consecutive days for AUD25,000 and AUD60,000 to bank accounts held by a casino and another gaming venue
- cash buy-ins of gaming chips totalling AUD275,000 during six visits to a casino, amounting to a total annual loss of AUD53,700[6]
- multiple structured cash buy-ins of gaming chips worth AUD9,000 and the suspect's refusal to show identification at a casino
- cash totalling AUD175,000 used to place bets at multiple gaming venues over a two-month period.

AUSTRAC information combined with analysis undertaken by law enforcement confirmed the identity of the suspect. AUSTRAC data identified phone numbers and address details used by the suspect which ultimately led to his arrest. AUSTRAC data also provided authorities with detailed information about the suspect's financial activities.

The suspect was arrested and extradited to the United States. He pleaded guilty to conspiracy to commit bank fraud, conspiracy to commit money laundering and computer fraud. He was sentenced to five years and 10 months imprisonment. The suspect also agreed to assist United States authorities to recover the stolen funds.

6 'Chip buy-in' is the process of converting cash into gaming chips to be used in casino gambling.

Offence	Money laundering Fraud
Customer	Business Individual
Industry	Banking (ADIs) Gambling services
Channel	Electronic Physical
Report type	IFTI SMR
Jurisdiction	Domestic International – Canada, Germany, Hong Kong, Indonesia, Luxembourg, Nigeria, the United Arab Emirates
Designated service	Account and deposit-taking services Gambling services
Indicators	Account activity inconsistent with customer/business profile High-value cash deposits at multiple bank branches over a short period of time High-value or structured casino chip cash buy-ins High-value transfers to accounts held in the name of a casino and gaming venue High-volume and high-value incoming international funds transfers to Australia for no apparent logical reason High-volume and/or high-value cash withdrawals at multiple bank branches and ATMs Incoming international funds transfers from a high-risk jurisdiction Large amount of cash used to place bets at a casino over a short period of time Multiple cash withdrawals below the AUD10,000 reporting threshold (that is, structured cash deposits) Multiple same-day cash withdrawals conducted at ATMs and the same bank branch Outgoing international funds transfers to pay out a mortgage Refusal to show identification when undertaking cash buy-ins of gaming chips Significant cash withdrawals over a short period of time Third-party transfers to and from accounts for no apparent logical reason Use of debit cards to purchase high-value goods



Case 5 – AUSTRAC data helped capture international cybercriminal

Case 6 – Accountant jailed for laundering money via Hong Kong and New Zealand

An Australian law enforcement agency conducted an investigation into a suspect believed to be involved in laundering money. AUSTRAC information linked the suspect to multiple companies and structured cash deposits. The suspect was charged with providing incomplete information in relation to a financial transaction.

The suspect pleaded guilty and was sentenced to nine months imprisonment and received a two-year good behaviour bond.

Over a two-year period an account held by the main suspect received more than 80 'structured' cash deposits, as a well as a small number of cheque deposits.[7] The cash and cheques were deposited into an account held by the suspect. The suspect, an accountant, regularly consolidated the funds from the various deposits and transferred the funds electronically to third-party domestic accounts. Authorities believed the suspect received a percentage of the funds he transferred as a commission for his services.

Although the exact source of the funds laundered by the suspect is unknown, authorities identified possible links between the funds and the importation of drugs into Australia. AUSTRAC information linked the suspect to approximately 50 companies and revealed that the structured cash deposits into the suspect's account were made on behalf of both companies and individuals.

AUSTRAC also received four suspicious matter reports (SMRs) from reporting entities detailing structured cash deposits undertaken by the suspect.

Further analysis by AUSTRAC identified that the suspect also undertook international funds transfer instructions (IFTIs) worth more than AUD700,000 to Hong Kong and New Zealand. The funds were transferred from accounts held in the suspect's name to overseas business accounts in amounts ranging from AUD400 to AUD50,000. In some instances the offshore recipient businesses shared the same name as businesses operated by the suspect in Australia.

The suspect was charged under section 31 of the *Financial Transaction Reports Act 1988* and section 142(1) of the *Anti-Money Laundering and Counter-Terrorism Act 2006* for providing incomplete information in relation to a financial transaction. He pleaded guilty and was sentenced to nine months imprisonment and received a good behaviour bond for a period of two years.

7 See the Glossary for a definition of 'structuring'.

Offence	Money laundering
Customer	Individual Business
Industry	Banking (ADIs)
Channel	Electronic Physical
Report type	IFTI SMR
Jurisdiction	Domestic International – New Zealand, Hong Kong
Designated service	Account and deposit-taking services Remittance service (money transfer)
Indicators	Multiple domestic transfers to third-party accounts Multiple international funds transfers which are inconsistent with the established customer profile Structured cash deposits into a bank account from third parties Structured financial transactions in personal and business names

Case 7 – Cash courier transferred millions of dollars to Hong Kong for money laundering syndicate

A law enforcement agency identified a suspect believed to be working as a cash courier for a suspected money laundering syndicate. AUSTRAC data revealed that the suspect and additional cash couriers were laundering millions of dollars internationally for the syndicate.

Three suspects were arrested and received sentences ranging from 11 months imprisonment, a 12-month intensive corrections order and a 12-month good behaviour bond. Authorities also seized AUD543,000 cash.

Analysis of AUSTRAC data revealed that suspect A and additional cash couriers were depositing and transferring millions of dollars internationally for the syndicate.

The syndicate used the following method to move funds:

- Suspect B instructs suspect A to open two business accounts. Suspect A is made the sole signatory for the accounts.
- When suspect B takes possession of illicit cash, she contacts suspect A, who then flies interstate to meet her.
- Suspect A meets suspect B at a designated location where suspect B provides suspect A with the cash to be deposited and instructions on where the funds are to be transferred overseas.
- Suspect A deposits the cash into one of the business accounts. She makes several deposits across a number of different bank branches on the same day.
- On suspect B's instructions, suspect A transfers the funds overseas to accounts in Hong Kong.
- Afterwards, suspect A gives the receipts for the deposits and transfers to suspect B.

AUSTRAC information identified a significant spike in suspect A's financial activity over a six-month period:

- During the first month of activity, the business accounts held by suspect A received more than AUD430,000 in cash deposits, by third parties in various states.
- In the first two months of activity, suspect A sent international funds transfer instructions (IFTIs) totalling more than AUD2.3 million to businesses located in Hong Kong.
- Although suspect A's business accounts appeared to be receiving significant amounts of money from various sources and then transferring the funds overseas on their behalf, the business was not registered with AUSTRAC as a remittance dealer.

Prior to the transaction activity described above, AUSTRAC had recorded minimal financial transaction activity undertaken by suspect A.

The subsequent three months saw the business account set up by suspect A receive cash deposits worth more than AUD4.8 million.

Suspicious matter reports (SMRs) submitted to AUSTRAC highlighted the extent of financial activity related to suspect A and his business account. Some of these details included:

- Each month suspect A's business account received hundreds of cash deposits and electronic domestic transfers. Some cash deposits were undertaken by third parties. These deposits and transfers totalled more than AUD1 million per month.
- Typically, around AUD200,000 of the total deposits each month was deposited in structured cash amounts of less than AUD10,000.[8] The remainder of the cash deposits were for larger amounts ranging from AUD10,000 to AUD70,000.
- A small portion of the funds was then debited from the accounts through cash withdrawals or domestic transfers.
- The majority of the funds were transferred via IFTIs to businesses located in Hong Kong, some of which were thought to be foreign exchange companies. These IFTIs ranged in value from AUD10,000 to AUD98,000
- The cash withdrawals, domestic transfers and IFTIs were usually conducted soon after a deposit was made into the account. This activity appeared to be inconsistent with the customer's established profile.

Three suspects were arrested by law enforcement and AUD543,000 cash was seized. Suspect A and B pleaded guilty to dealing in property reasonably suspected to be the proceeds of crime greater than AUD100,000.

Suspect A was sentenced to 11 months imprisonment, suspect B was given a 12-month intensive corrections order, and an additional suspect was given a 12-month good behaviour bond.

Offence	Money laundering
Customer	Business Individual
Industry	Banking (ADIs)
Channel	Electronic Physical
Report type	IFTI SCTR SMR
Jurisdiction	Domestic International – Hong Kong
Designated service	Account and deposit-taking services
Indicators	Frequent cash deposits occurring at different branches on the same day International funds transfers to overseas businesses similar in total value to recently received cash deposits Structuring of cash deposits below AUD10,000 to avoid reporting obligations Sudden increase in financial activity inconsistent with individual's transaction history Third parties making regular cash deposits into a business account Withdrawals conducted quickly after deposits

8 See the Glossary for a definition of 'structuring'.

Case 8 – AUSTRAC information revealed extent of people smuggling operation

AUSTRAC information assisted authorities with an investigation which disrupted an international people smuggling operation, resulting in the arrest of two Australia-based facilitators.

The two suspects received sentences of five years imprisonment and eleven-and-a-half years imprisonment respectively.

Law enforcement officers established that the people smuggling syndicate used boats to illegally transport foreign nationals from Indonesia to Australia. Authorities suspected that the syndicate members were in contact with Australia-based associates to organise the people smuggling operation.

Authorities alleged that suspects A and B were key players in the people smuggling syndicate, responsible for planning and facilitating the unlawful arrivals into Australia. The majority of prospective customers were Iraqi and Iranian nationals and the syndicate allegedly charged between AUD4,500 and AUD10,000 per person.

AUSTRAC analysis of financial transaction reports showed that over a five-year period suspect B sent 28 international funds transfer instructions (IFTIs) out of Australia totalling more than AUD42,000. The IFTIs were primarily sent to Indonesia.

The IFTIs undertaken by suspect B were conducted via remittance service providers for low-value transfers of between AUD100 and 5,000. A small number of the IFTIs were sent with payment details describing them as 'gift' or 'personal'.

AUSTRAC information also included threshold transaction reports (TTRs) which showed that:

- over a two-month period, bank accounts held in the name of suspect B received two cash deposits totalling more than AUD37,000
- over a one-year period, suspect B made four large cash withdrawals totalling more than AUD57,000. The cash withdrawals were conducted at various bank branches and were conducted on separate days.

AUSTRAC information indicated that suspect B also sent and received IFTIs while in Indonesia. AUSTRAC's financial intelligence database recorded suspect B as:

- an Indonesia-based 'ordering' customer, sending three IFTIs to Australia from Indonesia over a 10-day period, totalling more than AUD7,000. The 'details of payment' section of the IFTI report for these transactions was left blank by suspect B.
- an Indonesia-based beneficiary, indicating he received six IFTIs totalling more than AUD20,000 sent from Australia to Indonesia over a two-month period.

Law enforcement officers executed 10 search warrants across Victoria and New South Wales, with authorities seizing documents and computers, resulting in the arrests of suspects A and B.

Suspect A was charged with facilitating the proposed entry into Australia of a group of at least five non-citizens and providing material support to a person to engage in people smuggling activities contrary to the *Migration Act 1958*.

Suspect A was also charged with importing and possessing a marketable quantity of a border-controlled drug, namely methamphetamine, contrary to the *Criminal Code Act 1995* (Cwlth). It was alleged the drugs were sent via post to Australia from the Middle East and had an estimated street value of AUD750,000. He was sentenced to prison for eleven-and-a-half years for all offences.

Suspect B was charged with people smuggling contrary to the *Migration Act 1958*. He was found guilty of aggravated people smuggling and was sentenced to five years imprisonment.

Offence	Drug importation People smuggling
Customer	Individual
Industry	Banking (ADIs) Remittance services
Channel	Electronic
Report type	IFTI TTR
Jurisdiction	Domestic and international – Indonesia
Designated service	Account and deposit-taking services Remittance services (money transfers)
Indicators	Cash withdrawals conducted over multiple days Customer undertaking transactions that appear inconsistent with their profile and/or transaction history Multiple electronic transfers from third parties Multiple international funds transfers to a country of interest to authorities Multiple low-value international value transfers Unusually large volume of cash deposits and withdrawals

Case 9 – Suspicious funds transfers to Mexico unearthed million dollar drug trafficking syndicate

A suspicious matter report contributed significantly to a law enforcement operation which ultimately dismantled an international drug importation syndicate operating in Australia.

Authorities used AUSTRAC information to identify individuals of interest, establish links between syndicate members, support existing intelligence and identify financial transactions of interest to authorities.

Two suspects were convicted of attempting to possess commercial quantities of unlawfully imported border controlled drugs. One was sentenced to eight years and six months imprisonment, the other was sentenced to 17 years imprisonment.

The syndicate imported into Australia 14 kilograms of cocaine and 133 kilograms of methamphetamine with a combined estimated value of AUD14 million. The drugs were concealed in beer bottles in a consignment sent from Mexico.

The initial SMR disseminated by AUSTRAC to authorities detailed the financial activities of an individual who was later found to a member of the syndicate. The individual was found to be associated with two suspects (A and B) who were also members of the syndicate. The SMR included the following information:

- Over a four-day period the individual sent two international funds transfer instructions (IFTIs) of AUD9,000 each to Mexico.
- The funds transfers were paid for with cash.
- The transfers were seemingly 'structured' into amounts of less than AUD10,000 to avoid the threshold transaction reporting requirements.[9]

The SMR, combined with intelligence received from other authorities, prompted AUSTRAC to produce a financial intelligence report for its law enforcement partners detailing the financial activities of the syndicate.

AUSTRAC information was a significant source of intelligence used by authorities to identify links between key syndicate members. The information helped authorities link suspects who had not previously been associated with each other, including suspects A and B.

9 See the Glossary for a definition of 'structuring'.

Large cash deposits expose suspects A and B

Analysis of AUSTRAC information identified a number of threshold transaction reports (TTRs) which detailed large cash deposits made by suspect A. AUSTRAC information showed that:

- one year prior to the importation, suspect A made two cash deposits, worth AUD10,000 and AUD150,000, into his accounts on two different days
- in the four months preceding the importation, suspect A deposited approximately AUD160,000 cash into his accounts, staggered over four days. The value per transaction ranged between AUD10,000 and AUD70,000
- in the month preceding the importation, suspect A deposited AUD25,000 cash into his account
- a cash deposit funded an international funds transfer of AUD50,000 to an account in Turkey in the name of suspect A.

These deposits were believed to be illicit funds associated with the importation of drugs.

Analysis of AUSTRAC information also showed that two years prior to the importation suspect B deposited AUD130,000 cash into his personal bank accounts. The value per transaction ranged between AUD15,000 and AUD60,900. These transactions were reported to AUSTRAC via TTRs and significant cash transaction reports (SCTRs).

Searches of the AUSTRAC database revealed that members of the syndicate sent high-value IFTIs to various overseas beneficiaries:

- They transferred a total of AUD245,000 to multiple beneficiaries in Mexico over a three-year period. The value per transaction ranged from AUD200 to AUD9,000. The IFTIs were sent via remittance services and a financial institution.
- Syndicate members sent IFTIs totalling AUD1 million to an account in Turkey held in the name of suspect A. The value per transaction ranged from approximately AUD47,000 to AUD237,000. The funds were sent via banks over a 10-month period in the year preceding the importation.

Australian authorities received information from international counterparts in Turkey which revealed that the majority of the funds transferred to Turkey were transferred onwards to Mexico. Authorities believe these funds were transferred to Mexico to fund the drug importation. Suspect A withdrew approximately USD107,000 cash from his account while visiting Turkey.

Authorities executed search warrants on several properties and seized six kilograms of methamphetamine, weapons and ammunition. Also seized from suspect A's residential property were approximately 39 cases of empty beer bottles. Suspects A and B were arrested during the operation.

Suspects A and B were both convicted of attempting to possess commercial quantities of unlawfully imported border controlled drugs, namely cocaine and methamphetamine, contrary to the *Criminal Code Act 1995*.

Suspect A was sentenced to eight years and six months imprisonment, while suspect B was sentenced to 17 years imprisonment.

Offence	Drug importation
Customer	Individual
Industry	Banking (ADIs) Remittance services
Channel	Electronic Physical
Report type	IFTI SCTR SMR TTR
Jurisdiction	International – Mexico, Turkey
Designated service	Account and deposit-taking services Gambling services Remittance services (money transfers)
Indicators	Cash used to pay for international funds transfers High-value cash deposits High-volume account activity involving significant amounts of cash funds International funds transfers where an individual is both the ordering and beneficiary customer Large cash withdrawals in a high-risk jurisdiction Multiple customers conducting international funds transfers to the same overseas beneficiary Multiple international funds transfers to high-risk jurisdictions[10] Regular or multiple cash deposits just below the AUD10,000 cash transaction reporting threshold

10 See the Glossary for a definition of 'high-risk jurisdiction'.

Case 10 – Accountant's overseas tax evasion scheme landed clients in jail

AUSTRAC information assisted authorities to investigate a tax evasion scheme promoted and facilitated by an accountant in Australia.[11] The scheme used false invoices and loans to avoid tax. Authorities identified that a client of the accountant defrauded the Commonwealth of AUD2 million over a five-and-a-half year period.

The accountant was sentenced to six years imprisonment. The accountant's clients were sentenced to prison terms ranging from two to four years.

Authorities commenced an investigation into the accountant and a number of his clients, including suspect A.

Investigating authorities identified that suspect A operated an import business in Australia and was a participant in the tax evasion scheme operated by the accountant.

Suspect A and his wife were directors and shareholders of an Australian company (company 1). Suspect A was also a director and shareholder of another Australian company (company 2). An associate of suspect A was the co-director of company 2.

Authorities identified that the accountant controlled company 3, which was registered in Hong Kong and operated a bank account in Australia. This company was used to issue false invoices to companies 1 and 2.

False invoices

Over a five-and-a-half year period company 3 issued false invoices to companies 1 and 2 for supposed 'brokering services'. Suspect A paid the false invoices, which totalled more than AUD2 million, by directing companies 1 and 2 to pay company 3. Over the five-and-a-half year period, at suspect A's direction:

- company 1 paid company 3 a total of AUD1 million
- company 2 paid company 3 a total of AUD1 million.

The payment of the false invoices was made by either domestically transferring funds to company 3, or by company 2 issuing cheques made payable to company 3. For example, company 1 domestically transferred AUD50,000 to company 3 in one transaction, and company 2 issued cheques totalling AUD1 million made payable to company 3 over a six-month period.

The payments were supposedly for 'commissions' on commercial deals brokered by company 3. Enquiries revealed that company 3 was not a broker and no service had been provided to warrant the payments.

Companies 1 and 2 falsely claimed deductions in their tax returns for the 'commissions' paid to company 3, which reduced their taxable income.

11 'Tax evasion' involves taxpayers deliberately breaking the law and dishonestly abusing the tax system to obtain a financial benefit.

False loan

The funds paid to company 3, less the accountant's 10 per cent fee, were returned to suspect A and individuals associated with him.

Over the five-and-a-half year period, company 3 and other companies controlled by the accountant returned approximately AUD1.8 million of the funds originally paid by companies 1 and 2. The funds were distributed at suspect A's direction as follows:

- AUD100,000 by way of a loan to suspect A's business associate and co-director of company 2
- AUD200,000 to suspect A's wife
- AUD1.5 million to suspect A disguised as a 'loan'.

Analysis of AUSTRAC information identified two outgoing international funds transfer instructions (IFTIs) totalling AUD270,000 each, sent from company 3 to suspect A's bank account in Japan. The transfers represent part of funds returned to suspect A disguised as a 'loan'.

Suspect A claimed that the AUD1.5 million received from company 3 and other companies controlled by the accountant were a 'loan' from another company (company 4), which was registered in the British Virgin Islands and owned and controlled by the accountant. However, authorities found no evidence to support this claim: there was no record of any payments from company 4 to the suspect's personal bank accounts, company 4 did not have any bank accounts in Australia and it had not deposited any funds into any Australian banks.

Analysis of AUSTRAC data showed that suspect A and company 2 were both the ordering and beneficiary customers of international funds transfers from Australia to Japan totalling AUD1 million, sent over a period of three years.

Authorities believed these transfers were the proceeds of the tax evasion which were sent to Japan for the benefit of suspect A. In essence, suspect A directed companies 1 and 2 to make payments to company 3 in order for the funds to be transferred back to him tax free.

Authorities identified that suspect A spent approximately AUD400,000 of the funds received from companies controlled by the accountant on the demolition and rebuilding of his home, mortgage payments and living expenses.

Income tax inconsistencies

Authorities analysed the personal income tax returns of suspect A and identified that in one financial year he reported his gross income as AUD30,000. During the same financial year, AUD400,000 was deposited into a personal bank account held by suspect A, and AUD450,000 was withdrawn from the account.

Over the next three years, suspect A reported his gross personal income as AUD30,000 per year. Suspect A did not declare the AUD1.5 million he received from company A.

Authorities executed more than 20 search warrants on properties including the accountant's Australian accountancy business and suspect A's residential property, from which large quantities of documents were seized.

Charges and sentencing

Suspect A was charged with:

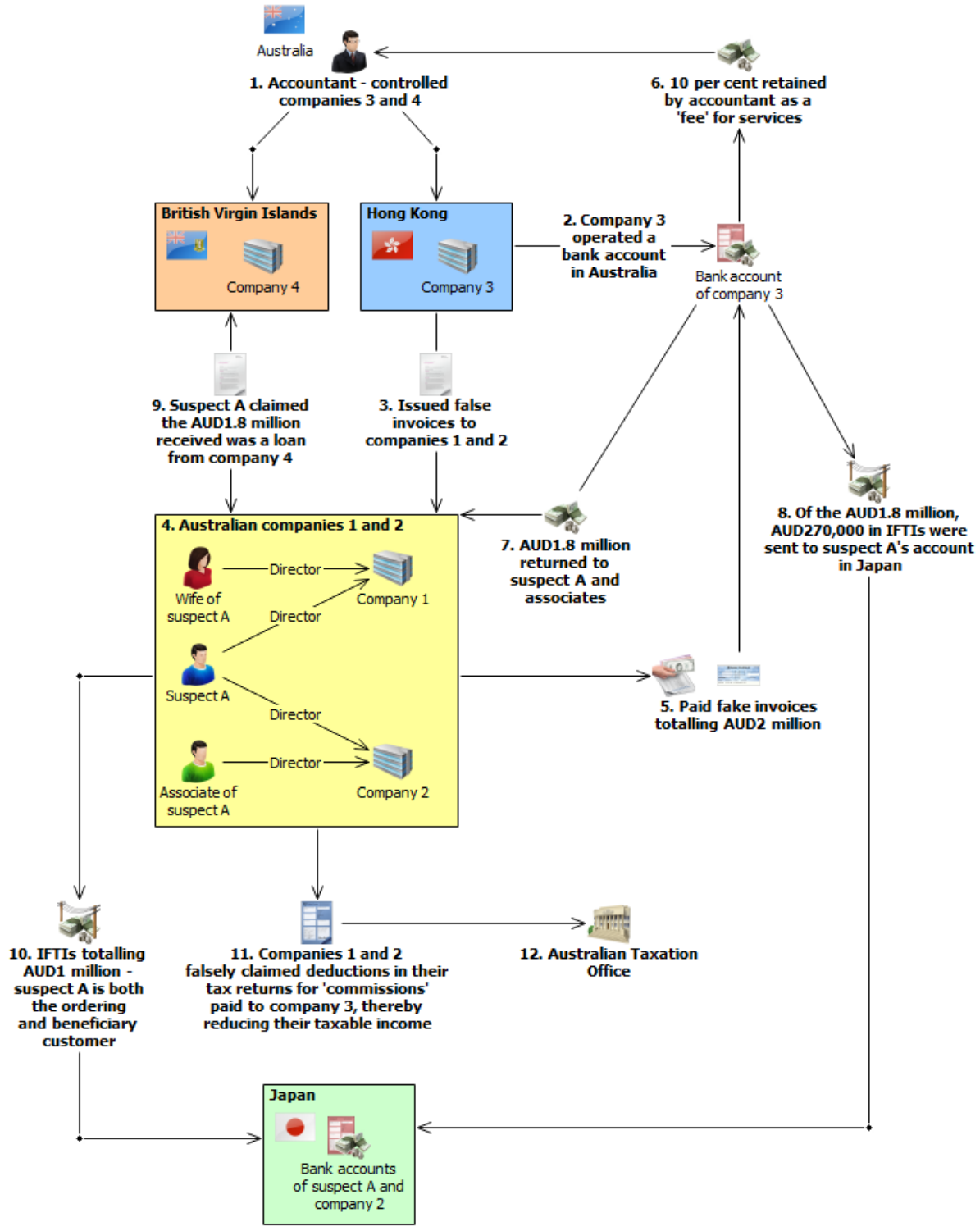
- three counts of being knowingly concerned in defrauding the Commonwealth under the *Crimes Act 1914*
- one count of aiding in general dishonesty causing a loss under the *Criminal Code Act 1995*
- one count of aiding in obtaining a financial advantage by deception under the Criminal Code Act
- four counts of obtaining a financial advantage by deception under the Criminal Code Act.

Suspect A was convicted and sentenced to four years imprisonment and required to pay a penalty of AUD1 million.

The accountant was convicted of aiding and abetting the commission of fraud against the Commonwealth and was sentenced to six years imprisonment.

A further three clients of the accountant were convicted of obtaining a financial advantage by deception. Two of the clients were sentenced to three years imprisonment and the third client was sentenced to two years imprisonment.

Offence	Tax evasion
Customer	Business Foreign entity Individual
Industry	Banking (ADIs)
Channel	Electronic
Report type	IFTI
Jurisdiction	International – British Virgin Islands, Hong Kong, Japan
Designated service	Account and deposit-taking services
Indicators	Customer is both the ordering and beneficiary customer for multiple outgoing international funds transfers Customer receives international funds transfers described as 'loan' Customer undertaking complicated transfers without a business rationale High-value international funds transfers from Australia with no apparent logical reason Use of an accountant to facilitate unusually complicated transactions Use of tax secrecy jurisdictions



Case 10 – Accountant's overseas tax evasion scheme landed clients in jail

Case 11 – Complex tax avoidance scheme hid funds in Samoa and New Zealand

AUSTRAC information assisted authorities to identify offshore bank accounts and international funds transfers in relation to a complex tax avoidance scheme involving funds transfers between Australia, Samoa and New Zealand.[12] The scheme involved the use of an offshore superannuation fund and a loan arrangement to avoid tax.

Authorities ultimately issued amended tax assessments to the individuals involved, resulting in approximately AUD2 million in additional tax, penalties and interest.

This complex case is presented in four parts:

- Part 1 covers international transfers made to an offshore superannuation fund and the rapid return of these funds to Australia.
- Part 2 covers the ongoing international transfers of funds under a fictitious loan arrangement over ten years.
- Part 3 describes the transfer of this loan arrangement to another Australian company when the original company went into liquidation. This covers a further four years worth of activities.
- Part 4 shows how a charity became involved in the loan arrangement.

Individuals A and B were family members who owned and controlled a group of Australia-based companies.[13] The companies undertook motor vehicle repairs and sold automotive products in Australia.

12 'Tax avoidance' involves taxpayers avoiding tax by deliberately using arrangements that provide tax benefits that are outside the intent of the law. See http://www.ato.gov.au/General/Tax-evasion-and-crime/Our-key-focus-areas/Tax-avoidance-schemes/.

13 The term 'group' is used here in its ordinary sense, rather than its legal sense under the *Corporations Act 2001*.

Arrangement 1 – Offshore superannuation fund

Individuals A and B received advice from an accountant about the purported benefits of offshore superannuation funds. As a result, individual A instructed his accountant to establish a superannuation fund in Samoa. The superannuation fund was established and a Samoa-based company acted as trustee of the fund.

Company 1 was owned and controlled by individuals A and B, and formed part of the Australia-based group. Company 1 made two contributions of AUD100,000 each to the superannuation fund in Samoa. The two international funds transfers were undertaken over an eight-day period and the funds were subsequently provided to a private bank in Samoa.

The Samoa-based private bank returned the AUD200,000 to company 1 in Australia in two international funds transfers of AUD100,000. The transfers were made within one month of the initial contributions being made to the superannuation fund. The two transfers of AUD100,000 were described as a 'loan' from the bank to company 1. There was no loan agreement in place to support the transfer of these funds.

Company 1 subsequently claimed deductions for the AUD200,000 offshore superannuation contribution in its tax return and was assessed as liable for less tax than it should have been, thereby avoiding its tax obligations.

The deductions were later disallowed and deemed not deductible under the Income *Tax Assessment Act 1936*. An amended tax assessment was issued to company 1 by the Australian Taxation Office (ATO).

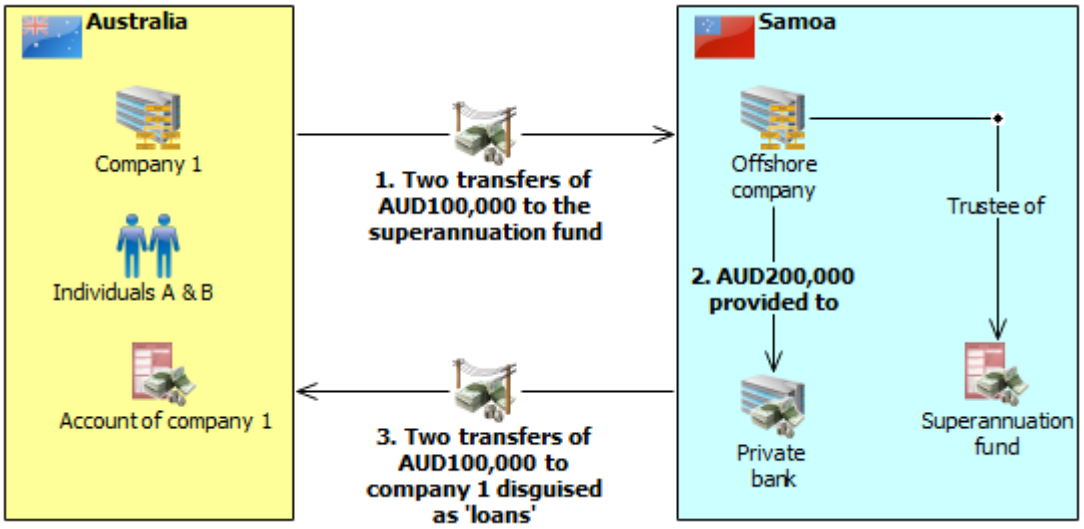


Figure 2 – Transfers to offshore superannuation fund in Samoa (Arrangement 1)

Arrangement 2 – Loan arrangement (years 1 to 10 of the scheme)

Individuals A and B entered into a loan agreement on behalf of company 1 with the Samoa-based private bank. This arrangement was separate to the AUD200,000 'loan arrangement' described above in 'Arrangement 1'. This second loan arrangement remained in place for more than 10 years and was later transferred to other companies in the group.

A subsidiary company of the Samoa-based private bank held a bank account in New Zealand. The subsidiary was instrumental in facilitating payments between the Samoa-based private bank and company 1, or companies and individuals associated with the Australia-based group.

In subsequent years, in accordance with the loan agreement, companies controlled by individuals A and B made annual 'interest' payments on the loan to the bank or its subsidiary, by way of international funds transfer.

The interest payments were then borrowed back from the Samoa-based private bank or its subsidiary, with funds transferred back to Australia to either company 1 or other companies and individuals associated with the group. The returned funds were generally described as 'draw downs' or 'loans'.

This complex 'round robin' tax avoidance arrangement aimed to disguise the funds movements as legitimate transactions associated with the loan. In reality, any funds sent overseas ultimately returned to the original beneficiary, either company 1 or other companies in the Australia-based group.[14]

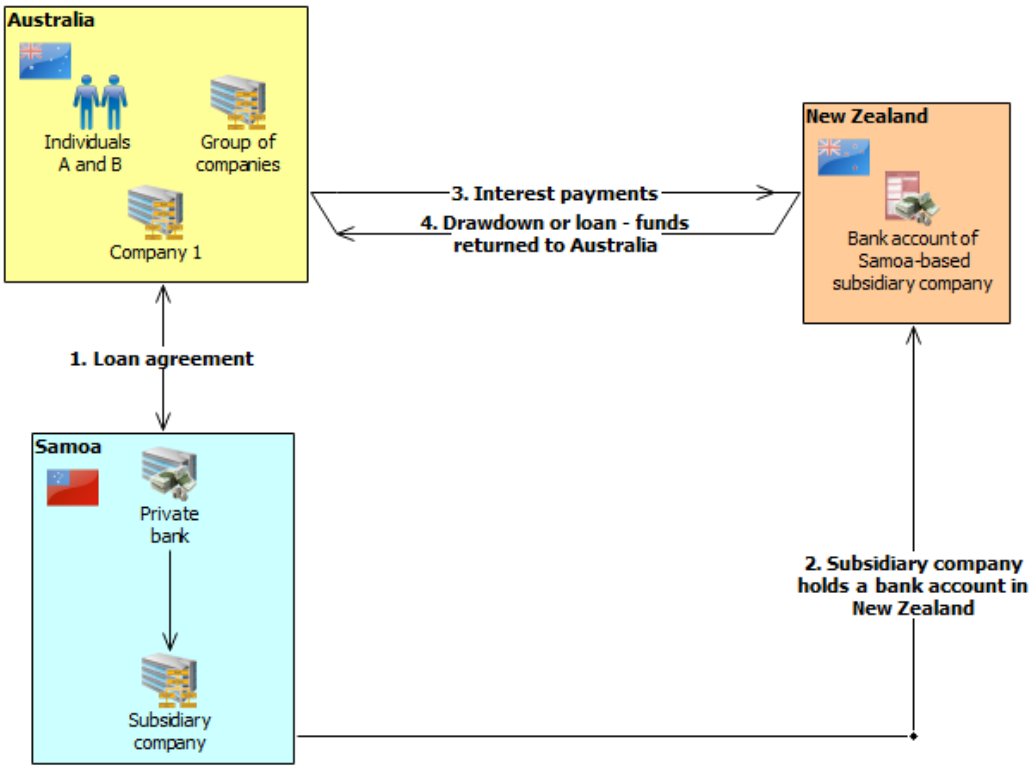


Figure 3 – Transfers to and from the subsidiary's New Zealand bank account disguised as loan payments (Arrangement 2)

14 See the Glossary for a definition of 'round robin tax evasion scheme'.

Transfer of the loan arrangement from company 1 to company 2 (years 11 to 14 of the scheme)

Company 1 changed its name and subsequently went into liquidation. As a result, the ATO was forced to write off a tax debt of AUD800,000 which had accrued on the income tax account of the company.

After company 1 went into liquidation the loan liability was transferred to company 2. Company 2 was incorporated in Australia and was associated with company 1 and individuals A and B. The loan liability at this time was approximately AUD3 million.

Company 2 continued to utilise the tax avoidance arrangement by making interest payments on the loan to the Samoa-based private bank via its subsidiary. Each time company 2 made interest payments to the bank, the bank's subsidiary subsequently transferred funds into company 2's bank accounts in Australia. These transfers were described as 'loan draw downs'.

Information in IFTIs, combined with information received by authorities, revealed four years worth of incoming and outgoing international fund transfers between company 2 in Australia and the bank's subsidiary company, which held a bank account in New Zealand.

Company 2 claimed that the funds received as 'loan draw downs' were lent to companies in the Australian group of companies by way of interest-free loans.

Introduction of an Australian charitable organisation (years 15 to 16 of the scheme)

To further complicate the loan arrangement, another Australian organisation was introduced to the transaction activity. This organisation was unrelated to the main group of companies and was described as a charitable organisation. The organisation facilitated the transfer of funds between the bank's New Zealand subsidiary and the Australian group of companies.

AUSTRAC information, combined with other information received by authorities, showed:

- company 2 sent funds representing 'interest payments' to the New Zealand bank account of the bank's subsidiary
- the subsidiary transferred funds, in similar amounts to the 'interest payments', from its New Zealand bank account to the bank account of the Australian charitable organisation. The transfers were described as 'draw downs' and 'transfer of funds'
- four to five days later, the charitable organisation conducted a domestic transfer for a similar amount into the bank account of company 2, described as a 'loan draw down'.

Figure 4 on the following page shows the direction and value of incoming and outgoing IFTIs between company 2, the subsidiary's New Zealand-based bank account and the Australian charitable organisation.

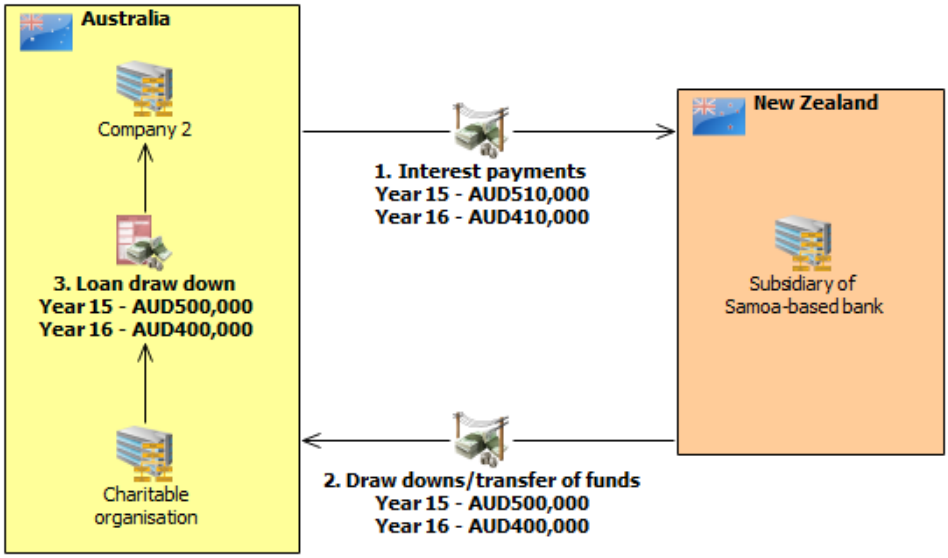


Figure 4 – Use of Australian charitable organisation to facilitate payments

In its tax returns, company 2 claimed deductions for interest expenses and fees paid to the Samoa-based private bank. As a result of claiming these deductions, company 2 reduced its taxable income and was assessed as liable for less tax than it should have been, thereby avoiding its obligations.

It was later determined that these expenses were not deductible and the deductions were disallowed. Amended assessments for company 2 were issued resulting in approximately AUD2 million in additional tax, penalties and interest.

Offence	Tax avoidance
Customer	Business
	Foreign entity
	Individual
Industry	Banking (ADIs)
Channel	Electronic
Report type	IFTI
Jurisdiction	International – Samoa, New Zealand
Designated service	Account and deposit-taking services
Indicators	Customer receives international funds transfers described as 'loan draw down' or 'loan advance'
	Customer undertaking complicated transfers without a business rationale
	International funds transfers to and from a high-risk jurisdiction
	Multiple high-value international funds transfers to and from Australia with no apparent logical reason
	Outgoing funds transfers sent to offshore entities followed soon after by incoming funds transfers of similar amounts from the same offshore entities
	Use of charitable organisation with a lack of business rationale
	Use of third-party company accounts in an attempt to complicate transaction activity
	Use of third-party or family member accounts

Case 12 – Street drugs smuggled into Australia inside stuffed toys and nappies

Suspicious matter reports assisted law enforcement with an investigation into a sophisticated drug importation criminal syndicate. AUSTRAC information also assisted authorities to identify the scale of the syndicate's financial activity.

A member of the syndicate was charged with attempting to import a marketable quantity of border-controlled drugs and precursors. He was sentenced to a maximum of six years and eight months imprisonment.

Law enforcement authorities disrupted a complex and sophisticated Adelaide-based criminal syndicate, which used stuffed toys, cushions and nappies to import large quantities of pseudoephedrine and methamphetamine into Australia. Authorities estimated that the drugs had a street value of AUD6.6 million.

The investigation was initiated after law enforcement officers examined cargo imported into Australia from Hong Kong and found approximately 126 grams of crystal methamphetamine hidden within a stuffed toy and concealed among other clothing.

Over a 13-day period authorities identified further drugs imported into Australia including approximately 535 grams of crystal methamphetamine concealed in stuffed toys and the lining of nappies and approximately 7 kilograms of pseudoephedrine concealed in cushions. The investigation led to the arrest of suspect A, who allegedly directed the importation of drugs.

Law enforcement authorities allege that in addition to importing multiple packages to various locations in Adelaide, the criminal syndicate also made multiple international funds transfers to China to fund the importation of drugs. AUSTRAC data showed that over a one-year period, syndicate members sent international funds transfer instructions (IFTIs) totalling more than AUD137,000 to China.

The AUSTRAC database revealed two suspicious matter reports (SMRs) involving a syndicate member:

- A reporting entity submitted an SMR following observations that, in one month, syndicate member #1 sent 15 IFTIs totalling more than AUD67,000 to China. The reporting entity formed its suspicions on the basis that:
  - all of the outgoing IFTIs were paid for with cash, in structured amounts below the AUD10,000 cash reporting transaction threshold
  - the IFTIs were sent to multiple beneficiary customers in a high-risk jurisdiction[15]
  - the volume and frequency of the funds transfers undertaken by the syndicate member was higher than normal for an average customer.
- Another reporting entity submitted an SMR detailing how another customer, syndicate member #2, attended a branch to deposit cash and conduct two IFTIs totalling AUD33,000 to China. The SMR noted that the funds were sent to the same China-based beneficiary that an apparently unrelated customer had sent IFTIs to the previous day. Further investigation revealed that this 'unrelated customer' was syndicate member #1 referred to above.

15 See the Glossary for a definition of 'high-risk jurisdiction'.

The bank identified that syndicate member #1 had attended the branch the day before and deposited AUD9,000 cash, in amounts of AUD1,000 and AUD8,000. The syndicate member then withdrew AUD8,000 and undertook an IFTI for AUD8,000 to the common beneficiary customer in China.

The reporting entity contacted syndicate member #1 about these transactions. He was guarded and evasive when asked about the reason for the transfer of funds to China, and his relationship to syndicate member #2 (who had sent AUD33,000 to the same individual in China the next day).

The bank determined that it was unusual that a total of AUD41,000 had been transferred to the same beneficiary in China over two consecutive days by two different customers. This, combined with syndicate member #1's reluctance to explain or provide further details about the transaction and the bank's inability to determine the purpose of the funds transfers, prompted the bank to submit an SMR to AUSTRAC.

The AUSTRAC database also showed that suspect A had sent 11 IFTIs to China totalling more than AUD37,000.

AUSTRAC information also assisted authorities to identify the scale of the activity. Since January 2008, syndicate members were linked to approximately 400 outgoing IFTIs to China totalling approximately AUD3 million and 40 outgoing IFTIs to Hong Kong totalling approximately AUD400,000.

Law enforcement authorities executed search warrants at two residential premises. Various items were seized including more than AUD14,000 cash, SIM cards, computers, documents, fake Chinese and Australian identification, stuffed toys with their contents removed, drugs paraphernalia including scales and 'deal' bags, and containers containing residual trace elements of methamphetamines.

Suspect A was charged with importing and attempting to import a marketable quantity of border-controlled drugs and precursors. He was sentenced to a maximum of six years and eight months imprisonment.

Offence	Drug importation
Customer	Individual
Industry	Banking (ADIs) Remittance services
Channel	Electronic Physical
Report type	IFTI SMR
Jurisdiction	International – China, Hong Kong
Designated service	Account and deposit-taking services Remittance services
Indicators	Customer is reluctant to provide further details about a transaction Multiple customers conducting international funds transfers to the same overseas beneficiary in a short time frame Multiple international funds transfers paid for in cash in amounts just below the AUD10,000 reporting threshold Multiple international funds transfers to a high-risk jurisdiction

Case 13 – Crime syndicate recruited Malaysian nationals for major credit card fraud

AUSTRAC information was used to verify the identities of an organised crime syndicate undertaking credit card fraud. A number of suspicious matter reports also assisted authorities to unravel the group's illicit financial activities.

Two members of the syndicate were charged with fraud-related offences. One was sentenced to two years and three months imprisonment and the other to 12 months imprisonment.

A Melbourne-based Asian organised crime syndicate operated a company arranging for overseas students to migrate to Australia. This company was also used to facilitate a credit card shopping fraud scheme. The syndicate recruited Malaysian nationals with significant gambling debts to assist in fraudulently purchasing high-value portable goods which could be resold easily.

The syndicate used false identity documents to create fake identities for the recruits. These documents were either fraudulently produced or were genuine documents obtained in false names. The false identities were used to obtain legitimate identity documents – for example, drivers licences – which were then used to set up bank accounts and apply for bank loans.

The syndicate provided the recruits with fraudulently obtained items such as credit cards. The recruits were then taken to several shopping centres around Australia to purchase portable high-value goods such as laptops, navigation devices, personal music devices, jewellery, department store gift cards and premium alcohol. The recruits provided the goods to the syndicate who on-sold the items to unwitting third parties for cash. The recruits were given a portion of the proceeds to pay off personal gambling debts.

AUSTRAC information was used by authorities to verify identities used by the syndicate and to identify related international funds transfer instructions (IFTIs). A number of suspicious matter reports (SMRs) also assisted authorities to unravel the group's illicit financial activities. AUSTRAC analysis and law enforcement investigations suggested that syndicate members used a portion of their criminal proceeds to purchase property, while other funds were laundered through Australian casinos.

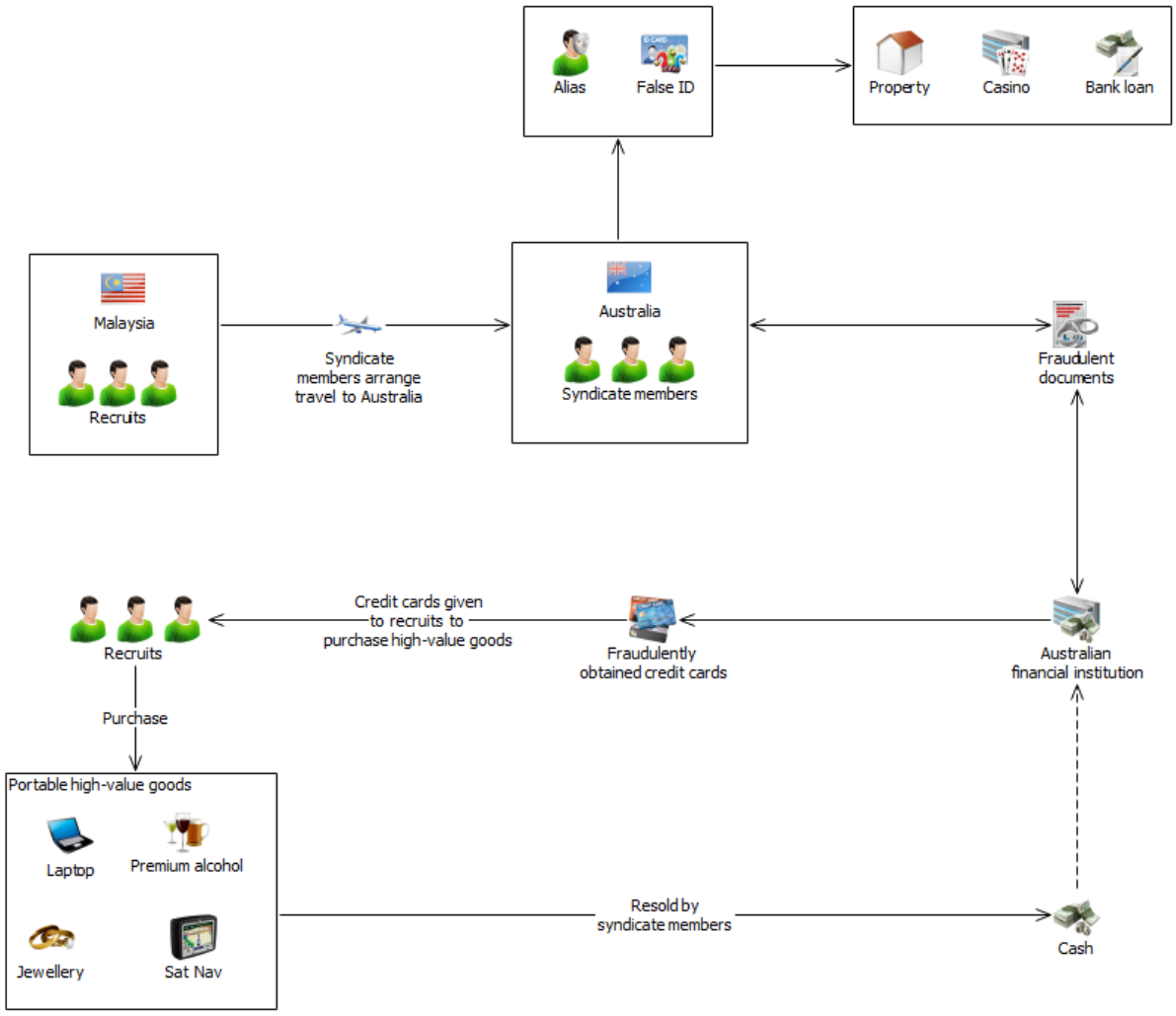
One SMR submitted by a casino revealed that a member of the syndicate had converted AUD32,000 of gaming chips for cash, providing a casino identity card that was not linked to any 'rated play' (gambling activity), at the casino.

Further investigation by the casino found that the same person had previously supplied a different casino identity card for other transactions on the same day. Significant cash transaction reports (SCTRs) submitted to AUSTRAC also linked the syndicate member to four other gaming chip cash-outs totalling AUD59,000 over a 14-month period.[16] The cash-outs were either conducted on the same day, or in the same week.

Two members of the syndicate were charged with fraud-related offences. One was sentenced to two years and three months imprisonment and the other to 12 months.

16 See the Glossary for a definition of 'chip cash-out'

Offence	Fraud Money laundering
Customer	Individual Business
Industry	Banking (ADIs) Gambling services
Channel	Electronic Physical
Report type	IFTI SCTR SMR
Jurisdiction	Domestic International – Malaysia
Designated service	Account and deposit-taking services Gambling services
Indicators	Multiple chip cash-out occurring on the same day Significant chip cash-out with minimal play at a casino Use of false identification



Case 13 – Crime syndicate recruited Malaysian nationals for major credit card fraud

Case 14 – Welfare recipients found with $75,000 cash and 15 kilograms of cannabis

AUSTRAC information helped initiate an investigation that resulted in the arrest of three suspects and the seizure of approximately 15 kilograms of cannabis. Authorities restrained a number of assets, including AUD100,000 in cash suspected to be the proceeds of crime, a property and numerous vehicles.

One suspect was sentenced to four years and 10 months imprisonment. The other suspect received a suspended sentence of two years and nine months imprisonment.

Information held by authorities indicated that a woman (suspect A) and husband (suspect B) had accumulated substantial assets, which was inconsistent with their declared income.

Additionally, a credit union submitted a suspicious matter report (SMR) detailing the financial activities of the suspects. AUSTRAC forwarded the SMR to authorities, which detailed the following:

- suspects A and B held a joint account with the reporting entity
- suspect A telephoned the credit union and indicated that she wanted to withdraw AUD15,000 cash from her personal account
- credit union staff advised the suspect that withdrawing AUD15,000 cash required the completion of a significant cash transaction report (SCTR)
- over two consecutive days, suspect A attended the credit union branch and withdrew AUD9,800 and AUD5,200 respectively.

The cash withdrawals totalled AUD15,000 and appeared to be 'structured' into two separate transactions to avoid the SCTR requirement.[17] Subsequent investigation of the account activity by social welfare investigators identified that:

- suspects A and B received government welfare payments
- a large number of transactions were made at a casino
- the account received large cheque deposits.

17 See the Glossary for a definition of 'structuring'

Analysis of AUSTRAC information identified additional SMRs submitted by a credit union. The SMRs included the following information:

- suspect A was a signatory to a credit union account held in a relative's name
- suspect A periodically deposited cash into the relative's account. Over a one-month period the relative's account received four cash deposits totalling AUD20,000 structured into amounts ranging from AUD2,000 to AUD9,000
- suspect A attended a branch of the credit union with her relative and they deposited AUD9,000 and AUD6,000 cash respectively into their personal accounts, at different counters
- credit union staff observed that the relative appeared 'nervous' while conducting cash deposits
- a cheque for AUD50,000 was withdrawn by the relative from his account to purchase a motor vehicle.

Enquiries conducted by authorities identified that:

- over a six-year period approximately AUD1.37 million was deposited into the accounts of suspects A and B
- the suspects purchased numerous assets including a house, two motor vehicles and three motorcycles
- suspect B frequently travelled overseas.

Analysis of AUSTRAC information showed that in the same year the SMRs were reported to AUSTRAC, suspect B completed an international currency transfer report (ICTR), which indicated he was carrying cash worth approximately AUD16,000 when he departed Australia for the Philippines.[18]

Enquiries showed that suspects A and B's income did not support their lifestyle. The SMRs, combined with information held by authorities, prompted law enforcement to investigate the suspects' unexplained wealth.

Further law enforcement investigations revealed that suspects A and B had obtained approximately 15 kilograms of cannabis and were arranging for a courier (suspect C) to transport the cannabis interstate.

Law enforcement officers intercepted a motor vehicle and found the cannabis concealed in the side panels of the vehicle. Suspect C was arrested and charged with possessing cannabis for sale or supply.

A search warrant was executed at suspect A and B's home. Authorities seized approximately AUD75,000 cash, numerous receipts for goods worth AUD400,000 purchased using cash, and various documents that indicated suspects A and B were trafficking in cannabis. Suspects A and B were arrested.

Suspect A pleaded guilty to:

- aiding, abetting or procuring another to traffic in a substance that is a controlled drug under the *Criminal Code Act 1995*
- jointly possessing approximately AUD75,000 being the proceeds of crime under the Criminal Code Act
- jointly dealing with approximately AUD330,000 being the proceeds of crime under the Criminal Code Act
- possessing a motor vehicle being the proceeds of crime under the Criminal Code Act.

18 Under the *Financial Transaction Reports Act 1988*, international currency transfer reports (ICTRs) were submitted when currency (coin or paper money) of AUD10,000 or more (or the foreign equivalent) was carried, mailed or shipped into or out of Australia.

Suspect A was sentenced to four years and 10 months imprisonment.

Suspect B died and court proceedings against him were discontinued.

Suspect C pleaded guilty to possessing cannabis for sale or supply and received a suspended sentence of two years and nine months imprisonment.

Law enforcement restrained a house, two motor vehicles, three motorcycles, approximately AUD75,000 in cash and AUD25,000 in a bank account.

The social welfare investigation revealed both suspect A and B had each accumulated debts of AUD69,944.45 for welfare payments they were not entitled to.

Offence	Drug trafficking Money laundering Welfare fraud
Customer	Individual
Industry	Banking (ADIs)
Channel	Physical
Report type	ICTR SMR
Jurisdiction	Domestic and international – Philippines
Designated service	Account and deposit-taking services
Indicators	Account activity inconsistent with customer profile Customer and relative(s) attend the same branch and make structured cash deposits into their own accounts at the same time Customer is a signatory to a relative's account and makes large cash deposits to the account High-value cash deposits Regular or multiple deposits below the AUD10,000 reporting threshold (that is, structured cash deposits) Third-party or relative appears to be nervous while conducting transactions

Case studies

Remittance services

Case studies – Remittance services (money transfers)

Case 15 – Suspect stockpiled illegal firearms and explosives

Law enforcement identified a suspect who appeared to be importing components used to build or modify a prohibited type of assault rifle. Authorities used AUSTRAC information to identify the suspect's online payment account and other associated financial activity.

The suspect was arrested and charged with various firearms offences.

Law enforcement consulted a number of data sources including the AUSTRAC database to further their investigation. AUSTRAC identified the suspect's online payment account and other associated financial activity. Once this account information was identified, law enforcement approached the relevant online payment providers to obtain the suspect's account details and other identifying information.

AUSTRAC information revealed that, over a five-year period, the suspect had sent approximately 160 low-value international funds transfer instructions (IFTIs) totalling AUD15,500. All IFTIs were below AUD1,000 and were sent via an online payment service to various overseas destinations.

The information provided by AUSTRAC, along with data from other sources, enabled law enforcement officers to obtain a search warrant for the suspect's residence.

During the search law enforcement seized two revolvers, a sawn-off shotgun, a rifle, various parts for assault rifles and other assorted gun parts, most of which had been imported illegally from overseas. The officers also found equipment to manufacture guns, hundreds of rounds of ammunition, body armour, machetes, three hand grenades, a claymore mine and an improvised explosive device.

The suspect was arrested and charged with various firearms offences under the *Firearms Act 1996* (NSW) including possessing, using, storing and manufacturing firearms.

Offence	Firearm importation
Customer	Individual
Industry	Remittance services
Channel	Electronic
Report type	IFTI
Jurisdiction	International
Designated service	Remittance services (money transfers)
Indicators	Low-value international funds transfers

Case 16 – International crime syndicate used underground banking to launder massive drug profits

AUSTRAC assisted an investigation which disrupted a global crime syndicate involved in money laundering and the importation of more than 30 kilograms of methamphetamine into Australia.

Three suspects were arrested and charged with importing a commercial quantity of a border controlled drug.

The syndicate operated a 'hawala'-type remittance system with cells based in Australia, the United Arab Emirates (UAE) and Nigeria. The syndicate head was located in Lebanon.[19]

The cells in Australia were headed by an Iranian national (suspect A) and an Iraqi-born Australian citizen (suspect B). The head of the syndicate coordinated the distribution of cash payments from drug trafficking networks operating in Australia to suspects A and B.

Suspect A operated a business in the Iranian community facilitating the immigration of Iranian nationals to Australia and other countries. Most of suspect A's financial activity involved large cash deposits (reported to AUSTRAC as threshold transactions reports, or TTRs) and regular incoming international funds transfer instructions (IFTIs) from companies in Canada, Iran, Slovenia, the UAE and Turkey.

TTRs received by AUSTRAC showed that, over a six-year period, suspect A received AUD715,000 in large cash deposits, while AUD63,000 cash was withdrawn from bank accounts associated with the suspect. Over that same period, the suspect and his company were the beneficiary of 41 incoming IFTIs totalling AUD521,000.

Suspect A was also the subject of two suspicious matter reports (SMRs) submitted by a bank. The SMRs described the various activities observed that gave it grounds for suspicion:

- suspect A's unusual account activity
- funds being sent to/received from high-risk jurisdictions
- large cash deposits made at different bank branches on the same day
- third parties making cash deposits into suspect A's account.

Over a one-year period suspect B was the ordering customer for 56 outgoing IFTIs totalling AUD244,000. Suspect B sent the funds to approximately 38 overseas-based beneficiary customers in 12 different countries, with the top five countries being the United States, Lebanon, China, Luxembourg and Syria. All but six IFTIs were conducted through remittance dealers. Over the one-year period suspect B conducted multiple 'same-day' IFTIs, on the majority of occasions conducting the transactions through different remitters.

19 See the Glossary for a definition of 'hawala'

Suspect B was also the subject of two SMR reports submitted by a bank, detailing the following activity:

1. Suspect B deposited cash into third-party bank accounts, with one beneficiary account holder identified to be an Iranian national without any work entitlements in Australia.
2. The suspect's trading account received regular large cash deposits, which were followed by cheque withdrawals issued to third parties.
3. Suspect B's mortgage account exhibited unusual transaction behaviour, being used for very large cash deposits and withdrawals (worth hundreds of thousands of dollars).
4. The suspect made many large cash deposits; behaviour which was inconsistent with the suspect's claimed occupation as a shop assistant.

Law enforcement also investigated the activities of a third suspect, suspect C, because of his involvement with a suspected money launderer. Authorities believe that suspect C arranged to transfer AUD300,000 to Mexico using the unregistered remittance service provided by suspect B. Suspect B was not registered with AUSTRAC as a remittance service provider.

Suspect C was arrested as he was departing Australia on a flight to Mexico. In his possession was USD9500, AUD660, two diamonds valued at AUD50,000 each and casino chips valued at AUD170,000.

A search of the AUSTRAC database showed that suspect C had a gambling turnover of AUD11 million over a three-month period. Suspect C was also the subject of four SMRs, which detailed his unusual gambling activity and practice of making cash deposits in amounts just below the AUD10,000 reporting threshold. The suspect conducted multiple, same-day gambling-related transactions on a regular basis. The gambling-related transactions were in close succession, which suggested the suspect was undertaking a bare minimum of gambling in between transactions.

The three suspects were arrested and charged with importing a commercial quantity of a border controlled drug contrary to the *Criminal Code Act 1995*. Suspect C was also charged with dealing in money or property valued in excess of AUD100,000, which is believed to be the proceeds of crime, contrary to section 400.4 of the Criminal Code Act.

Offence	Drug trafficking Money laundering
Customer	Individual Business
Industry	Banking (ADI) Gambling services Remittance services
Channel	Electronic Physical
Report type	IFTI SMR TTR
Jurisdiction	International – primarily Canada, Iran, Lebanon, Mexico, Nigeria, Slovenia, Syria, Turkey, United Arab Emirates
Designated service	Account and deposit-taking services Gambling services Remittance services (money transfers)
Indicators	Cash deposits into third-party accounts High-value transactions inconsistent with customer profile High-value/volume gambling transactions with minimal gambling activity International funds transfers to high-risk jurisdictions Large cash deposits made at different bank branches on the same day Multiple same-day gambling activity Unusual transaction activity through business accounts, suggesting the account is being used for unregistered remittance activity

Case 17 – AUSTRAC information identified Australian victim of $2 million overseas investment scam

AUSTRAC information was instrumental in identifying an Australian victim who sent approximately AUD2 million to a highly organised international crime syndicate committing 'advance fee' fraud. [20]

Using this information, authorities were able to identify the victim and discourage him from sending more money to the international crime group.

AUSTRAC analysis of international funds transfer instruction (IFTI) reports showed that over a seven-year period an Australian individual sent AUD1.2 million to multiple overseas beneficiaries in Ghana, Lebanon, Malaysia, Nigeria, Spain and the United Kingdom. The IFTIs ranged in amounts between AUD200 to AUD123,000 and were sent via various remittance services and banks.

AUSTRAC also identified several relevant suspicious matter reports (SMRs) in its database and disseminated these to Australian authorities. The SMRs showed:

- The individual used cash to fund outgoing IFTIs to multiple beneficiaries in Egypt, Lebanon, Nigeria, Spain, Sri Lanka and the United Kingdom.
- The IFTIs were for amounts ranging between AUD700 and AUD8,500.
- The funds were transferred via remittance services.

Authorities analysed AUSTRAC financial intelligence and identified that the individual was a likely victim of fraud. They then contacted the victim to alert him that he was probably being scammed and warn him not to send any more money overseas.

Further investigation revealed that the victim communicated with the overseas fraudsters over the internet. The fraudsters invited the victim to send money to recover allegedly 'lost funds' and to establish investments in Australia.

The victim sent a total of AUD2 million to the fraudsters. The victim believed the funds were for various 'fees and taxes', which, once paid, would secure the release of GBP32 million worth of lost funds from the United Kingdom.[21]

The victim stopped sending funds after authorities contacted him. This is an example of authorities using AUSTRAC information to investigate a highly organised scheme by international criminal groups to defraud Australian citizens.

20 See the Glossary for a definition of 'advance fee fraud'.

21 GBP (Great Britain Pounds).

Offence	Fraud
Customer	Individual
Industry	Banking (ADIs) Remittance services
Channel	Electronic Physical
Report type	IFTI SMR
Jurisdiction	International – Egypt, Ghana, Lebanon, Malaysia, Nigeria, Spain, Sri Lanka, United Kingdom
Designated service	Account and deposit-taking services Remittance services (money transfer)
Indicators	High volume of international funds transfers from Australia for no apparent logical reason International funds transfers to a high-risk jurisdiction

Case 18 – Suspicious million dollar transfers undid major methamphetamine operation

Multiple law enforcement agencies worked together to dismantle a major drug syndicate operating in Australia and Vietnam. The investigation uncovered one of the most elaborate methamphetamine operations in Victoria's history and led to the arrest of eight suspects.

AUSTRAC information detailed international funds transfers undertaken by the syndicate.

Law enforcement targeted the drug syndicate after monitoring the financial activity and assets belonging to the suspects, most of whom were operating from Vietnam.

Analysis of AUSTRAC information by law enforcement showed that over a 12-month period, approximately AUD24 million was sent via international funds transfer instructions (IFTIs) to Vietnam. All IFTIs were paid for entirely with cash. The syndicate mainly used remittance dealers to send the outgoing IFTIs. Law enforcement also believed that the individuals sending the funds were using false driver licences and credit cards.

The syndicate was the subject of 53 suspicious matter reports (SMRs). The majority of these were submitted by the remittance providers facilitating the outgoing IFTIs to Vietnam. The grounds for suspicion mainly related to the large amounts of cash possessed by the network and the transfer of funds to common beneficiaries in Vietnam.

Banking institutions also submitted four SMRs related to the syndicate, with the nominated grounds for suspicion including suspicious cash activity undertaken by the syndicate members, including apparent 'structuring' of account deposits and withdrawals. The SMRs noted that some of the beneficiary customers in Vietnam shared the same address and the large amounts of cash sent by the syndicate were inconsistent with the stated occupations of many of its members.

Eight members of the syndicate were arrested and charged with trafficking a large commercial quantity of methamphetamine. They were remanded in custody.

Offence	Drug trafficking
Customer	Individual
Industry	Banking (ADIs) Remittance services
Channel	Electronic Physical
Report type	IFTI SMR
Jurisdiction	International – Vietnam
Designated service	Account and deposit-taking services Remittance services (money transfers)
Indicators	Financial activity does not match established customer profile Large international funds transfers to common beneficiaries Large amounts of cash to pay for international funds transfers Multiple customers conducting international funds transfers to the same overseas beneficiary Multiple international funds transfers to a high-risk jurisdiction Multiple international funds transfers to beneficiaries with same address Structuring of cash deposits and withdrawals over a period of time to avoid reporting requirements Use of false identification to conduct transactions

Case 19 – Director of remittance business jailed for laundering cash for criminals

AUSTRAC provided financial intelligence to assist law enforcement with their investigation into a remitter suspected of laundering illicit funds for crime syndicates.

AUSTRAC analysis identified additional entities, bank accounts and telephone numbers associated with the remitter. The remittance company director was charged and pleaded guilty to dealing with money reasonably suspected to be the proceeds of crime. He was sentenced to three months imprisonment and given an 18-month good behaviour bond.

Law enforcement commenced an investigation into a remittance company and its directors who were suspected of laundering illicit funds for criminal syndicates and individuals. The company also operated as a legitimate remitter sending funds primarily to individuals in Iran and Iraq.

Through its regular financial transaction reporting to AUSTRAC, the remittance company reported sending AUD6 million to Iran and Iraq on behalf of its legitimate customers. However, according to transaction data submitted by banks which dealt with the remittance business as a customer, the remitter sent AUD3.66 million to overseas beneficiaries over the same period. This resulted in a AUD2.34 million shortfall between the amount of money the remitter company claimed to have sent overseas and the amount the company actually remitted. The bank transaction data also showed that the remitter made significant cash deposits (cash deposits of AUD10,000 or more) totalling AUD3.14 million.

Along with the company director, a number of other individuals also played a key role in the company, including an associate and his son.

The company director was charged and pleaded guilty to dealing with money reasonably suspected to be the proceeds of crime contrary to section 400.9(1) of the *Criminal Code Act 1995*. He was sentenced to three months imprisonment and given an 18-month good behaviour bond. He also received a forfeiture order under section 48 of the *Proceeds of Crime Act 2002* allowing for the seizure of AUD225,000 The other two men were not charged.

Offence	Money laundering
Customer	Individual Business
Industry	Remittance services
Channel	Electronic
Report type	IFTI
Jurisdiction	International – Iran, Iraq
Designated service	Remittance services (money transfers)
Indicators	International funds transfers to high-risk jurisdiction Large cash deposits used to pay for IFTIs Third-party cash deposits

Case 20 – Suspect used casinos, remitters and airline pilots to launder proceeds of crime

A law enforcement agency conducted an investigation into a suspect believed to be part of an international money laundering scheme. AUSTRAC information revealed the syndicate's financial activities and assisted authorities to identify the suspect.

The suspect was charged with dealing with property reasonably suspected of being the proceeds of crime and received a 12-month good behaviour bond.

Authorities alleged that the suspect was part of a scheme to launder approximately AUD2.4 million from the proceeds of crime. AUSTRAC information provided an insight into the financial activities of the syndicate and assisted in identifying the suspect.

The investigation was initiated following the identification of three Chinese airline crew who attempted to depart Australia while carrying a total of more than AUD100,000 of undeclared currency.[22] Authorities identified that two of the airline crew were found to be carrying both Australian and foreign currency equivalent to more than AUD40,000 and AUD30,000 respectively. The third crew member was in possession of foreign currency equivalent to more than AUD30,000.

Following the identification of the three crew members, law enforcement authorities obtained information that prompted them to begin investigating a number of Australian-based individuals, believed to be part of the international money laundering scheme.

Suspicious casino gambling activity

Law enforcement officers began investigating the suspect after AUSTRAC received a suspicious matter report (SMR) concerning the suspect's activities. The SMRs highlighted inconsistent gaming activity at a casino by the suspect. One SMR described how the suspect had lost more than AUD3 million in one year while gambling in the casino. The suspect's losses in other years were comparatively smaller, ranging from approximately AUD3,000 to AUD30,000.

During further investigations, authorities observed the suspect take possession of a bag. Authorities intercepted the suspect and found approximately AUD200,000 cash inside the bag. Law enforcement officers seized the cash and the suspect was arrested.

Law enforcement officers subsequently established that the suspect had previously given the three airline crew large amounts of cash for them to 'courier' from Australia to China as part of the money laundering scheme.[23]

22 Under the AML/CTF Act, when a person carries currency of AUD10,000 or more (or foreign currency equivalent) into or out of Australia, a cross-border movement of physical currency (CBM-PC) report must be completed upon entry into Australia or prior to leaving Australia. It is an offence not to declare currency above the threshold of AUD10,000 (or foreign currency equivalent).

23 See the Glossary for a definition of 'cash couriers'.

Suspicious transfers to China and huge cash deposits

Authorities established that the suspect was a known associate of an individual employed by a remittance service provider. On several occasions the individual received a commission for transferring a significant amount of funds to China on behalf of the suspect. Authorities suspected that the individual used false names and altered records to the international funds transfers.

An Australian bank submitted an SMR about this individual's activities after she made two unusually large cash deposits totalling AUD600,000 on the same day to the same bank account. AUSTRAC also received two significant cash transaction reports (SCTRs) for the two large deposits. Authorities also alleged that the individual deposited a further AUD800,000 on a different day.

The suspect was charged under the *Criminal Code Act 1995* with dealing with property reasonably suspected of being proceeds of crime. The suspect received a 12-month good behaviour bond.

Offence	Money laundering Undeclared currency
Customer	Individual Business
Industry	Remittance services Banking (ADIs) Gambling services
Channel	Physical Electronic Agent/third party
Report type	SMR IFTI SCTR
Jurisdiction	International – China
Designated service	Remittance services (money transfers) Account and deposit-taking services Gambling services
Indicators	Multiple cash deposits on the same day into the same bank account Multiple high-value international funds transfers Sudden large increase in gambling activity inconsistent with customer's established gambling profile Third-party individuals making large cash deposits into accounts Use of cash couriers Use of third parties to deposit funds

AUSTRAC's work with multi-agency task forces

AUSTRAC's work with multi-agency task forces

AUSTRAC is an important member in a number of multi-agency government task forces which have been set up to combat serious national crime. AUSTRAC regularly meets with major partner agencies to ensure that its priorities are aligned and its resources are focused on addressing the nation's primary criminal threats.

Forming and maintaining effective partnerships has been a cornerstone of AUSTRAC's work for more than 20 years. Partnerships and collaboration will continue to be crucial to the agency's success at combating ML/TF as major crime threats adapt and become more dynamic.

Two examples of AUSTRAC's contribution to multi-agency task forces are Project Wickenby and Task Force Eligo.

Project Wickenby

Project Wickenby is a multi-agency task force, led by the ATO, which targets internationally promoted tax evasion schemes.

Project Wickenby uses AUSTRAC's financial intelligence to identify the flow of funds between Australia and overseas tax secrecy jurisdictions and uncover potential matters for investigation including individuals participating in a range of illegal offshore arrangements. Illegal offshore arrangements are an established way of evading tax, laundering funds and concealing beneficial ownership.

Money laundering vulnerabilities

The money laundering vulnerabilities associated with illegal offshore arrangements include:

- **The layering of funds through overseas jurisdictions.** This adds complexity to the money trail and enables criminals to distance themselves from the illegal activity that generated the funds.[24]
- **Disguising beneficial ownership and control.** The use of offshore accounts, corporate structures and transactions assists criminals to hide the true owner and/or controller of funds.
- **Illicit international funds flows can be difficult to identify when disguised as legitimate transactions.** This could be in the form of payment for false loans or payment of false invoices.

Tax evasion and money laundering typology

Project Wickenby has identified the use of false invoices and loans in illegal offshore arrangements. This typology involves the Australian entity making funds transfers into an overseas account (or a series of accounts), disguising the transfers as payments for expenses, before the funds are later returned to Australia disguised as a 'loan'. The arrangement aims to:

- create false tax deductions by claiming tax deductions for false expenses
- generate tax-free funds
- launder these funds to hide the ultimate beneficial owner.

24 See the Glossary for a definition of 'layering'.

This methodology, depicted in figures 5 and 6 below, often includes the following elements:

- An Australian company (company A) enters into an agreement with a tax scheme promoter based in a tax secrecy jurisdiction (country 1). The promoter benefits from the confidentiality and privacy offered in the tax secrecy jurisdiction.
- The tax scheme promoter owns and/or controls two offshore companies (companies B and C). Control may involve the use of a trust or the use of third parties; for example, a relative or associate may act as the director of the offshore companies.
- Company B provides consultancy and/or management services and is incorporated in country 2.
- Company C provides a financial service (as a lender of money, for example) and is incorporated in country 3.
- Companies B and C hold bank accounts in country 4. The promoter controls and operates these accounts.

Figure 5 provides an overview of the tax scheme promoter's operating structure.

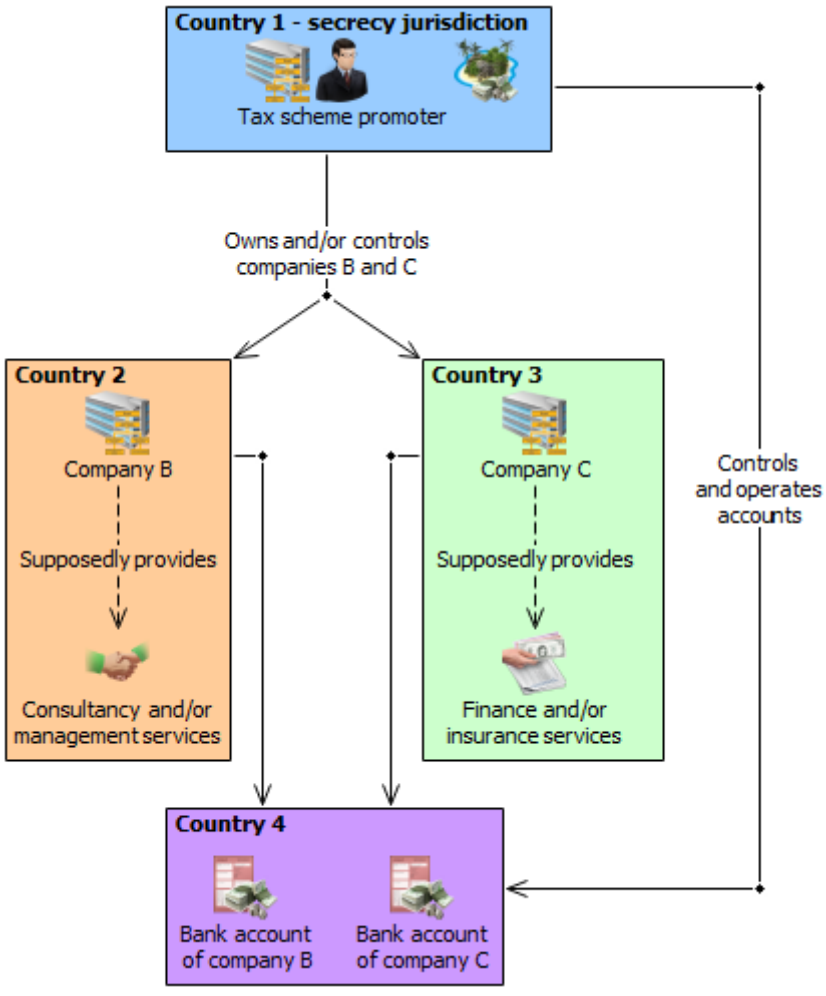


Figure 5 – Overview of tax scheme promoter's operating structure

Transfer of funds out of Australia

- Company B generates false invoices and issues them to Australia-based company A for supposed consultancy and/or management services. This gives the appearance of a legitimate commercial transaction, although no consultancy and/or management services were provided to company A.
- Australia-based company A pays the invoices by international funds transfer, transferring funds from its bank account in Australia to company B's bank account in country 4.
- Company A then claims these payments as deductible business expenses in its tax returns, thereby fraudulently reducing the company's taxable income and the amount of tax it will be assessed as liable to pay.

Layering of funds to obscure or hide ownership of funds

- The promoter electronically transfers the funds to the bank account of company C in country 4. In doing so, the funds are further layered to disguise their true origin and beneficial owners.[25]
- Alternatively, the promoter transfers the funds through a series of offshore accounts in several countries before they are transferred to company C. This further complicates the tax evasion and money laundering process in an effort to avoid detection.

Integration of funds back into Australia's financial system

- The promoter electronically transfers the funds back to the directors or controlling shareholders of company A in Australia, disguised as 'loans'
- To disguise the funds being transferred back to Australia, false documents are created purporting to be a loan agreement between company C and company A's directors or controlling shareholders.
- Disguising the funds as a 'loan' gives the appearance the funds have come from a legitimate source. At this point, the funds have essentially been integrated into the legitimate Australian financial system.[26]
- Before being returned to the beneficial owners (that is, company A's directors or controlling shareholders) the funds have passed through various companies and bank accounts. The circular nature of these transactions is a characteristic of a 'round robin' tax evasion scheme.[27]
- After the funds are returned to Australia the directors or controlling shareholders use the funds for personal and/or living expenses, or lend the funds back to company A.
- Effectively, the 'loan' facilitates the untaxed distribution of funds back to the ultimate beneficial owners, company A's directors or controlling shareholders.
- The funds, disguised as loans, are not disclosed in the personal tax returns of the directors or controlling shareholders. The directors or controlling shareholders are assessed as liable for less tax than they should have been, thereby avoiding income tax obligations.

25 See the Glossary for a definition of 'layering'.

26 See the Glossary for a definition of 'integration'.

27 See the Glossary for a definition of 'round robin tax evasion scheme'.

The 'loan' received by company A's directors or controlling shareholders originated as funds from company A which were disguised by the scheme, allowing the evasion of both company and personal tax.

Figure 6 below provides an overview of using false invoices and loans to evade tax and launder funds.

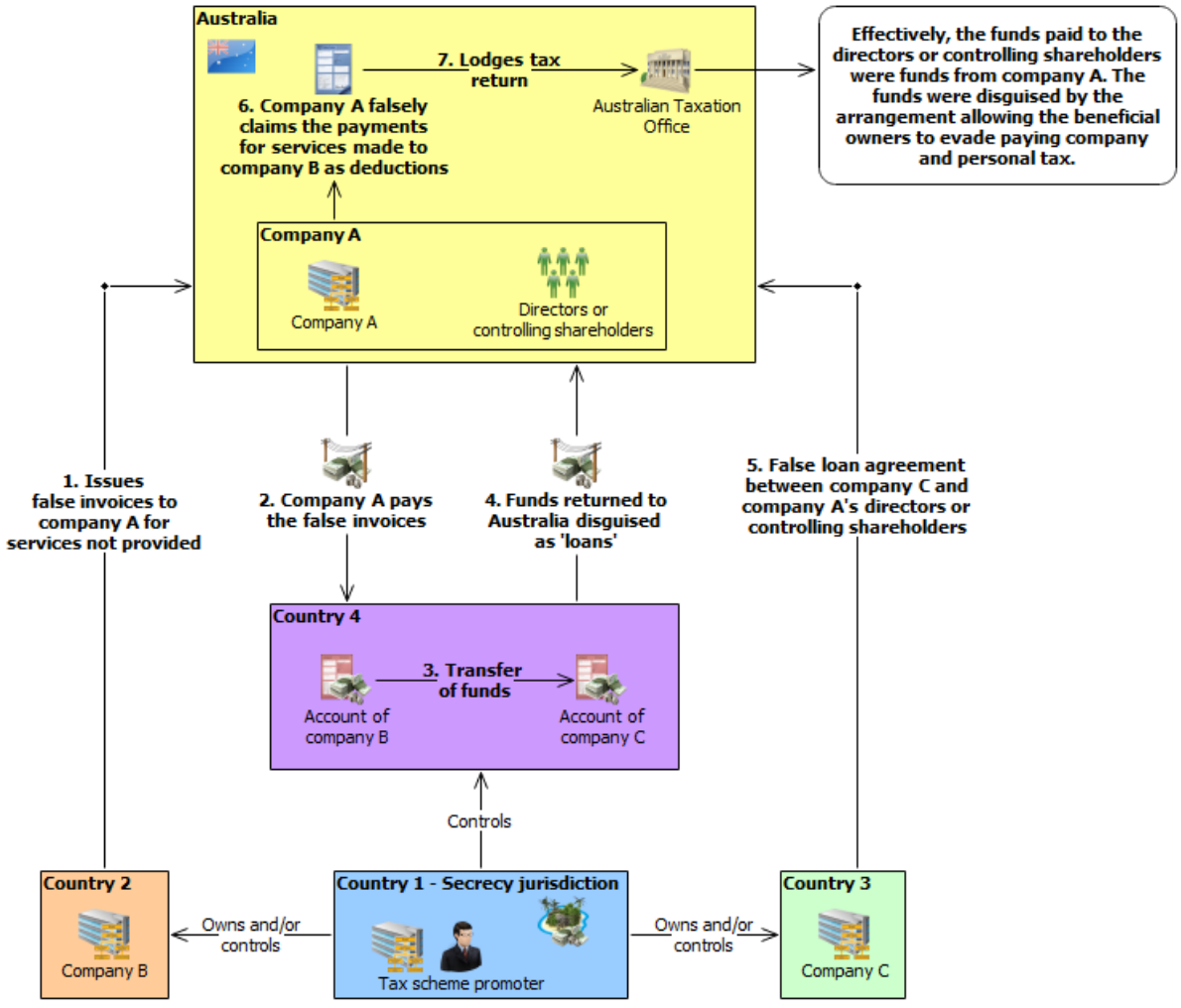


Figure 6 – Method for using false invoices and loans to evade tax and launder funds

Case studies 10 and 11 in this report demonstrate how AUSTRAC information and analysis directly contributes to Project Wickenby investigations.

Previous typologies and case studies reports also demonstrate AUSTRAC's contributions to Project Wickenby – case study 1 in AUSTRAC's 2013 typologies and case studies report is an example.

Indicators

The following indicators highlight potential suspicious customer behaviour involving false invoices and loans in an illegal offshore arrangement:

- Customer in Australia receives a loan from an offshore entity, which was preceded by the customer transferring funds out of Australia
- Customer sends multiple international funds transfers without a business rationale
- Customer sends/receives international funds transfers to and from jurisdictions known to be tax secrecy jurisdictions
- Customer sends/receives multiple high-value international funds transfers to and from Australia with no apparent logical reason
- Different ordering customers in Australia send international funds transfers to the same beneficiaries
- Use of offshore company structures and bank accounts to transfer funds seemingly to disguise the true nature and beneficial owner of funds

Task Force Eligo

The Eligo National Task Force was established in December 2012 to address money laundering vulnerabilities within the alternative remittance sector, including the potential for exploitation by serious and organised crime groups.

Task Force Eligo comprises the ACC, AUSTRAC and the AFP, in partnership with the Australian Customs and Border Protection Service and state and territory police. The task force's activities complement AUSTRAC's ongoing regulatory activities to increase AML/CTF awareness and professionalism within the remittance sector.

AUSTRAC's role and contribution to Task Force Eligo

AUSTRAC's role in Task Force Eligo is to provide financial intelligence to partner agency operations, lead engagement with industry, especially major banks and the remittance sector, and, where appropriate, use its regulatory powers to secure the compliance of high-risk remitters. AUSTRAC leads the taskforce's engagement with industry, especially in sharing information about the nature of money laundering and terrorism financing risk with the sector.

AUSTRAC's contribution to the task force since its commencement has included:

- the dissemination of 170 financial intelligence reports and profiles of entities of interest to Task Force Eligo partner agencies
- the referral of 258 SMRs to partner agencies
- the dissemination of two intelligence reports to international partners regarding entities of interest in those jurisdictions
- the dissemination of 46 data mining information reports, containing geographic analysis of remittance payments and international money flows
- 30 disseminations to partner agencies detailing the AML/CTF compliance of entities under investigation by Task Force Eligo
- posting an intelligence analyst full-time with the ACC.

Case studies 16 and 18 within this report are examples of the contribution AUSTRAC has made to Task Force Eligo and highlights the effectiveness of joint task forces and state and federal authorities working together to counter serious and organised crime.

Since its commencement, Task Force Eligo has delivered significant operational outcomes culminating in the disruption of 12 serious organised crime groups. For the period 2013–14, the task force has seized drugs with the estimated street value of AUD140 million and more than AUD21 million in cash and restrained more than AUD30 million worth of assets.[28]

28 Australian Crime Commission, *Australian Crime Commission Annual report 2013–14*, ACC, Canberra City, ACT, 2014, viewed 10 November 2014, www.crimecommission.gov.au/australian-crime-commission-annual-report-2013-14

Money laundering vulnerabilities

The money laundering vulnerabilities associated with the alternative remittance sector include:

- The **cash intensive and high volume nature** of the sector makes it vulnerable to exploitation for money laundering.
- The sector can offer **an inexpensive service for transferring funds to countries and locations which do not have modern formal banking services.** However, this can present an ML/TF vulnerability as funds may be transferred to high-risk jurisdictions or to jurisdictions with weak AML/CTF regimes.
- Smaller businesses operating in the sector may experience **difficulties complying with or understanding regulatory obligations**, particularly anti-money laundering risk programs and reporting requirements. This may be compounded where the business owner is from a non-English speaking background. This leaves some remittance businesses exposed to the risk of customer identity fraud, money laundering and other serious and organised crime.
- The **common remittance method of 'offsetting'** – also known as 'informal value transfer systems' (IVTS)[29] or 'hawala'[30]– enables the international transfer of value without transferring actual money between two remittance dealers operating in different countries. As outlined in the typology below (see 'Offsetting and money laundering typology'), criminals can exploit this practice to:
  - conceal the amount of illicit funds being transferred
  - obscure the identity of those involved in the transfer
  - avoid the legal requirement for remitters to report all separate international funds transfers to AUSTRAC.
- Independent remitters **bundling individual customer transactions** into a single bulk payment which is transferred through mainstream banking channels, often after the original deposit by the customer. This process can (inadvertently or deliberately) obscure or hide the sender and beneficiary details of each individual transaction.[31]

Offsetting and money laundering typology

Organised crime groups can exploit offsetting to conceal the amount of illicit funds being transferred and obscure the identity of those involved, including through non-reporting or incorrect reporting to AUSTRAC.

This method, shown in Figure 7 below, can be explained as follows:

- Third parties in Australia collect illicit cash on behalf of an international money launderer based in country 2. They deposit large amounts of illicit cash into bank accounts held by a remitter based in Australia. Some of the deposits are 'structured' so they fall below the AUD10,000 cash transaction reporting threshold.

29 See the Glossary for a definition of 'informal value transfer systems'

30 See the Glossary for a definition of 'hawala'

31 Australian Transaction Reports and Analysis Centre, *Money Laundering in Australia 2011*, AUSTRAC, West Chatswood, NSW 2011, viewed 20 February 2014, http://www.austrac.gov.au/publications/corporate-publications-and-reports/money-laundering-australia-2011

- Once the deposits are made, the international money launderer instructs the remitter in Australia to transfer the illicit funds into overseas accounts controlled by the international money launderer.
- Separately, a legitimate business in country 3 provides funds to another complicit remittance dealer and requests the funds be remitted to a manufacturing business in country 2. These funds are payment for goods which the business seeks to legitimately purchase from the overseas manufacturer.
- Rather than transfer the payment from the legitimate business in country 3 to the overseas manufacturer in country 2 as instructed, the complicit remitter pays the manufacturer using the illicit funds which have been transferred from Australia to an account located in country 2. The manufacturer is unaware of the illicit origin of the funds, and accepts as legitimate the payment sent by the business in country 3.
- The funds given to the complicit remitter in country 3 by the legitimate business (and intended to be used to pay to the manufacturer) are instead given to the organised crime group, located in country 3. As a result, the illicit profits from the criminal activity in Australia are transferred to country 3, without leaving a money trail that connects the illicit cash in Australia to the payment received by the crime group.

Figure 7 below provides an overview of how the money trail can be concealed through offsetting.

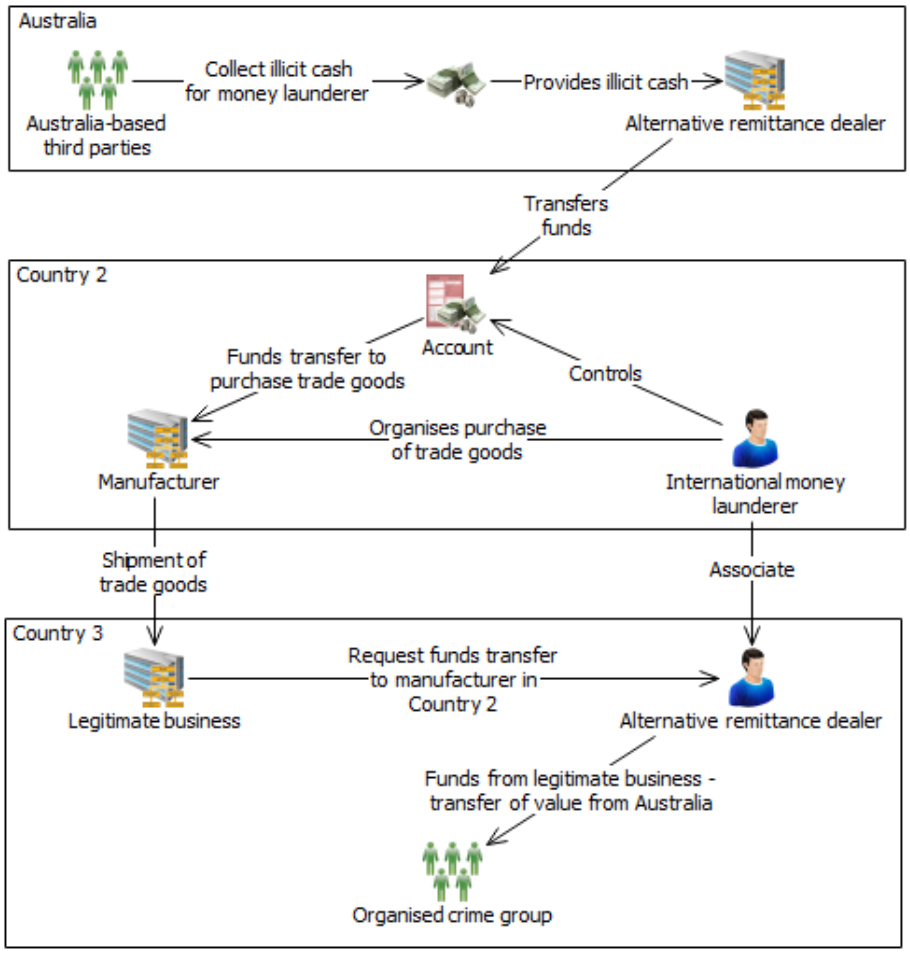


Figure 7 – Overview of concealing the money trail through offsetting

Indicators

The following indicators highlight potentially suspicious customer behaviour involving the alternative remittance sector.

- Business account activity inconsistent with customer profile
- Cash deposits made by third-party into remitter's accounts
- Customer structuring cash deposits and withdrawals over a period of time to avoid transaction threshold reporting requirements
- Financial activity does not match established customer profile
- High-value transactions inconsistent with customer profile
- International funds transfers to high-risk jurisdictions
- Large amounts of cash used to pay for international funds transfers
- Large cash deposits made at different bank branches on the same day
- Large international funds transfers to common beneficiaries
- Multiple customers conducting international funds transfers to the same overseas beneficiary
- Multiple international funds transfers to different beneficiaries sharing the same overseas address
- Multiple international funds transfers undertaken through different remitters on the same day
- Use of false identification to conduct transactions

Money laundering typology

Money laundering typology – Third-party cash couriers misusing remitter accounts

The typology outlined below is intended to inform stakeholders about one technique which criminals have used to launder the proceeds of their illicit activity.

Law enforcement investigations identified a number of instances where individuals (known as 'third-party cash couriers') were depositing large amounts of illicit cash into the bank accounts of remittance businesses registered with AUSTRAC.[32, 33] In an attempt to make the deposits appear legitimate, the third-party cash couriers are instructed to claim they are employees of the registered remitter. This cover story is used to explain to the bank the (legitimate) source of the cash.[34]

Investigations revealed that another individual (the recruiter), who may be a member of an organised crime group, is responsible for coordinating the various cash couriers depositing cash into the remitters' accounts.

Money laundering typology

As shown in Figure 8 on the following page, the use of third-party cash couriers to deposit illicit cash into the bank accounts of remitters may involve the following:

- A job advertisement is placed online or in a local paper for a role as an 'office assistant'.
- The cash courier responds to the advertisement and is offered the job of depositing cash into the accounts of remitters. When recruited, the cash courier may not be aware of the true (illicit) source of the funds.
- The cash courier meets the recruiter at the recruiter's office and the two visit various banks.
- The recruiter carries the cash until they reach the bank and then hands the cash over to the cash courier to deposit. The cash is generally carried in a shopping bag to avoid suspicion.
- The recruiter instructs the cash courier to deposit the cash into specific banks and branches and provides them with completed deposit slips to use for each transaction. The cash is usually deposited in amounts of less than AUD10,000 in order to avoid suspicion.
- If questioned, the cash courier is instructed to advise bank staff that they are an employee of the remitter.
- Deposits are made at different banks and branches across central business district (CBD) locations.
- The cash courier may also be instructed to use the services of different banks in various suburbs outside the CBD in an attempt to reduce the chances of detection.
- Once the cash is deposited, the recruiter will contact the remitter and provide details of where to send the funds overseas. The remitter instructs the bank to send the funds via an IFTI to a beneficiary overseas.

32 See the Glossary for a definition of 'cash couriers'.

33 See the AUSTRAC website for more information on remitter registration<http://www.austrac.gov.au/acg-chapter-5-registration.html>

34 Dealing in the proceeds of crime is an offence under sections 400.3 to s400.9 of the *Criminal Code Act 1995*.

» In some cases, the remitter is unwittingly involved and unaware that their bank accounts and services are being used by criminal groups to transfer illicit cash.

» The recruiter may also ask the cash courier to open accounts using the cash courier's own identification (for example, a drivers licence) and give the recruiter the authority to operate the account. The account is established to receive cash deposits from the recruiter. The recruiter may then transfer the funds in the account to the remitter's account, to be subsequently transferred offshore.

» The cash courier is paid one per cent of the total cash they have deposited after the deposit is made.

Figure 8 outlines the money laundering method described above.

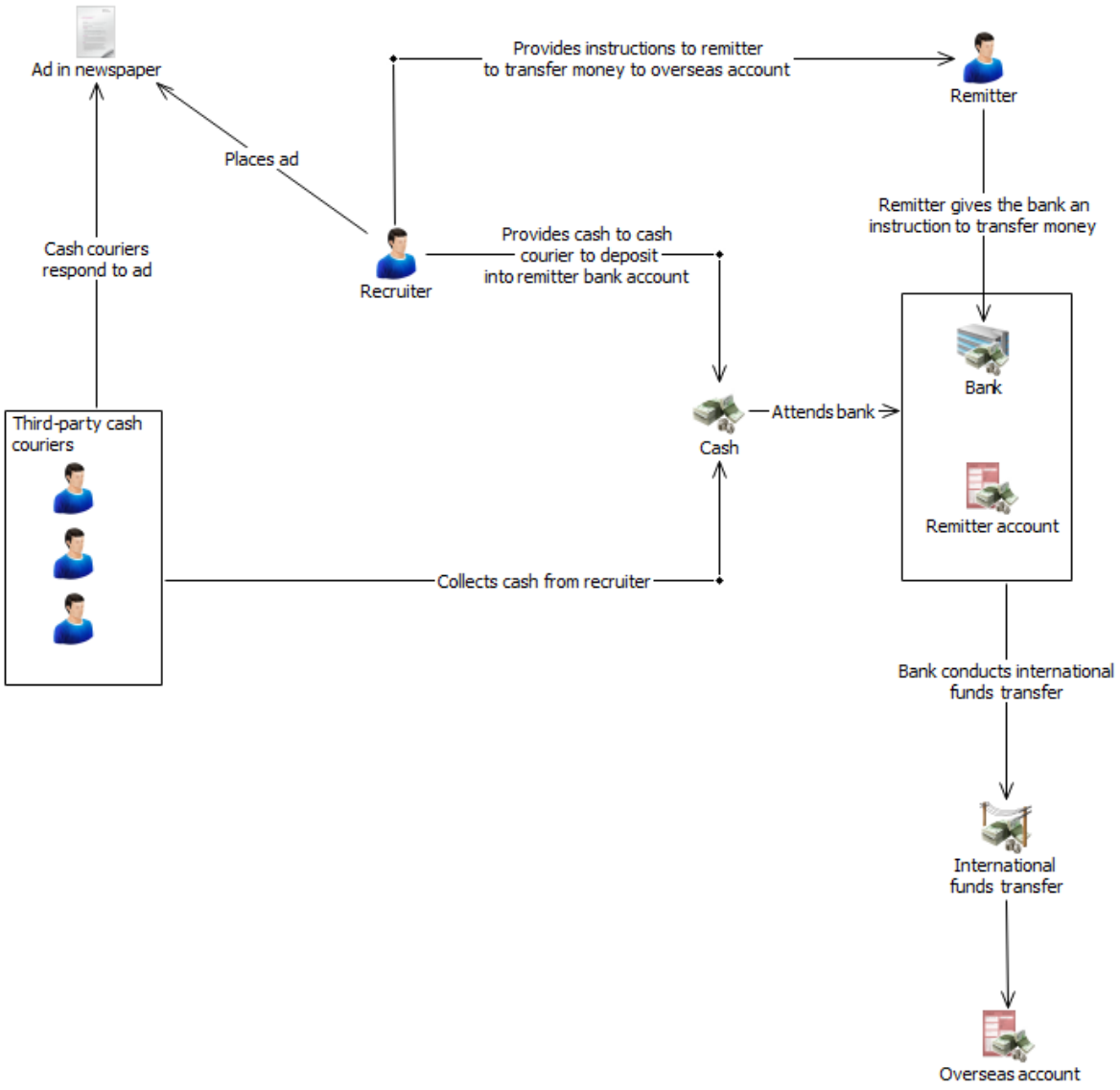


Figure 8 – Overview of third-party cash couriers depositing cash into remitter accounts

Indicators

The following indicators may assist reporting entities to identify potential money laundering activity involving third-party cash couriers depositing cash into remitter accounts.

- Cash deposits conducted by a third party where the reporting entity has doubts about the validity of the identification document used by the third party
- Depositor unable to produce evidence of employment or address/contact numbers
- Depositor claims to be an employee of more than one remitter
- Depositor unable to specify where they collected the cash as it is given to them by someone else
- Individuals make regular trips to bank branches to deposit large amounts of cash into remitter accounts
- Large cash deposits being made into multiple bank accounts belonging to remitters
- Same-day international funds transfers occurring through multiple remitters to the same overseas beneficiary
- Sudden increase in cash deposits into remitter bank accounts
- The same individual making large cash deposits at several bank branches or different banks across CBD locations
- Use of third parties to make large cash deposits

Law enforcement has previously detected a variation of this method whereby third parties are recruited from overseas. The recruited couriers are used to smuggle significant amounts of illicit cash into Australia or, once in Australia, used to deposit illicit cash into accounts for subsequent transfer overseas. This method is outlined in more detail in the *AUSTRAC typologies and case studies report 2012*. [35]

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

35 *AUSTRAC typologies and case studies report 2012*, p. 13, http://www.austrac.gov.au/typologies-and-case-studies-report-2012

Appendixes
Case study index
Glossary and abbreviations

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

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

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

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

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

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

- Cash provided by customer has a distinct or unusual odour
- Customer and relative/associate attend the same branch and make structured cash deposits into accounts at the same time
- Customer becomes irate when questioned over financial transactions
- Customer is both the ordering and beneficiary customer for multiple outgoing international funds transfers
- Customer receives international funds transfers described as 'loan'
- Customer receiving/undertaking high-volume and high-value international funds transfers for no apparent logical reason

- Customer undertaking complicated transfers without a business rationale
- Customer undertaking transactions that appear to be inconsistent with their profile and/or transaction history
- Customer unwilling to produce identification when requested by reporting entity staff
- Frequent cash deposits occurring at different branches on the same day
- International funds transfer to high-risk jurisdictions
- Multiple customers conducting international funds transfers to the same overseas beneficiary
- Multiple international funds transfers paid for with cash, in amounts just below the AUD10,000 reporting threshold
- Outgoing funds transfers sent to offshore entities, followed soon after by incoming funds transfers of similar amounts, from the same offshore entities
- Regular or multiple cash deposits structured to fall below the AUD10,000 cash transaction reporting threshold
- Significant chip cash-outs despite minimal customer play at a casino
- Structuring of gaming chip cash outs to avoid cash transaction reporting obligations
- Sudden large increase in gambling activity inconsistent with customer's established gambling profile
- Third-parties undertaking transfers to and from accounts for no apparent logical reason
- Unusual transaction activity through business accounts, suggesting the account is being used for unregistered remittance activity
- Use of charitable organisation despite a lack of business rationale

Appendix B – References and further reading

» AUSTRAC, *AUSTRAC Typologies and case studies report 2012*, www.austrac.gov.au/typologies-and-case-studies-report-2012

» AUSTRAC, *Money Laundering in Australia 2011*, www.austrac.gov.au/publications/corporate-publications-and-reports/money-laundering-australia-2011

» AUSTRAC, *AUSTRAC compliance guide*, www.austrac.gov.au/businesses/obligations-and-compliance/austrac-compliance-guide

» Australian Crime Commission, *Australian Crime Commission Annual Report 2013–14*, www.crimecommission.gov.au/publications/annual-reports/australian-crime-commission-annual-reports/australian-crime-commissio-10

» Australian Taxation Office, *Tax avoidance schemes*, www.ato.gov.au/General/Tax-planning/Tax-avoidance-schemes/

» Investopedia, *Protect yourself from HELOC fraud*, www.investopedia.com/articles/mortgages-real-estate/09/heloc-fraud.asp

Appendix C – Report types

AUSTRAC receives financial transaction reports and reports of suspicious matters from entities that provide designated services under the AML/CTF Act. The agency also receives a small number of reports from 'cash dealers' regulated under the FTR Act.

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

The types of reports AUSTRAC receives under the AML/CTF Act are:

Financial transaction reports

International funds transfer instruction (IFTI) reports

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

In 2013–14 AUSTRAC received almost 85 million reports of IFTIs from industry.

Suspicious matter reports (SMRs)

Under the AML/CTF Act, a reporting entity must submit an SMR if, at any time while dealing with a customer, the entity forms a reasonable suspicion that the matter may be related to an offence, tax evasion, or the proceeds of crime.

Entities must submit SMRs to AUSTRAC within three days of forming the suspicion (or within 24 hours for matters related to the suspected financing of terrorism). The equivalent report type for entities regulated under the FTR Act is the suspect transaction report (SUSTR).

In 2013–14 AUSTRAC received more than 64,000 reports of suspicious matters from industry.

Threshold transaction reports (TTRs)

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

In 2013–14 AUSTRAC received more than 5 million reports of cash transactions worth AUD10,000 or more from industry.

Cross-border movement reports

Cross-border movement of physical currency (CBM-PC) reports

Under the AML/CTF Act, CBM-PC reports are submitted when physical currency of AUD10,000 or more (or the foreign equivalent) is carried, mailed or shipped into or out of Australia.

When a person carries the currency, a CBM-PC report must be completed at the first Customs and Border Protection examination area upon entry into Australia or before leaving Australia.

When a person mails or ships the currency into or out of Australia, a CBM-PC report must be submitted within five business days of the currency being received in Australia, or at any time before the currency is sent out of Australia.

In 2013–14 AUSTRAC received almost 40,000 CBM-PC reports.

Cross-border movement of bearer negotiable instrument (CBM-BNI) reports

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

In 2013–14 AUSTRAC received more than 600 CBM-BNI reports, which were forwarded by its partner agencies.

Appendix D – Information sources

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

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

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

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

- Australian Crime Commission
- Australian Customs and Border Protection Service
- Australian Federal Police
- Australian Taxation Office
- Department of Human Services
- New South Wales Police
- Victoria Police
- Western Australian Police.

The contributions of these agencies complement the research undertaken by AUSTRAC into money laundering and terrorism financing risks and methodologies.

Case study index

Subject	Case study no.
accountant	6, 10, 11
automatic teller machine (ATM)	5
cash couriers	7, 20
cash deposit	1–9, 12, 14, 16, 18–20
cash withdrawal	1–5, 7–9, 12, 14, 16, 18
casino	2, 5, 13, 14, 16, 20
charity	11
cheques	5, 6, 10, 16
company/business accounts	5–7, 10, 11, 16, 19
couriers, see *cash couriers* and *drug mules/couriers*	
credit card	13, 18
credit union	14
digital currency	1
director (company director)	10, 19
drug mules/couriers	14
drugs/narcotics	1, 2, 6, 8, 9, 12, 14, 16, 18
false/fraudulent identification	2–5, 12, 13, 18, 20
family members/relatives	4, 10, 11, 14
firearms/weapons	1, 9, 15
foreign nationals	3, 4, 5, 8, 13, 16, 18, 20
fraud (see also *scams*)	4, 5, 10, 13, 17
gambling	2, 5, 9, 13, 14, 16, 20
high-risk jurisdiction	4, 5, 9, 11, 12, 16–19

Subject	Case study no.
international funds transfers (inc. IFTIs)	1, 3–13, 15–20
internet/online banking	4, 15
loan services	10, 11, 13
money laundering	2, 5–7, 13, 14, 16, 19, 20
motor vehicles	5, 14
organised crime/syndicates	3, 5, 7–9, 12, 13, 16–20
overseas bank accounts	4, 6, 7, 11
people smuggling	4, 8
people trafficking	3
proceeds of crime	2, 4, 7, 10, 14, 16, 19, 20
real estate/property	5, 10, 13, 14
remittance services (money transfers) (designated service)	4, 6–9, 12, 15–20
scams (e.g. 'advance fee fraud')	17
SCTRs (significant cash transaction reports)	3, 4, 7, 13, 14, 20
structuring (of transactions)	2–7, 9, 12, 14, 18
SMRs (suspicious matter reports)	1, 2, 4–7, 9, 12–14, 16–18, 20
taxation (evasion, avoidance)	10, 11
third parties	4–8, 11, 13, 14, 16, 19, 20
TTRs (threshold transaction reports)	1, 8, 9, 16
underground banking/'hawala'/informal money remittance	16
unexplained income/wealth	4–8, 14, 16, 18, 20
welfare fraud	14

Glossary and abbreviations

Glossary

Term	Description
advance fee fraud	A scam, also commonly referred to as 'the Nigerian scam', in which victims are approached, usually by email, and deceived into forwarding 'advance fee' payments, or divulging financial information such as bank account details. These scams attract their victims with promises of overseas lottery wins, unexpected inheritances or government windfalls.
beneficiary (or beneficiary customer)	The person (or organisation) who is the ultimate recipient of funds being transferred.
chip cash-out	The process of converting casino gaming chips into cash.
cash couriers/ third-parties	People who physically transport cash on their person or as part of their luggage between international jurisdictions. Couriers may be directly connected to criminal activity and the proceeds of crime, or they may be third parties (or 'mules') recruited specifically for the task of moving the money offshore. To avoid direct involvement in the money laundering process, criminals may use third parties to undertake certain high-risk transactions that might expose the criminals to law enforcement or regulatory bodies.
channel	The means by which the individuals undertook or attempted to undertake transactions (predominantly these are transactions conducted in person, via electronic means or through an intermediary or third party).
customer	The type of customer/s involved in the offence (this can be an individual, business or foreign entity).
designated service	The category of 'designated service' (as listed in section 6 of the AML/CTF Act), or other financial product, used in the offence. The case studies within this report have been grouped according to the primary designated services used (for example, account and deposit-taking services or remittance services).

Term	Description
hawala	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 minimal documentation. In Australia, it is an offence for a person to provide a registrable designated remittance service unless registered with AUSTRAC on the Remittance Sector Register in accordance with the AML/CTF Act.
high-risk jurisdictions	These include: » jurisdictions known to be a source or conduit of narcotics or other significant criminal activity » any jurisdiction subject to Australian Government sanctions » jurisdictions known to be a secrecy haven or preferential tax regime » jurisdictions linked to proscribed terrorist organisations.
home equity line-of-credit fraud	A fraud type in which an applicant or interested party makes misstatements, misrepresentations or omissions to a financial institution to commit fraud. Organised crime groups use public records to identify and collect personal information about potential victims. The group uses this personal information to contact the victim's financial institution to gain access to the victim's funds. The funds are then transferred into accounts held by the crime groups.[36]
indicators	Also known as 'red flags', these are customer behaviours or activities that indicate possible money laundering or terrorism financing activity.
industry	The industry involved in the financial transactions (some case studies involve multiple industries).
integration	The final stage in the money laundering cycle. See the entry for 'money laundering cycle' in this glossary.
jurisdiction	The location (Australian or international) where the transactions originated or were undertaken.

36 Investopedia, *Protect yourself from HELOC fraud*, viewed 1 September 2014, www.investopedia.com/articles/mortgages-real-estate/09/heloc-fraud.asp

Term	Description
layering	The second stage in the money laundering cycle. See the entry for 'money laundering cycle' in this glossary.
informal value transfer system (IVTS)	Global networks for undertaking financial transactions which transfer the value of currency without necessarily physically relocating that currency. IVTS use informal funds transfers that take place outside of the conventional banking system through non-bank financial institutions or other business entities. IVTS operations are mostly used for legitimate funds transfers and are found in most countries. IVTS are known by various names across different regions, including 'hawala' (the Middle East, Afghanistan, Indian subcontinent), 'hundi' (India) and 'fei ch'ien' (China).
money laundering cycle	The money laundering cycle describes the typical three-stage process criminals may use to conceal the source of illicit funds and make funds appear legitimate: » Placement – Introducing illegal funds into the formal financial system (for example, making 'structured' cash deposits into bank accounts). » Layering – Moving, dispersing or disguising illegal funds or assets to conceal their true origin (for example, using a series of complex transactions involving multiple banks and accounts, or corporations and trusts). » Integration – Investing these now distanced funds or assets in further criminal activity or legitimate business, or purchasing high-value assets and luxury goods. At this stage the funds or assets appear to have been legitimately acquired.
money laundering syndicate	A criminal group, based in Australia or overseas, that provides specific money laundering services to domestic and international crime groups operating in Australia. Also called specialist money laundering syndicates because money laundering is the primary or only illicit activity they undertake. They differ from other crime groups that undertake money laundering as a secondary enabling activity for their primary criminal activity (such as drug trafficking).
offence	The criminal or civil offence involved in a case (these do not necessarily represent actual charges brought against the perpetrators).
proceeds of crime	Money or other property that has been derived, directly or indirectly, through the commission of an offence against a law of the Commonwealth, a state, a territory or a foreign country.

Term	Description
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. Remitters transfer value using a communication, message or transfer, or through a clearing network to which the money/value transfer system belongs.
report type	The types of financial transaction reports or reports of suspicious matters submitted by regulated entities, either under the FTR Act or AML/CTF Act, which contributed to the investigation or operation detailed in each case study
round robin tax evasion scheme	A scheme where money is transferred to an overseas account and then transferred back to personal accounts in the country of origin, usually disguised as a tax-free loan.
structuring	A money laundering technique which involves the deliberate division of a large amount of cash into a number of smaller deposits to evade threshold reporting requirements. Under section 142 of the AML/ CTF Act structuring is punishable by up to five years imprisonment and/or 300 penalty units. Structuring can also involve the layering of payments for international funds transfers to prevent the transfers attracting scrutiny from authorities.
tax avoidance	Where taxpayers minimise their tax liability by deliberately using arrangements that provide them with tax benefits that are outside the intent of the law.
tax evasion	Where taxpayers deliberately break the law and dishonestly abuse the tax system to obtain a financial benefit.
tax secrecy jurisdiction or haven	A country, region or state that does not divulge information about an individual's financial/banking affairs or structures. These jurisdictions may be exploited to conceal income and evade tax in Australia because they do not have effective information exchange arrangements with Australia.

Abbreviations

- ACC – Australian Crime Commission
- ADI – authorised deposit-taking institution
- AFP – Australian Federal Police
- AML/CTF – anti-money laundering and counter-terrorism financing
- AML/CTF Act – *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*
- ATM – automatic teller machine
- ATO – Australian Taxation Office
- AUD – Australian dollars
- AUSTRAC – Australian Transaction Reports and Analysis Centre
- CBD – central business district
- CBM-PC – Cross-border movement – physical cash
- CBM-BNI – Cross-border movement – bearer negotiable instrument
- GBP – Great Britain Pounds
- FIU – financial intelligence unit
- FTR Act – *Financial Transaction Reports Act 1988*
- ICTR – international currency transfer report
- IFTI – international funds transfer instruction
- IVTS – informal value transfer system
- MDMA – methylenedioxymethamphetamine
- ML/TF – money laundering and terrorism financing
- NSW – New South Wales
- SCTR – significant cash transaction report
- SMR – suspicious matter report
- TTR – threshold transaction report
- UAE – United Arab Emirates
- USD – United States dollars

How can I contact AUSTRAC?

You can contact the AUSTRAC Contact Centre 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