Australian Government

Australian Transaction Reports and Analysis Centre

Parliamentary Joint Committee on Law Enforcement

Inquiry into Financial Related Crime

Australian Transaction Reports and Analysis Centre

Submission

May 2014

Contents

Executive summary

Every year, serious and organised crime costs Australia an estimated $10–$15 billion. To use the proceeds of their crimes, criminals need to ‘clean’ or ‘launder’ this money—making it appear to have come from legitimate sources (*Money laundering in Australia 2011*. AUSTRAC).

Money laundering threatens Australia’s prosperity, undermines the integrity of our financial system and funds further criminal activity that impacts on community safety and wellbeing. For these reasons, strategic intelligence assessments recognise money laundering as a critical risk to Australia.

Tackling this critical risk requires a collaborative response globally and nationally. Law enforcement and intelligence agencies work alongside other government authorities and industry to identify, disrupt and prevent money laundering.

As an anti-money laundering and counter-terrorism financing (AML/CTF) regulator, AUSTRAC monitors the compliance of its regulated population with the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) and takes enforcement action where necessary in relation to breaches of the Act. In its capacity as financial intelligence unit (FIU), AUSTRAC analyses financial information and works with partner agencies and industry sectors to identify patterns of suspicious activity and contribute to law enforcement operations.

The AUSTRAC database currently holds more than 350 million reports and receives on average 280,000 new reports each day.

AUSTRAC analyses reports with other information and disseminates the resulting financial intelligence to 41 domestic revenue, law enforcement, national security, human services, regulatory and other Commonwealth, state and territory partner agencies in Australia (referred to in the AML/CTF Act as 'designated agencies'). In addition, AUSTRAC has agreements in place with 69 international counterparts for the exchange of financial intelligence information, and one agreement with an international counterpart for the exchange of regulatory information.

AUSTRAC provides ongoing support to financial crime investigations through engagement with law enforcement agencies at the operational level, as well as operational support to financial crime investigations undertaken by the Australian Crime Commission (ACC), Australian Federal Police (AFP), the NSW Crime Commission and other law enforcement agencies.

These agencies use the financial intelligence to detect money laundering and terrorism financing (ML/TF) activity, investigate financial crimes including tax evasion, and secure prosecutions. This supports national priorities to protect national security, apprehend criminals, protect the integrity of Australia’s financial markets and maximise revenue collection. AUSTRAC also makes a vital contribution through major national operations and task forces, including those focusing on money laundering, criminal assets, tax evasion and border security including people smuggling.

The AML/CTF Act, with its combination of rule-making, exemption and modification powers provides an effective and efficient set of regulatory tools which enable the AUSTRAC Chief Executive Officer (CEO) to provide regulatory relief to low-risk reporting entities (including small business) while maintaining the integrity of the AML/CTF Act.

The AML/CTF Act is principles-based legislation that promotes a risk-based approach to AML/CTF compliance. As required by the Financial Action Task Force (FATF), the AML/CTF Act sets out the principal obligations for reporting entities, which are required to develop risk-based systems and controls tailored to the nature, size and complexity of their business and proportionate to the level of ML/TF risk they face.

AUSTRAC contributes to law enforcement strategies and counter-terrorism financing and other national security matters. Key points to note are that AUSTRAC:

- contributes to whole-of-government task forces and investigations as required
- provides support through its financial intelligence products, monitoring data for high-risk activities, and outposted intelligence officers
- plays a significant role in supporting the criminal investigations of other agencies – AUSTRAC does not prosecute offences under the AML/CTF Act but has the power to take civil penalty action for regulatory breaches.

The effectiveness of Australia's AML/CTF regime is measured by its success and providing benefits to the community in numerous ways, including preventing, detecting and disrupting crime. AUSTRAC's financial intelligence contributes to multi-agency investigations that target money laundering and tax evasion criminal networks, in addition to a range of predicate crimes such as drug trafficking, fraud, identity crime, people smuggling and national security matters.

AUSTRAC's partner agencies include not only Commonwealth law enforcement agencies, but also state and territory police forces, crime commissions and anti-corruption bodies. AUSTRAC plays a key role in the initiation of law enforcement investigations into financial crime.

AUSTRAC shares AML/CTF compliance-related information, financial transaction information and intelligence with international counterparts. This information strengthens the global effort to combat ML/TF and benefits the operational work of FIUs and law enforcement agencies tracking the international movement of the proceeds of crime. In return, AUSTRAC receives valuable financial intelligence from its international partners to assist in its own detection and analysis of illicit transactions.

1. The character, prevalence and impact of financial related crime in Australia

AUSTRAC is Australia's AML/CTF regulator and specialist FIU. Its 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.

The publicly available *Organised Crime in Australia* report is produced every two years by the ACC and is informed by the Organised Crime Threat Assessment. As a comprehensive profile of organised crime in Australia, it provides industry and the public with information to better understand and respond to current and emerging organised crime threats.

Organised crime exploits numerous sectors and avenues for money laundering. The crime of money laundering involves diverse and often sophisticated methodologies. It corrupts and intermingles illicitly gained funds with legitimate transactions in areas such as banking and finance, casinos and gambling, high-value assets like real estate and luxury vehicles, international trade, and international remittance and foreign exchange services. Less visible channels or enablers include professional advisers, legal entity structures, cash-intensive businesses, electronic payment systems, cross-border movement of cash and bearer negotiable instruments, and investment vehicles.

Tackling this critical risk requires a collaborative response globally and nationally. Law enforcement and intelligence agencies work alongside other government authorities and industry to identify, disrupt and prevent money laundering.

ML/TF activities have the potential to undermine the soundness and stability of financial institutions and systems, discourage foreign investment and distort international capital flows. Australia's AML/CTF regime enhances our economic stability. Businesses that comply with the AML/CTF regime reduce their risk of being exploited by organised crime for money laundering purposes. Businesses benefit when regulatory actions detect and disrupt undermining criminal activities such as embezzlement of funds, loan fraud and international scams. Maintaining a strong AML/CTF regime also enhances the reputation of Australian businesses, particularly financial institutions, in the eyes of overseas investors and international markets.

Money laundering is defined broadly in Division 400 of the *Criminal Code Act 1995* (Criminal Code) to include more than just concealing the proceeds or instruments of crime. The Criminal Code makes it an offence to 'deal with' the proceeds of crime or an instrument of crime. 'Deal with' is defined as a person receiving, possessing, concealing or disposing of money or other property as well as importing, exporting or engaging in a banking transaction relating to money or other property.

Australia has intentionally adopted a risk-based approach to its AML/CTF framework and regulation. This recognises that industry sectors are best placed to identify and manage the money laundering risks they face. It also recognises that the level and nature of money laundering risks vary from sector to sector, as well as within each sector.

Australia's anti-money laundering and counter-terrorism financing framework

The AML/CTF Act and the *Financial Transaction Reports Act 1988* (FTR Act) provide the foundation for Australia's regulatory regime to detect and deter ML/TF.

The AML/CTF Act was introduced in 2006 to strengthen Australia's capacity to deter, detect and combat serious and organised crime and ML/TF. It also brought Australia's AML/CTF regime into line with the FATF Recommendations at that time. The policy goals of the AML/CTF regime are to implement a regulatory framework that:

- minimises the risk of ML/TF in the Australian economy
- supports domestic and international efforts to combat serious and organised crime and terrorism
- does not impose unnecessary burden on Australian business
- is consistent with international best practice in combatting ML/TF.

Introduction of the AML/CTF Act significantly expanded the operation and regulatory coverage of Australia's regime. From fewer than 4,000 'cash dealers' under the FTR Act, the regime now has a regulated population of over 13,900 individuals and businesses ('reporting entities') in the financial, remittance, gambling and bullion sectors. AUSTRAC was given stronger compliance and enforcement powers to use in supervising this larger regulated population.

Following the introduction of the AML/CTF Act, transaction reporting increased, as did the number of government agencies that could access and use this information. Transaction reporting from industry to AUSTRAC grew from 18 million reports in 2007-08 to over 84 million reports in 2012-13 – a 466 per cent rise.

Transaction reports collected

AUSTRAC receives the following types of reports of financial transactions and suspicious matters.

- International funds transfer instruction (IFTI) reports – if a reporting entity sends or receives an instruction to or from a foreign country, to transfer money or property, the reporting entity must submit an IFTI report to AUSTRAC.
- Suspicious matter reports (SMRs) – a reporting entity must submit an SMR if at any time while dealing with a customer, the reporting entity forms a reasonable suspicion that the matter may be related to an offence, tax evasion, or the proceeds of crime.
- Threshold transaction reports (TTRs) – if a reporting entity provides a designated service to a customer, involving the transfer of physical currency (or e-currency) of AUD10,000 or more (or the foreign currency equivalent), then the reporting entity must submit a TTR to AUSTRAC.

Reports are received from a wide range of regulated entities in the financial, remittance, bullion and gambling sectors. The majority of reports are submitted under the AML/CTF Act.

Under the AML/CTF Act, AUSTRAC also receives reports of cross-border movements of physical currency and bearer negotiable instruments, mostly from travellers entering or leaving Australia. AUSTRAC receives a small number of transaction reports from 'cash dealers' and solicitors under the FTR Act.

AUSTRAC received 84,634,614 transaction reports in the 2012-13 year. This increased from 59,244,235 in the previous year and consisted of:

- 79,334,421 IFTI reports (53,770,266 in 2011-12)
- 5,224,751 TTRs
- 44,062 SMRs
- 30,725 cross-border movements of physical currency
- 655 cross-border movements of bearer negotiable instruments.

The AUSTRAC database currently holds more than 350 million reports and receives on average 280,000 new reports each day.

AUSTRAC's partner agencies use the financial intelligence to detect ML/TF activity, investigate financial crimes including tax evasion, and secure prosecutions. This supports national priorities to protect national security, apprehend criminals, protect the integrity of Australia's financial markets and maximise revenue collection. AUSTRAC also makes a vital contribution through major national operations and task forces, including those focusing on money laundering, criminal assets, tax evasion and border security including people smuggling.

AUSTRAC information is key to identifying suspected tax avoidance involving the abuse of overseas tax and secrecy havens. The Australian Taxation Office (ATO) is the largest user of AUSTRAC information. Analysis of AUSTRAC information has had a direct impact on annual tax assessments raised. In the 2012-13 financial year, the ATO reported an additional $572 million in tax assessments raised as a result of using AUSTRAC information.

The strong regulatory controls in place for mainstream financial institutions in Australia, particularly banks, may displace criminal activity towards products and services considered to attract less regulatory attention. AUSTRAC analyses the reports it receives from regulated entities to uncover patterns of criminal activity.

AUSTRAC produces annual typologies and case studies reports <www.austrac.gov.au/typologies.html> to assist reporting entities to fulfil their AML/CTF obligations and help industry and government partners detect ML/TF threats. Each report contains numerous case studies detailing the various methods criminals use to conceal, launder or move illicit funds, both in Australia and overseas. A range of indicators are included to assist businesses identify potential ML/TF among the financial activity of their customers. The typologies reports highlight the importance of the combined role that Australian Government agencies and business play in disrupting criminal activity in the international financial environment.

In 2011, AUSTRAC produced Australia's first National Threat Assessment (NTA 2011) on money laundering. It provides a consolidated picture of the key systemic money laundering threats facing Australia. Since its completion, the NTA 2011 has:

- been disseminated to many of AUSTRAC's domestic partner agencies, as well as foreign counterparts in Canada, New Zealand, United Kingdom, United States of America and others

- strengthened AUSTRAC's specialist FIU reputation within domestic and international circles by influencing FATF guidance on national risk assessments

- informed strategic priorities under the Commonwealth Organised Crime Strategic Framework

- provided the strategic basis for the establishment of a national task force on high-risk remitters (Taskforce Eligo) and an interagency working group on trade-based money laundering.

To complement the NTA 2011, AUSTRAC led the recently completed first national risk assessment on terrorism financing (NRA TF). The assessment provides a consolidated picture of the terrorism financing environment based on operational intelligence and expertise on terrorism financing activity, as detected or suspected within Australia and in relation to high-risk countries that affect the Australian environment. By building a stronger intelligence picture of terrorism financing threats in Australia and involving foreign countries, the NRA TF will enhance Australia's counter-terrorism effort and contribute to our international obligations to identify, assess and understand terrorism financing risks and vulnerabilities. The NRA TF will also contribute to any future consideration of national security legislative reform. The NRA TF was completed in April 2014.

2. The methods and practices used by the perpetrators of financial related crime (including the impact of new technologies)

Criminals use diverse methods to deal with money or other property that is the proceeds of crime. As with other criminal activity, these methods evolve to sidestep regulatory and law enforcement measures and to exploit market and technology developments, including harnessing new products or technologies such as e-commerce and m-commerce (buying and selling through mobile wireless devices).

Money laundering can involve:

- moving money or other property across borders (for example, international funds transfers, remittances, bulk cash smuggling and cross-border movement of bullion and jewellery)

- concealing money or other property domestically (for example, purchasing high-value goods and real estate, gambling and putting money into legitimate businesses).

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 transactions into bank accounts).

- **Layering –** moving, dispersing or disguising illegal funds or assets to conceal their true origin (for example, using a maze of complex transactions involving multiple banks and accounts, or corporations and trusts).

- **Integration –**investing these now distanced funds or assets in further criminal activity or legitimate business, or purchasing high-value assets and luxury goods. At this stage the funds or assets appear to have been legitimately acquired.

Money laundering behaviour reflects the dynamic and adaptive nature of organised crime. There are four key behaviours that have been identified in Australia's current money laundering environment:

- **Intermingling (or commingling) legitimate and illicit financial activity –** for example, through cash-intensive businesses and front companies. This process of reinvesting criminal proceeds and providing a cover for criminal enterprise is a well-established money laundering methodology.

- **Engaging professional expertise –** criminal groups and networks engage the services of professionals (such as lawyers and accountants) to enhance their capacity to operate in both legitimate and criminal markets and conceal their illicit activity, including money trails.

- **Engaging specialist money laundering syndicates –** specialist syndicates, based in Australia and overseas, provide specific money laundering services to domestic and international crime groups operating in Australia.

- **The 'internationalisation' of the Australian organised crime environment –** there is almost always an international component to the money laundering cycle for major crime groups operating in Australia.

AUSTRAC works to develop Australia's AML/CTF regime to keep pace with changing money laundering methods and emerging threats.

Methods used to launder money through the banking system

Criminals use a range of strategies to try to get around the AML controls that have been put in place by banks operating in Australia. These strategies include:

- **Structuring –** depositing large amounts of cash by first breaking it down into smaller amounts to avoid raising suspicion or triggering mandatory reporting (TTRs) of cash transactions of AUD10,000 or more under the AML/CTF Act.

- **Complex company and trust ownership structures –** these structures, which can involve multiple entities in multiple jurisdictions, are used to screen the ultimate source of funds and the true beneficial owners of those funds.

- **Third parties or third-party accounts –** these are used to blur the connections between criminals, the proceeds of their crimes and attempts to launder funds. A technique called 'smurfing' involves numerous third parties conducting transactions on behalf of criminals. Large cash amounts are broken into multiple smaller amounts and then given to third parties to deposit in accounts held in different financial institutions. These third parties may be complicit or unwittingly involved in this money laundering activity.

- **Identity crime –** transactions made using stolen, fraudulently obtained or fictitious identities obscure the link between the funds and their true source or origin.

Example of AUSTRAC's role in responding to the threat of money laundering through the banking system

The AUSTRAC CEO has a power to make AML/CTF Rules in relation to certain matters under the AML/CTF Act. He uses this power to respond to the level of threat in various industry sectors; for example, by exempting low-risk entities or classes of entities from all or part of the regime, or by imposing particular requirements as permitted by the AML/CTF Act.

On 1 October 2011, AML/CTF Rules came into effect requiring all reporting entities to identify third parties undertaking threshold transactions of AUD10,000 or more. This obligation is in addition to reporting the details of the holder of the account regarding which the transaction is being conducted. This reporting requirement provides valuable intelligence to help identify people who attempt to disguise their income by accessing or controlling another person's account, or who seek to distance themselves from an account or a transaction.

AML/CTF Rules introducing enhanced customer due diligence (CDD) measures will take effect on 1 June 2014. These measures will strengthen the requirements for reporting entities to identify their customers and other third parties in relation to complex ownership structures involving companies and trusts.

AUSTRAC's role in Project Wickenby is to provide specialised analysis of AUSTRAC's data holdings. AUSTRAC information and analysis have been used by Project Wickenby for the initial identification of possible targets, financial profiling and target development of suspected international tax fraud, and exchange of financial intelligence with a number of international counterparts.

Through the analysis of IFTIs, mostly reported through the banking system, AUSTRAC continues to monitor the number of Australian entities transacting with tax secrecy havens, including Vanuatu, Liechtenstein, Jersey and Switzerland. Project Wickenby has identified 13 tax secrecy havens of interest. Not all of these jurisdictions have been publicly disclosed. AUSTRAC performs comprehensive analysis of the movement of funds between Australia and tax secrecy havens to assess Project Wickenby's impact and identify any changes which may indicate funds have been displaced (moved) to other secrecy jurisdictions.

Case study: Asian crime syndicate recruited foreign students to steal and launder money

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

The scam began with the theft of cheques and credit cards from private mailboxes. The stolen documents were altered to create forgeries of sufficient quality to deceive bank tellers. The foreign students would deposit the cheques into their own bank accounts or accounts set up using false names. When a cheque cleared, the money was withdrawn and gambled at casinos to mix or commingle it with legitimate cash – a common money laundering methodology.

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

One suspect was arrested and charged with eight counts of dealing with the proceeds of theft. The individual had allegedly stolen a cheque for more than AUD500,000 from a deceased estate and attempted to launder the proceeds of the cheque through a casino. A second suspect was arrested and charged with six offences, including making a false document to obtain a financial advantage. A third suspect was arrested and charged with identity fraud and money laundering offences.

Methods used to launder money through money transfer businesses and alternative remittance services

- **Structuring –** as in the banking sector, the technique of breaking down transactions into smaller amounts is widely used to try to avoid detection.

- **Cuckoo smurfing –**this has emerged as a key money laundering methodology over the past decade. It involves complicit remittance dealers operating as 'go-betweens', depositing illicit funds (for instance, the proceeds from drug deals) into accounts of innocent parties who are expecting transfers from legitimate transactions made overseas.

In exchange, criminals receive matched payments overseas without leaving a money trail back to them.

- **Offsetting –** the common alternative remittance practice of offsetting — hawala or hundi — enables the international transfer of value without actually transferring money. This is possible because the arrangement involves a financial credit and debit (offsetting) relationship between two or more dealers operating in different countries. Criminals can exploit offsetting to conceal the amount of illicit funds transferred, obscure the identity of those involved and avoid detection by AUSTRAC of non-reporting.

- **Remitters as third party –** law enforcement agencies have detected cases where Australia-based remittance businesses are used as a third party to move funds or settle transactions involving two or more foreign countries. Similar to cuckoo smurfing, this involves overseas-based remittance dealers accepting legitimate transfer instructions from innocent parties (for example, to import or export goods) but instead of conducting the transfer themselves they send instructions to Australian counterparts. This is common practice among alternative remittance businesses, as part of their routine settlement of debts, to ease cash flow constraints or take advantage of foreign exchange differences. However, some Australian remittance dealers have exploited this opportunity to launder cash from Australian organised crime by transferring it to recipients overseas. Likewise, the overseas remittance dealers supply 'clean' cash to overseas-based crime groups with links in Australia.

- **Manipulation by specialist money laundering syndicates –** law enforcement agencies have also identified specialist money laundering syndicates exploiting remittance businesses to move illicit funds, particularly where the business has links to high-risk countries. Some of these syndicates are based in Australia, while others operate from overseas and rotate teams into Australia to move illicit money on behalf of organised crime.

Examples of AUSTRAC's role in responding to the threat of money laundering through the alternative remittance sector

To address the sector's high-risk nature, remittance businesses must register their business with AUSTRAC. This requirement is in line with the FATF standards, which recommend that countries implement licensing or registration schemes for the sector. These businesses are reporting entities for the purpose of the AML/CTF Act and must comply with all relevant obligations, including CDD and submission of transaction reports to AUSTRAC.

Amendments to the AML/CTF Act in 2011 strengthened the registration requirements for remitters and enhanced the AUSTRAC CEO's powers to deal with their compliance with the Act. These new measures include requiring remittance providers to undergo a more rigorous registration process and enable the AUSTRAC CEO to refuse, suspend, cancel or impose conditions on registration. To date, AUSTRAC has cancelled the registration of one remitter, five entities have been refused registration on the Remittance Sector Register, 15 entities have had conditions imposed on their registration, and in November 2013 AUSTRAC imposed a fine of almost a quarter of a million dollars on one of the world's top three remittance network providers for failing to register affiliates and providing services through unregistered affiliates.

In addressing high-risk remitters being misused by serious and organised crime, AUSTRAC jointly formed Taskforce Eligo in 2012 with the ACC. Taskforce Eligo is detailed below in section 7 – The role of the Australian Crime Commission and the Australian Federal Police in detecting financial related crime.

Case study: Money laundering remitter jailed after sending false reports to AUSTRAC

Law enforcement conducted an investigation into a remittance service provider suspected of falsifying customer information on transaction reports and submitting false information to AUSTRAC, to facilitate money laundering. AUSTRAC information was critical to the law enforcement investigation to help identify that the remitter and his remittance business had assisted a criminal syndicate with laundering the proceeds of identity fraud that involved money fraudulently withdrawn from the bank accounts of innocent third parties. A key element in laundering criminal proceeds involved the remitter disguising the funds and concealing the identity of the criminal syndicate members.

The typical activity undertaken to launder the illicit funds involved a syndicate member obtaining access to a victim's account and arranging for funds from the account to be sent as an IFTI into an Australian account operated by the remitter. The remitter would place an order with a currency exchange business to collect an amount of foreign currency equivalent to the value of the stolen funds. Using the stolen money, the remitter would transfer funds into the currency exchange's customer deposit account, then visit the currency exchange to collect the foreign currency. With the original stolen funds now laundered into foreign currency, the remitter would provide the foreign currency, less a commission, to a syndicate member. As a last step in concealing the money trail, the remitter would file a significant cash transaction report (SCTR, under the FTR Act) with AUSTRAC detailing the payment to the syndicate member, but using false identification details to conceal the recipient's true identity.

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

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

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

Law enforcement collected evidence confirming the remitter was involved in money laundering on behalf of third parties. The remitter was charged and convicted on multiple counts of dealing with the proceeds of crime worth more than AUD100,000, contrary to

section 400.4 of the Criminal Code. The remitter was sentenced to five years and six months imprisonment, with a minimum of three years and seven months. The remitter was also charged and convicted of money laundering offences.

Methods used to launder money through the gaming sector

- **Exchanging illicit cash for casino chips or gaming tokens.** This is a common gaming-related money laundering method observed by law enforcement agencies. The casino chips are then cashed in as 'winnings' and the money, which is now linked to a legitimate source, is spent domestically or transferred to overseas accounts. These methods are often used in the placement and layering phases of money laundering.

- **Exploiting third parties – 'mules' and 'cleanskins'.** To avoid direct involvement in the money laundering process, criminals may use 'mules' (people unrelated to the initial criminal activity, who are used to unwittingly transfer funds to criminals overseas) or 'cleanskins' (complicit third parties who have no criminal record) to carry out the risky transactions on their behalf. In some instances, these people may be known to the criminal – they may be family members or associates. For example, in one case an organised crime group used third parties to gamble cash proceeds from heroin importation. They recruited mules to purchase gaming chips and cash them in. The cash-ins were structured into smaller amounts to try to avoid mandatory threshold reporting. The group later sent the funds to criminal entities in South-East Asia through a complicit alternative remittance business.

- **Casino VIP rooms and high-stakes gambling**. Casino VIP rooms offer exclusive access to high-stakes gaming tables to Australian and overseas players. VIP members can place high-value bets in these rooms. In compliance with their AML regulatory obligations, casinos closely monitor and track VIP and high-stakes gaming activity. High-stakes gaming is vulnerable to abuse because it is common for players to gamble with large volumes of cash, the source and ultimate ownership of which may not be readily discernable.

- **Casino-based tourism and junkets.** Casino-based tourism is recognised nationally and internationally as being potentially susceptible to money laundering. Junket operators organise gambling holidays to casinos. Common risks include people carrying large amounts of cash into or out of countries, junket operators moving large sums electronically between casinos or to other jurisdictions, and layers of obscurity around the source and ownership of money on junket tours — players may elect to have junket representatives purchase and cash-in casino chips on their behalf. Junket representatives are often the main contact between the casino and the playing group, which can limit the face-to-face contact between gaming venues and players. This can restrict the venue's ability to conduct effective customer due diligence on individual junket players.

- **Electronic gaming machines.** Electronic gaming machines commonly found in casinos, pubs and clubs offer criminals an accessible way to launder smaller amounts of cash proceeds of crime. Intelligence and case studies reveal criminals can launder illicit cash through these machines by claiming gaming machine payouts from legitimate players (that is, paying cash to a player who has accumulated credits and then requesting a cheque from the gaming venue for the credits). Another method involves putting large

amounts of cash or credits through gaming machines and then cashing out these credits as 'winnings'.

- **Online gambling.** Overseas investigations indicate that crime syndicates use online gambling platforms to launder funds.

Examples of AUSTRAC's role in responding to this threat of money laundering through the gaming sector

The AML/CTF Act applies to the provision of a range of designated services in the gaming sector, including accepting bets, paying out winnings, allowing a person to play on a gaming machine and exchanging money for chips. These designated services are recognised as vulnerable to abuse by criminals for money laundering purposes. Under the AML/CTF Act, gaming facilities which provide designated services to a customer are generally obligated to:

- develop and maintain an AML/CTF program
- identify and verify customer identity where the services (for example, accepting bets, paying winnings, exchanging money for chips) involve AUD10,000 or more
- report to AUSTRAC regarding suspicious matters, cash transactions of AUD10,000 or more and IFTIs (reports of international funds transfers mainly relate to casinos).

Methods used to launder money through high-value goods

- **Commingling legitimate and illicit financial activity.** Criminals may pay for goods such as real estate using a mix of cash from crime and legitimate sources. Criminal proceeds and legitimate money (or assets) can also be channelled through company accounts which are used as a front for the purchase of other legitimate assets for personal use such as motor vehicles.
- **Adding layers and concealing ownership**. Criminals commonly conceal asset ownership to avoid confiscation. This can involve registering high-value assets such as real estate or cars in family or associate names, or purchasing assets in false names.
- **Real estate.** Money may be laundered through real estate by manipulating property values, mortgage and investment schemes, complex corporate vehicles and loan arrangements. In 2004 it was estimated that $651 million worth of laundered funds were invested in real estate annually. (AUSTRAC, John Walker and RMIT University, 2004, *The extent of money laundering in and through Australia in 2004*, Criminology Research Council, www.criminologyresearchcouncil.gov.au/ reports/200304-33.pdf)
- **Art, antiques and jewellery.** These high-value goods are used to disguise the real amount of money laundered because a true 'market price' can be hard to establish. Criminals can misrepresent the value of these goods by under- or over-valuation to disguise the amount of criminal income laundered through their purchase.
- **Semi-precious stones and jewellery, gold and silver bullion and valuable coins.** These assets are easily transportable and enable criminals to move value within or across borders with low risk of generating suspicion or detection.

Examples of AUSTRAC's role in responding to this threat of money laundering through high-value goods

Confiscating the assets derived from crime is a key tool for countering organised crime. In 2002, Commonwealth legislation was strengthened with the introduction of a non-conviction based regime and more recently with the addition of unexplained wealth laws in 2010 under the *Proceeds of Crime Act 2002* (POCA). Measures available under POCA include:

- forfeiture orders – property/instrument is forfeited to the Commonwealth
- pecuniary penalty orders – offender pays amount equal to the benefit they are calculated to have gained from crime
- literary proceeds order – offender pays amount calculated as the benefits received through commercial exploitation of their notoriety from offending.

The unexplained wealth laws place the onus of proof on the individual whose wealth is in dispute, and require that person to attend court and show that their wealth was obtained legitimately. If a person is unable to do so, the court may order the person to pay the amount of their wealth that they cannot demonstrate was legitimately obtained to the Commonwealth.

In 2011 a multi-agency Criminal Assets Confiscation Taskforce was established to provide a more coordinated and integrated approach to identifying and removing the profits derived from organised criminal activity. Led by the AFP and using resources from the ACC, the ATO and the Commonwealth Director of Public Prosecutions, the task force has stepped up the government's fight against organised crime through a more intensive targeting of criminals' accumulated wealth. AUSTRAC information and analysis is a valuable source of financial intelligence for this task force.

Less visible money laundering channels and sectors

Organised crime groups are increasingly using networks of businesses, companies, partnerships and trusts to support criminal activity and launder illicit funds. In this context, it is becoming more common for organised crime to engage a range of professionals to provide advice, establish and, in some cases, administer these complex structures which disguise illicit money flows.

Some professionals are unwittingly exploited by criminals, while others are criminal entities in their own right. Australia-based and overseas-based crime groups use professionals such as lawyers, accountants, financial advisers and real estate agents to help undertake transactions to:

- obscure ultimate ownership through complex layers and structures
- conceal proceeds of crime
- legitimise illicit funds
- avoid tax
- avoid regulatory controls

- provide a veneer of legitimacy to criminal activity
- avoid detection and confiscation
- frustrate law enforcement investigations.

Australian legal professionals have advised AUSTRAC of receiving unusual requests from prospective clients, particularly targeted at passing funds through solicitors' trust accounts. Examples of these requests include:

- a foreign company requesting legal services involving debt recovery, with the legal firm receiving substantial payments into its trust account from purported debtors (both in Australia and overseas), with little debt recovery work actually being required to be undertaken by the firm
- a foreign investor transferring large amounts into a firm's trust account, ostensibly for property and other investments, but then halting the investment and asking for the money to be paid to multiple recipients according to the direction of a third party.

Example of AUSTRAC's role in responding to this threat – reforms to CDD requirements

Australia's AML/CTF regime needs to continue to evolve to effectively address identified vulnerabilities. One such example is amendments proposed to be made by the AUSTRAC CEO to the CDD requirements in the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No 1)* (AML/CTF Rules). The amendments come into effect on 1 June 2014 and will require reporting entities to:

- determine the beneficial owner of a customer (the ultimate individual who owns or controls the customer) by looking through complex legal structures
- determine if the customer or beneficial owner is a politically exposed person (PEP)
- consider, within a reporting entity's AML/CTF program, the risks associated with beneficial ownership, control structures, PEPs, and the purpose and intent of the business relationship
- undertake reasonable measures to update information in relation to their customers.

Without measures to increase the transparency of beneficial ownership, criminals and terrorists will be able to continue to abuse legal structures to aid ML/TF.

CDD and reporting by businesses is critical to enabling the detection, investigation and prosecution of offences and protecting the Australian financial system, revenue base and national security interests. Regulated businesses are best placed to assess their money laundering risks. To properly assess these risks, businesses need a full understanding of their customers.

Electronic payment systems and new payment methods

Electronic payment systems and new payment methods have become an integral part of the globalised economy. Their dynamic nature and rapid technology developments offer opportunities for criminals to exploit these systems for money laundering purposes.

Areas of concern internationally and in Australia fall into two main categories: ATM/EFTPOS networks and cards; and online and new payment methods. While these systems differ in many ways, they can both provide anonymity and do not require face-to-face business relationships and transactions. These systems are used to:

- **commingle illicit cash with legitimate business takings** — for example, merchant-filled ATMs, where funds for dispersal are privately stocked, could be exploited to place illicit funds into the legitimate financial system

- **move illicit funds across borders** — for example, through international use of credit and debit cards which provide instant access around the world to ATM withdrawals, and through online payment systems which provide a quick and easy way to transfer funds between individuals or businesses

- **conceal criminal proceeds and send them offshore** — for example, through stored value cards which enable real-time transfer of cash domestically or overseas, and through digital currencies or e-currencies which can be exchanged for traditional currency using either cash or electronically via credit card or bank account.

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

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

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

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

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

'Digital currencies' and so-called 'virtual worlds' offer opportunities for criminals to launder money due to their global reach, lack of face-to-face transactions and the convenience of using electronic commerce. While the nature and extent of money laundering through digital currencies and virtual worlds are unknown, it is important to recognise their potential for criminal exploitation, particularly in response to tighter regulation of established or traditional financial channels.

The evolution of digital currencies has led to the development of internet-based, electronic means of transferring 'real-world' value. In contrast to traditional physical currencies issued by national governments, digital currencies (such as Bitcoins, SolidCoins and Linden dollars) are issued by commercial enterprises and are not backed by traditional currencies, precious metals or other physical commodities.

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

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

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

However, there are some disadvantages for criminals using digital currencies for illicit purposes. In general, digital currencies at this time are not widely accepted as payment for goods and services. There are also subject to substantial and rapid exchange rate fluctuations and can be hacked into and stolen. This limits the avenues through which digital currency can be used to convert, move and launder illicit funds. In contrast, traditional financial channels (such as banks and remittance services) interact with a wide range of economic sectors through which illicit funds in large volume can be moved, commingled and concealed. The overall utility of digital currencies for criminals at this point may currently be limited to niche crimes in the cyber environment and individual or smaller scale illicit activity.

Virtual worlds (also known as gaming platforms, 3D environments and massive multiplayer online games) are internet-based simulated 'worlds' with their own virtual 'economy'. The economy generally based upon a digital currency that can be purchased and/or converted into real currency. Users interact with each other in a virtual, borderless environment, purchasing virtual property, trade goods, services and currency. This provides potential for criminals to

launder money with anonymity – for example, to purchase 'virtual real estate' using illegally obtained money in an attempt to legitimise the transfer of funds to a third party. The proceeds of these transactions can subsequently be converted into real currencies or transferred offshore or to third-party accounts.

The vulnerabilities associated with digital currencies and virtual worlds include:

- Digital currencies and virtual worlds are generally not captured by AML/CTF legislation around the world. Because there is limited or no regulation of digital currency transactions, authorities have difficulty monitoring criminal activity that exploits digital currencies.

- Online DCEs provide the opportunity for criminals to exchange digital currencies for other digital currencies before converting them into real-world currency. This provides additional 'layering' in the money laundering cycle.

- Criminals can use their illegally obtained physical currency to purchase the digital currency of a virtual world. Depending on the virtual world platform or online DCE, digital currency can be purchased using a debit card, credit card, internet payment service provider or, in some instances, using an online voucher payment.

- The proceeds of some transactions can be converted into traditional or real currency by linking a virtual account to a debit card or through DCEs. These channels would allow individuals to trade digital currencies and receive payment via a debit card, credit card or internet payment service provider.

Case study: Potential misuse of virtual worlds and digital currency examples

An international investigation by a foreign law enforcement agency and FIU identified an international internet payment service provider who was suspected of laundering illicit proceeds from fraudulent schemes. The complex money laundering investigation revealed multiple DCEs, precious metals providers and stored value card providers implicated in the scheme, either unwittingly or otherwise.

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

AUSTRAC's ability to respond to the threat of money laundering through electronic payment systems and new payment methods

Funds transferred via digital currencies and virtual worlds will almost always intersect with the traditional financial channels (such as banks and remittance services) at some point (whether as physical currency or electronic funds). As such, transaction reporting to AUSTRAC by mainstream financial service providers and monitoring by AUSTRAC does provide an important mechanism for keeping track of activity in the digital area.

3. The involvement of organised crime

AUSTRAC released a public report, *Money laundering in Australia 2011* (MLA 2011), derived from the classified NTA 2011. Commonwealth, state and territory law enforcement, intelligence, revenue, regulatory and policy-making bodies are using the NTA 2011 to inform their response to organised crime.

The NTA 2011 confirmed the view formed in law enforcement strategic assessments that money laundering is one of the critical organised crime risks to the Australian community. It is the common denominator of almost all serious and organised crime and continues to pose a threat to the integrity of Australia's business and financial systems. Money laundering exploits vulnerabilities in products and services in an attempt to conceal proceeds of illicit activities and commit financial and other serious crimes. It is also intrinsic to serious tax crimes and a threat to revenue.

AUSTRAC's annual typologies and case studies reports <www.austrac.gov.au/typologies.html>, produced since 2007, contain hundreds of law enforcement cases that have used AUSTRAC information. Many of these cases involve organised crime.

4. In relation to money laundering—the large number of high denomination banknotes in circulation

AUSTRAC does not collect information in relation to the number of high denomination banknotes in circulation – this falls under the role of the Reserve Bank of Australia. AUSTRAC does, however, collect information in relation to cash transactions of AUD10,000 or more, in TTRs.

TTRs from 2011 to 2013

Industry sector	**Average number of TTRs/year**	
	Cash amount $10K-$100K	*Cash amount over $100K*
Alternative remittance	40,236	1,454
Gambling	86,163	1,401
Cash-in-transit	1,668,963	415,956
Financial institutions	2,976,935	15,136
Foreign exchange	45,434	5,585

These figures show the average number of TTRs (1 January 2011 to 31 December 2013) submitted per year by the major industry sectors. The reports are divided into two groups:

- Cash amount $10K to $100K
- Cash amount greater than $100K.

5. In relation to identity fraud—credit card fraud in particular

The AML/CTF Act requires that businesses must verify the identity of their customers, monitor their customers' behaviour and keep appropriate records. The 'know your customer' (KYC) and CDD processes are a fundamental element of an effective AML/CTF system and provide a direct means of preventing and detecting identity fraud. Reporting entities are required to indicate in each SMR they submit to AUSTRAC, the suspected offence underpinning the suspicious matter report (the 'offence type'), as well as their 'reason for suspicion'. Offence types and reasons for suspicion for SMRs received in 2012–13 relating to identify fraud include:

Suspect activity types recorded 2012-13

Activity type	***Total***
Social security issue/fraud	1,185
Fraud – credit/loan	1,162
Fraud – other	819
Refusal to show ID/ complete cash transaction report	402
False identity/name	285
Fraud – cheque	271
Fraud – internet banking/phishing scam	94
Total	***3,033***

Offence type as reported by industry in SMRs 2012-13

Person/agent not who they claim to be	1,112

Reasons for suspicion as reported by industry in SMRs 2012-13

Activity type	***Total***
False name/identity or documents	2,002
Refusal to show identification	402
Internet fraud	1,629
Social security issue	1,173
ATM/cheque fraud	494
Unauthorised account transactions	549
Credit/loan facility fraud	908
Credit card fraud	201
Phishing	23
Total	***7,381***

Case study: Superannuation accounts targeted in a multi-million dollar identity theft

AUSTRAC information was used extensively by a law enforcement agency to investigate a multi-million dollar identity theft and fraud syndicate which targeted superannuation accounts. Syndicate members stole cheques, superannuation and personal bank statements from victims' mailboxes and used this information to produce high-quality counterfeit identity documents, which were then used to conduct frauds. Syndicate members also approached some victims directly, offering early access to their superannuation funds and requesting details of their funds to facilitate access to their benefits. The syndicate used the following methods:

1. Syndicate member steals a victim's identification papers and opens a self-managed superannuation fund (SMSF) in the victim's name, then sets up a linked (but fraudulently obtained) bank account using the details of the new SMSF. Assuming the victim's identity, the syndicate member contacts the victim's superannuation provider and requests they 'roll over' the funds from the legitimate superannuation fund into the new (fraudulent) SMSF. The syndicate member then withdraws the funds from the new SMSF and sends them to the member's offshore account using remittance service providers.

2. Syndicate member offers a victim the chance to access their superannuation funds early. Scammers usually target victims struggling with debt, unemployed and/or from non-English speaking backgrounds. The victim provides their financial and identification details to the syndicate member, who withdraws the funds and takes approximately 20 per cent as their fee. The balance is paid to the victim in cash. In a variation of this method, the syndicate member steals all the victim's superannuation funds and the victim receives nothing.

3. Syndicate member offers to roll over a victim's superannuation into a legitimate fund that they claim will offer a better return. The victim provides their financial and identification details. The syndicate member rolls over the victim's funds into the syndicate member's fraudulent SMSF and then withdraws the funds from the bank account.

AUSTRAC received SMRs and SUSTRs about individuals suspected of perpetrating the fraud. These reports, combined with further AUSTRAC analysis, identified the large criminal syndicate that was receiving regular cheque deposits into newly opened accounts and paying an additional fee to ensure the cheques cleared quickly. Once the cheques were deposited, the funds were withdrawn from the accounts, either via cash (in amounts of AUD1,000–AUD20,000) or cheques (between AUD6,500 and AUD45,000) made payable to third parties. The cash withdrawals of AUD10,000 or more were reported to AUSTRAC as significant cash transactions. The syndicate was also identified as submitting fraudulent applications to roll over funds from victims' superannuation funds managed by retail or industry fund managers, into accounts held by the syndicate members.

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

Twenty-five syndicate members were charged with more than 2,500 offences involving laundering over AUD8 million in fraudulently obtained funds. The syndicate head, who controlled three bank accounts which turned over AUD1.6 million, was charged and found guilty of 57 counts of identity fraud and money laundering relating to transactions valued at more than AUD550,000.

Case study: Ten thousand fake credit cards seized from money laundering syndicate

An SMR was the catalyst for a law enforcement operation which resulted in the arrest of three foreign nationals. The operation revealed a multi-million dollar money laundering syndicate that was laundering illicit proceeds derived from producing fraudulent credit cards. As a result of the SMR referral, authorities seized more than 10,000 fake credit cards that they believed had the potential to fund AUD25 million worth of fraudulent transactions.

The initial SMR related to the main suspect making an outgoing IFTI to China, funded with AUD500,000 in cash from an unknown source. Two foreign nationals were recruited by the main suspect to conduct similar transactions. The SMR lodgement triggered AUSTRAC's automated monitoring systems and initiated AUSTRAC enquiries of related financial transactions. The enquiries revealed that the syndicate used remitters who primarily sent funds to Chinese beneficiaries, and identified other high-value transactions made by the main suspect. Those transactions included cash deposits of more than AUD10,000, which were reported to AUSTRAC via TTRs.

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

A further seven SMRs were submitted to AUSTRAC from reporting entities over the next four months, detailing transactions worth AUD2 million including cash deposits and IFTIs. The SMRs identified that the syndicate was: depositing large values of cash into the account of a remittance business, to fund IFTIs sent immediately after the deposit; and conducting multiple domestic transfers from several bank accounts into the same remitter's bank account, to fund IFTIs equal in value to the domestic transfers. AUSTRAC assisted authorities with further searches on related financial transaction reports and found that the syndicate had, over the same four-month period, deposited more than AUD5 million in cash and conducted AUD6.5 million worth of outgoing international funds transfers to China and Hong Kong.

Authorities arrested the main suspect and two other foreign nationals, and seized fraudulent credit cards, sophisticated card-making equipment and AUD60,000 cash. Two of the syndicate members pleaded guilty to dealing with cash reasonably suspected of being the proceeds of crime, and were sentenced to seven months and 12 months imprisonment respectively. The main suspect was charged with offences relating to the manufacture of counterfeit credit cards, possessing proceeds of crime, money laundering offences and having a false passport. The suspect was sentenced to a maximum of five years and nine months.

6. The operation and effectiveness of Commonwealth legislation, administrative arrangements and law enforcement strategies

The AML/CTF Act, regulations and AML/CTF Rules

The AML/CTF Act, with its combination of rule-making, exemption and modification powers provides an effective and efficient set of regulatory tools which enable the AUSTRAC CEO to provide regulatory relief to low-risk reporting entities (including small business) while maintaining the integrity of the AML/CTF Act.

The AML/CTF Act is principles-based legislation that promotes a risk-based approach to AML/CTF compliance. As required by FATF, the AML/CTF Act sets out the principal obligations for reporting entities, which are required to develop risk-based systems and controls tailored to the nature, size and complexity of their business and proportionate to the level of ML/TF risk they face. It is the responsibility of the reporting entity to determine how it can meet these obligations. This approach recognises that the reporting entity is in the best position to assess the risks its business faces in relation to customers, products and services, and provides the flexibility for reporting entities to allocate appropriate resources to counter those risks.

Under section 229 of the AML/CTF Act, the AUSTRAC CEO may, in writing, make AML/CTF Rules. AML/CTF Rules (which are binding legislative instruments) set out specific requirements under the AML/CTF Act. AUSTRAC develops the AML/CTF Rules in consultation with the Attorney-General's Department, relevant government agencies, industry and other stakeholders.

The AML/CTF Rules are also used to exempt reporting entities from obligations, either in full or part – for example, where an assessment of the level of ML/TF risk posed by small business reporting entities justifies a full or partial exemption from obligations under the AML/CTF Act.

The AML/CTF Act also includes a framework that enables the AUSTRAC CEO to provide regulatory relief to specific entities. Under section 248 of the AML/CTF Act, the AUSTRAC CEO may exempt a reporting entity from one or more provisions of the Act or modify the operation of provisions of the Act in relation to reporting entities.

This flexibility, provided for in the AML/CTF Act and practised by AUSTRAC as a regulator, meets a number of the recommendations made by the Productivity Commission in its 2013 report *Regulator Engagement with Small Business – Research report*. In particular, recommendation 5 states that: ‘Regulators should adopt a risk based approach, ensuring that decisions about the nature and level of compliance obligations and enforcement responses consistently reflect an assessment of the relative risks posed by business activities.’

In accordance with section 251 of the AML/CTF Act, and following an announcement by the Minister for Justice, the Hon Michael Keenan MP, a statutory review of the operation of the AML/CTF Act, regulations and AML/CTF Rules commenced on 4 December 2013. Refer to '10. The need for any legislative or administrative reform' (below) for further information.

As noted below, Australia is currently the subject of an evaluation by FATF. This evaluation will consider not only the technical compliance of Australia’s regime with the international

standards, but also our effectiveness in the context of 11 objectives. The evaluation is due to be completed for report to the FATF plenary in February 2015.

Regulatory approach with regard to AML/CTF

As Australia's AML/CTF regulator, AUSTRAC educates, monitors and works with reporting entities to improve their compliance with the requirements of the AML/CTF Act, AML/CTF Rules and the FTR Act. In some circumstances AUSTRAC seeks to enforce compliance through more formal mechanisms. AUSTRAC takes a risk-based approach to its regulation of reporting entities.

AUSTRAC has a regulated population of approximately 13,900 reporting entities (as at 1 April 2014), which can be broken down into the following categories.

- **Banks and other lenders:** This sector comprises approximately 1,200 entities, covering authorised deposit-taking institutions (ADIs – including domestic banks, foreign bank branches and subsidiaries, credit unions and building societies) and other lending institutions (including finance companies, micro lenders and specialist credit providers).

- **Non-bank financial service providers**: This sector comprises approximately 2,650 entities providing a variety of services such as financial planning, funds management, stockbroking, custody, superannuation and life insurance. The entities in this sector range from large, sophisticated organisations through to small businesses.

- **Gambling and bullion service providers:** This diverse sector comprises approximately 4,300 entities, including casinos, TABs, hotels and clubs with electronic gaming machines, corporate bookmakers, bookmakers and bullion dealers.

- **Money service businesses and remittance dealers:** This large and diverse sector comprises approximately 5,750 entities, including remittance service providers, cash carriers and currency exchange dealers.

AUSTRAC's regulatory approach is outlined in the *AUSTRAC supervision strategy 2012-14*, which is published on the AUSTRAC website <www.austrac.gov.au/strategies.html>.

AUSTRAC has a range of enforcement tools at its disposal including persuasive remediation and formal powers. AUSTRAC's enforcement approach is outlined in the *AUSTRAC enforcement strategy 2012-14* <www.austrac.gov.au/strategies.html>.

AUSTRAC has increased its enforcement action since the commencement of the AML/CTF Act in 2006. Most of the obligations under the AML/CTF Act did not come into effect until two years after its commencement, at which time reporting entities were subject to a two-year Policy (Civil Penalty Orders) Principles period. This meant that AUSTRAC could initiate civil penalties against reporting entities only when the entities had failed to take reasonable steps to comply with their obligations. AUSTRAC was well placed, as a result of strengthening its enforcement capability, to take action when non-compliance was identified and the full suite of powers came into effect from 2008.

Summary of AUSTRAC enforcement actions from 2008-2014

Enforcement action	2008–09	2009–10	2010–11	2011–12	2012–13	2013-14
Infringement notices (section 184)						1
Enforceable undertakings (section 197)	1	3	7 (one reporting entity group)	1	1	
Remedial direction (section 191)		1	1	1		
Notices to appoint an authorised external auditor (section 162)		7 (one reporting entity group)		1		
Removal from the Register of Providers of Designated Remittance Services			2			
Imposed conditions on Remittance Sector Register (RSR)				3	5	
Refused applications for registration on RSR					2	3
Conditions imposed on RSR						7
Cancellation of registration on RSR						1
Assessments conducted		386	311	359	317	117
Requirements and recommendations issued		2572	1053	1656	1187	686

AUSTRAC's Compliance branch, after assessing compliance with AML/CTF obligations, issues a compliance assessment report requiring an entity to take specific actions to remedy non-compliance within specific time frames. These actions are in the form of 'requirements' that set out the provisions of the AML/CTF Act or AML/CTF Rules that have not been met, and 'recommendations' that set out proposals for action or procedural changes that should be formally considered for implementation. Where requirements are not satisfactorily addressed, AUSTRAC will consider a proportionate regulatory response which can include using its enforcement powers.

The enforcement action that AUSTRAC has taken since 2008 is an important component of the agency's regulatory approach in not only correcting non-compliance at an individual reporting entity level, but also deterring non-compliance at an industry level. To provide an effective deterrent effect, enforcement must present as a credible risk to reporting entities that non-compliance will be detected and that the cost of enforced compliance will outweigh the

benefits of that non-compliance. AUSTRAC has broadened and strengthened its enforcement action over time, as the regulatory regime has matured and as reporting entities have had time to voluntarily meet their obligations.

AUSTRAC has continued to build its capacity as an FIU through ongoing enhancements to its intelligence systems, by strengthening its partnerships with domestic and international partners and closely monitoring developments in the ML/TF risk environment. AUSTRAC contributes to global efforts to combat ML/TF and serious organised crime through information exchange with foreign FIUs and regulators, involvement in international AML/CTF forums, and ongoing monitoring of the effectiveness of Australia's AML/CTF framework to meet international standards. AUSTRAC's international technical assistance and training provided to foreign counterparts further enhances the quality of intelligence available within the region.

In 2012-13, AUSTRAC received more than 84 million individual reports of financial transactions. There was a particularly significant rise in the number of IFTIs reported. Incoming and outgoing international transfer reports numbered almost 80 million in 2012–13, with a total value of more than $3.5 trillion. AUSTRAC also received more than 40,000 SMRs.

Transaction reporting data is the foundation of AUSTRAC's intelligence work and supports hundreds of major investigations by law enforcement, national security and other competent authorities each year. During 2012–13 AUSTRAC's intelligence contributed to national and international investigations into a wide range of criminal activities, including professional money laundering syndicates, people smuggling, tax evasion, drug trafficking and investment fraud. In 2012-13 AUSTRAC made 1,341 disseminations to domestic partner agencies and undertook 245 financial intelligence exchanges with foreign FIUs. In addition, over 3,000 law enforcement officials have direct access to financial data via AUSTRAC's systems for use in their day-to-day operations.

Where appropriate, some of this information is released through publications such as AUSTRAC's typologies and case studies report series. Sharing this knowledge enables government and industry to develop and strengthen preventive strategies to detect terrorism financing.

Beyond law enforcement, financial information is also critical to AUSTRAC's role as Australia's AML/CTF regulator. FIU analysis that is informed by regulatory activity further enhances the quality of financial intelligence and its relevance to competent authorities.

AUSTRAC's role in law enforcement strategies

In considering AUSTRAC's contribution to law enforcement strategies and counter-terrorism financing and other national security matters, key points to note are that AUSTRAC:

- contributes to whole-of-government task forces and investigations as required
- provides support through its financial intelligence products, monitoring data for high-risk activities, and outposted intelligence officers

- plays a significant role in supporting the criminal investigations of other agencies – AUSTRAC does not prosecute offences under the AML/CTF Act but has the power to take civil penalty action for regulatory breaches.

The effectiveness of Australia's AML/CTF regime is measured by its success and providing benefits to the community in numerous ways, including preventing, detecting and disrupting crime. AUSTRAC's financial intelligence contributes to multi-agency investigations that target money laundering and tax evasion criminal networks, in addition to a range of predicate crimes such as drug trafficking, fraud, identity crime, people smuggling and national security matters.

For example, AUSTRAC is a key partner in the joint AUSTRAC/ACC Taskforce Eligo, through which law enforcement powers are combined with AUSTRAC's intelligence and regulatory functions to fight money laundering and financial crime facilitated by the remittance sector, and to improve regulatory compliance in that sector.

AUSTRAC was a key partner in the ACC-led Taskforce Galilee, which examined the problem of serious and organised investment fraud in Australia. AUSTRAC has also identified victims suspected of being involved in international dating and online scams.

In addition to the more general benefits derived from maintaining a stable financial system and enhancing the capacity of law enforcement and national security agencies to target criminal activities, Australia's AML/CTF regime directly helps protect members of the public. Monitoring transactions enables financial institutions and law enforcement agencies to detect irregular activity that might reveal that a customer's personal and account details have been stolen or misused. This monitoring also helps identify attempts by criminal groups to defraud individuals via 'Nigerian' or 'cold calling' scams.

International context

Australia's AML/CTF framework was developed in response to the FATF recommendations, which set the international global standards for combating ML/TF and proliferation financing for weapons of mass destruction. Australia is a founding member of FATF. The FATF standards were revised in February 2012 and are known as the FATF Recommendations – *International Standards on Combating Money Laundering & the Financing of Terrorism and Proliferation.*

FATF periodically reviews, by way of a 'mutual evaluation', the compliance of member countries with the FATF standards. Australia is currently subject to such an evaluation. The outcome of Australia's mutual evaluation will inform the Government of identified deficiencies and form major input into the current review of the AML/CTF Act and any subsequent reforms. As such, the AML/CTF Act review will be finalised once the mutual evaluation has concluded and reported its findings to FATF.

In February 2013, a revised FATF methodology for assessing the technical compliance of a member country and the effectiveness of its AML/CTF regime was published. Australia is among the first member countries to be assessed against the new methodology in the FATF 4th round of mutual evaluations. The resulting report is due to be presented to the FATF membership for consideration in February 2015.

Australia (Attorney-General's Department, AUSTRAC and Department of Foreign Affairs and Trade – DFAT) are currently engaging with the FATF assessment team regarding:

- the technical compliance assessment, which addresses specific requirements of the FATF Recommendations as they relate to the relevant Australian legal and institutional framework, and the powers and procedures of competent authorities

- the effectiveness assessment, which assesses the extent to which Australia achieves a defined set of outcomes central to a robust AML/CTF system and analyses the extent to which Australia's legal and institutional framework is producing the expected results.

Australian National Audit Office

In August 2012 the Australian National Audit Office (ANAO) commenced an audit of the effectiveness of AUSTRAC's arrangements for processing and disseminating financial intelligence to support domestic partner agencies and international counterparts. The ANAO consulted a number of AUSTRAC's domestic partner agencies as part of the audit.

The ANAO report was tabled in Parliament on 18 June 2013. The ANAO's overall conclusions were that AUSTRAC's financial intelligence is highly valued both domestically and internationally and that AUSTRAC has well-established, sound arrangements for processing and disseminating financial intelligence. This recognises AUSTRAC's significant effort in establishing a strong governance framework to manage and protect its data holdings and intelligence products.

ANAO recommended that AUSTRAC strengthen monitoring of partner agency personnel access to, and further dissemination of, AUSTRAC information; enhance management of unassessed transaction reports; and refine its performance reporting. AUSTRAC has accepted, and is working to implement, these recommendations. This includes re-negotiating and updating memoranda of understanding (MOUs) with domestic partner agencies, which will include stronger safeguards around the use and dissemination of AUSTRAC data and intelligence. AUSTRAC has also reviewed its approach to gathering structured feedback from partner agencies to measure the use, value, quality and relevance of AUSTRAC's financial intelligence.

7. The role of the Australian Crime Commission and the Australian Federal Police in detecting financial related crime

AUSTRAC plays a key role in the initiation of law enforcement investigations into financial crime, through the dissemination of SMRs and detections based on analysis of organic data holdings. AUSTRAC is also able to provide ongoing support to financial crime investigations through engagement with law enforcement agencies at the operational level. AUSTRAC provides operational support to financial crime investigations undertaken by the ACC, AFP and other law enforcement agencies.

The following examples demonstrate the extent to which AUSTRAC information has been used by investigating partner agencies to develop evidence and trace financial related crime, including criminal proceeds related to money laundering, associated predicate offences and terrorism financing.

Taskforce Eligo

AUSTRAC is a key partner in the multi-agency Taskforce Eligo, established in December 2012 to address money laundering vulnerabilities within the remittance sector, including the potential for exploitation by serious and organised crime. The task force is jointly led by AUSTRAC and ACC. Taskforce Eligo aims to professionalise the remittance sector through coordinated activity to disrupt money laundering and make it harder for organised crime to exploit this sector. The task force's activities complement AUSTRAC's ongoing regulatory activities to increase AML/CTF awareness and professionalism within the sector.

AUSTRAC's role is to provide support to partner agency operations, lead engagement with industry, especially major banks and across the remittance sector and, where appropriate, use its regulatory powers under the enhanced remitter regulation reforms in relation to high-risk remitters.

Since its commencement, Eligo has undertaken significant operational activity culminating in the disruption of several global money laundering and drug syndicates. During 2012–13 AUSTRAC's contribution to Eligo included the dissemination of intelligence reports and SMRs to Eligo partner agencies and international partners, undertaking data analyses, disseminating information about reporting entities' AML/CTF compliance and posting an intelligence analyst full-time with the ACC.

Attero National Task Force – Rebels outlaw motorcycle gang

Australia's law enforcement and Commonwealth agencies joined forces to establish a national task force to target one of Australia's highest risk criminal threats—the Rebels outlaw motorcycle gang. The Attero National Task Force is aimed at targeting, disrupting, disabling, dismantling and investigating the criminal activity of the Rebels in Australia. The Rebels is the largest outlaw motorcycle gang in Australia, with chapters in each state and territory, as well as overseas. AUSTRAC has contributed to the intelligence-gathering phase of the task force through financial analysis and identification of financial transaction reporting linked to known members of the Rebels.

$29 million restrained from Russian nationals' bank accounts

In December 2013, the AFP restrained $29 million in Australian bank accounts held by Russian nationals. This was brought to AFP's attention through information provided by reporting entities, who submitted financial reports to AUSTRAC relating to high-value funds transfers from companies in Hong Kong and China (some of which had been registered or had links to tax haven countries), into Australian bank accounts held by Russian nationals. The funds remain restrained while the investigation is ongoing.

200kg methamphetamine seizure – multi-agency

In October 2013, a multi-agency task force seized more than 200kg of methamphetamine concealed in truck tyres, and arrested three men in Melbourne. The methamphetamine had an estimated potential street value of up to $200 million. This was one of the largest multi-agency operations involving joint waterfront task forces in Brisbane (Jericho), Sydney (Polaris) and Melbourne (Trident), as well as the Sydney-based Joint Organised Crime Group and the Melbourne-based Joint Organised Crime Taskforce.

AUSTRAC intelligence was important in confirming intelligence related to the importation through international funds payments between entities and companies involved in the operation. The AUSTRAC information is further being used by the AFP to assist international law enforcement agencies to identify the potential source/supplier of the consignment. AUSTRAC information will be used by the AFP Criminal Asset Confiscation Taskforce to assist asset forfeiture actions.

Identifying fraud victims – Western Australian Police

Project Sunbird is a Western Australian (WA) Police and WA Department of Commerce project aimed at identifying and targeting WA-based entities who are likely victims of advance fee fraud. The project relies predominantly on AUSTRAC information to identify potential victims. WA Police analysts refine and analyse AUSTRAC information to identify individuals recorded as sending significant funds overseas, which may also indicate that the individual is a potential victim of fraud.

As part of this analysis, a WA individual was identified as having sent AUD1,175,543 to a number of overseas beneficiaries in West Africa. The WA Police contacted the man in June 2013 to advise that it was likely he was being defrauded, and recommended the cessation of any further money transfers. The police received a response from the man in September 2013, resulting in follow-up investigations that revealed a total loss of approximately AUD2 million to an online investment 'money wash' fraud. AUSTRAC and WA Police continue to work together to identify potential victims to assist in preventing further payments to scammers.

Other investigations that referred extensively to AUSTRAC financial intelligence

Between 2012 and 2013, partner agencies referred to AUSTRAC reporting entities that were suspected of being linked to, or complicit in, the financing of people smuggling. In support of partner agency investigations, AUSTRAC conducted on-site assessments of reporting entities' compliance with the AML/CTF Act. Particular focus was placed on KYC obligations and compliant transaction reporting.

AUSTRAC supported AFP investigations that led to the arrest of people smugglers in Australia in March 2012, June 2012, January 2013 and August 2013. In March 2012, an AFP investigation into people smuggling led to various search warrants being executed in Sydney and Melbourne, resulting in four persons being charged with people smuggling under the *Migration Act 1958* (Migration Act). AUSTRAC information assisted with gaining search warrants and was also disseminated via law enforcement channels to Thailand and Malaysia, resulting in the arrest of one person in Thailand in relation to creating false documents.

In June 2012, AUSTRAC information assisted AFP operations against a remitter with operations in Auburn, NSW and Dandenong, Victoria, where search warrants were executed.

On 5 January 2013, the AFP arrested an individual for suspected involvement in people smuggling operations. He was charged with people smuggling offences under the Migration Act, money laundering offences under the Criminal Code, and for producing a false document to a reporting entity contrary to the AML/CTF Act. The individual was initially identified through AUSTRAC information, which revealed financial transactions to a suspected Indonesia-based people smuggler during 2010 and 2011. AUSTRAC information assisted AFP enquiries into aliases and other details used by this individual.

The AUSTRAC database continues to assist AFP people smuggling operations and investigations. In August 2013, AUSTRAC data was used during an AFP period of targeted action related to various AFP investigations into people smuggling and resulted in the arrest of four persons for their alleged role in people smuggling offences. AUSTRAC disseminated assessments and provided information to the AFP, which assisted with lines of inquiry and gaining search warrants.

In response to a March 2014 questionnaire conducted by AUSTRAC, the ACC responded as follows:

> AUSTRAC information plays an important role in all criminal investigations undertaken by the ACC where criminal individuals acquire or deal with large quantities of money, whether this is the proceeds or instruments of crime. AUSTRAC information is one tool in the ACC's investigative and intelligence generation arsenal. It enhances, and is enhanced by, information sourced via a wide range of traditional and coercive intelligence collection methods.
>
> The identification and tracking of anomalous money movements, through the use of AUSTRAC information, is valuable to the detection of previously unknown criminal networks and activities. It is also valuable as a means of identifying criminal associates, both onshore and offshore. The ACC utilises AUSTRAC information in conjunction with numerous other sources of information, including Taxation and Centrelink data, criminal intelligence holdings, communication interception material and covert human source material, to develop robust operational intelligence to inform intervention and disruption outcomes. This intelligence often informs broader strategic intelligence products that aim to inform prevention and policy outcomes.

8. The interaction of Commonwealth, state and territory legislation and law enforcement activity

AUSTRAC plays a key role in the initiation of law enforcement investigations into financial crime through the dissemination of SMRs and detections based on analysis of organic data holdings. AUSTRAC is also able to provide ongoing support to financial crime investigations through engagement with law enforcement agencies at the operational level. AUSTRAC also provides operational support to multi-agency task forces combating financial crime. As previously described, AUSTRAC is a key partner in Taskforce Eligo, as well as the AFP Criminal Assets Confiscation Team through which law enforcement powers are combined with AUSTRAC's intelligence and regulatory functions to fight money laundering and financial crime facilitated by the remittance and financial sectors, and to improve regulatory compliance in these sectors.

AUSTRAC is working closely with partner agencies including the AFP and Australian Customs and Border Protection Service (ACBPS) to identify entities that are linked to, or complicit in, the funding or facilitating of smuggling people to Australia. To combat people smuggling, AUSTRAC provides financial intelligence support to the operational efforts to the AFP, ACBPS and other partner agencies. AUSTRAC supported AFP investigations that led to the arrest of people smugglers in Australia in March 2012, June 2012, January 2013 and August 2013.

AUSTRAC's work supports national priorities to protect national security, apprehend criminals, protect the integrity of Australia's financial markets and maximise revenue collection. AUSTRAC's work is part of a whole-of-government approach that involves collaboration with other intelligence, regulatory and law enforcement agencies and, importantly, with industry and the community. Given the reach and breadth of money laundering activities, engaging with industry is essential for a strong and sustained response. By working with industry, AUSTRAC and partner agencies develop a more complete and detailed picture of the money laundering environment in Australia, including vulnerabilities and emerging threats. Sharing this knowledge enables government and industry to identify and target criminal activities.

Money laundering

As both the Commonwealth and the states/territories have money laundering offences, both Commonwealth and state/territory law enforcement agencies are able to investigate money laundering. In practice, only the Commonwealth or the state/territory would normally investigate a particular instance of money laundering conduct. If both were investigating the conduct, this would normally be part of a joint investigation or task force. An offender would also only be prosecuted for either a Commonwealth or state/territory money laundering offence. The investigative agency (or lead agency in a task force) will normally decide whether Commonwealth or state/territory offences will be pursued.

Money laundering is often an inter-jurisdictional and transnational crime. The Commonwealth, with its broad oversight over Australia's states and territories, is often best placed to provide a coordinated response to the challenges posed by money laundering investigations. Commonwealth law enforcement agencies conduct the majority of money laundering investigations in Australia, particularly investigations into large-scale money laundering that is associated with serious and organised crime and with transnational links.

This reflects the fact that major profit-making predicate offences such as international drug importation and corporate and financial crime offences are Commonwealth offences.

Joint operations, particularly task forces, involving Commonwealth, state and territory agencies are also used where the scale of the money laundering or predicate crime, or the crime risks these pose, warrants a combined response.

All relevant law enforcement agencies, whether Commonwealth, state or territory, are designated agencies under the AML/CTF Act and have access to AUSTRAC information. Relevant requirements are set out in Part 11 of the AML/CTF Act.

9. The extent and effectiveness of relevant international agreements and arrangements

AUSTRAC supports international AML/CTF initiatives by providing technical assistance and training to FIUs in Africa, Asia and the Pacific. AUSTRAC hosts delegations from international FIUs and regulators and other international organisations, agencies and private sector entities, to establish and enhance productive relationships with international counterparts. Visit programs benefit AUSTRAC and its international counterparts by fostering high-level dialogue on strategic AML/CTF issues. AUSTRAC also benefits by increasing its awareness of the AML/CTF frameworks in place in foreign jurisdictions and the operations of other agencies.

AUSTRAC shares AML/CTF compliance-related information, financial transaction information and intelligence with international counterparts. This information strengthens the global effort to combat ML/TF and benefits the operational work of FIUs and law enforcement agencies tracking the international movement of the proceeds of crime. In return, AUSTRAC receives valuable financial intelligence from its international partners to assist in its own detection and analysis of illicit transactions.

Before exchanging information with a foreign FIU or regulator, AUSTRAC negotiates an exchange instrument, typically in the form of an MOU. Each exchange instrument provides a framework and parameters for information exchange with that particular foreign jurisdiction. AUSTRAC's total number of exchange instruments with international counterparts is currently 69 for the exchange of financial intelligence with overseas FIUs, and one for the exchange of regulatory information. AUSTRAC also receives financial transaction information and intelligence from other foreign jurisdictions that do not require an exchange instrument to be in place before AUSTRAC can accept information from them.

AUSTRAC has experienced increased financial intelligence exchange with counterpart FIUs. In 2012-13 AUSTRAC undertook 245 financial intelligence exchanges with overseas FIUs, which equates to 124 per cent of planned disseminations. This total comprises both incoming and outgoing exchanges and includes both spontaneous disclosures and responses to requests for information.

International intelligence exchanges, 2009–10 to 2012–13

	2009–10	**2010–11**	**2011–12**	**2012–13**
Requests to foreign FIUs	108	37	49	58*
Requests from foreign FIUs	80	81	97	88**
Outgoing spontaneous exchanges	23	24	39	36
Incoming spontaneous exchanges	48	59	47	63
Totals	**259**	**201**	**232**	**245**

* AUSTRAC also made two requests to foreign FIUs with which it did not have an MOU.

** AUSTRAC also received 22 requests from foreign FIUs with which it did not have an MOU.

In addition to intelligence exchanges, in 2012-13 AUSTRAC received and responded to a number of requests in relation to general AML/CTF information from both MOU and non-MOU international counterparts. These requests for information are varied and can relate to topics such as AUSTRAC's AML/CTF regulatory and supervisory activities, AUSTRAC's governance framework, identified typologies, and requests from foreign counterparts to enter into MOU arrangements, primarily for sharing financial intelligence.

During 2012–13 AUSTRAC conducted eight international technical assistance and training programs in four regions. AUSTRAC delivered regional workshops and training programs and conducted in-country visits and mentoring to international counterparts. The programs aim to strengthen institutional capacity, improve compliance with international standards and encourage economic stability and security, thereby contributing to overall international AML/CTF efforts.

AUSTRAC also works with other Australian Government departments and agencies to ensure Australia's international AML/CTF activities align with both domestic priorities and international standards. AUSTRAC regularly liaises with partner agencies to determine priority jurisdictions for the establishment of exchange instruments and with DFAT on foreign policy matters.

Australia is a leading member of a number of international organisations committed to the development and maintenance of AML/CTF standards. AUSTRAC leads and participates in a series of Australian delegations to meetings of international AML/CTF bodies including FATF, the Egmont Group of FIUs and the Asia/Pacific Group (APG) on Money Laundering.

Financial Action Task Force

Australia is a founding member of, and derives significant benefit from its ongoing role in, the Financial Action Task Force (FATF). There are increasing synergies in strategic priorities of FATF to support the outcomes of the G7, G20, OECD, International Monetary Fund and World Bank. Australia consistently provides input in relation to the policy direction of the international community to combat money laundering and the financing of terrorism and proliferation. Equally, Australia plays an important role in reviewing and supporting regional implementation of the FATF Recommendations. Australia's, and in particular AUSTRAC's, role is further expanded below in relation to the APG, a FATF-style regional body of which Australia is a permanent co-chair.

One of the core outcomes of FATF meetings is the development of guidance and best practice to support the private sector in implementing the FATF Recommendations. Of equal benefit is the engagement with the private sector in relation to trends and shifts in global financial operations. Learnings from these meetings carry through to the significant work of FATF to produce information in relation to ML/TF trends and typologies. Australia provides law enforcement and intelligence information to support the development of annual typologies reports and upon completion, alerts Australian authorities and business to their availability.

Asia/Pacific Group

Australia is a founding member of APG, established in 1997, which currently consists of 41 members and a number of international and regional observers. Australia has played a prominent role in the APG since its inception – a reflection of the importance Australia places on the regional response to global AML/CTF efforts and implementation of the FATF Recommendations. Australia hosts the APG Secretariat in Sydney and is a permanent co-chair of APG (via the AFP). AUSTRAC leads the Australian delegation to APG and currently holds the position of co-chair for the Mutual Evaluation Working Group.

APG, in conjunction with FATF and the other FATF-style regional bodies, constitute an affiliated global network to combat ML/TF. In 2006, APG became an associate member of FATF, which gives it direct access to the policy-making and standard-setting processes of FATF.

APG's functions are to:

- assess compliance by APG members with the FATF standards through a robust mutual evaluation program
- coordinate regional technical assistance and training to improve compliance by APG members with the global AML/CTF standards
- participate in, and cooperate with, the international AML/CTF network – primarily with FATF and other regional AML groups
- conduct research and analysis into ML/TF trends and methods to better inform APG members of systemic and other associated risks and vulnerabilities
- contribute to global policy development of AML/CTF standards as an associate member of FATF.

Egmont Group

AUSTRAC is a founding member of the Egmont Group of FIUs which was established in 1995. The Egmont Group currently consists of 139 members. It provides a global network for enhancing cooperation among FIUs especially in the areas of information exchange, training and sharing knowledge and expertise, and in fostering the implementation of domestic AML/CTF programs. It also sets international standards that must be met by FIUs to gain membership.

AUSTRAC has had significant engagement with the Egmont Group since its inception and currently represents the Oceania Group of FIUs in the Egmont Committee, the organisation's executive body. Australia provides ongoing input into the Egmont Group's policy directions, strategic planning and FIU operational issues. This includes the development process relating to potential changes to standards, principles and processes for FIUs. Australia played a key role in the recent review of Egmont's governing documents stemming from the review of the FATF standards. AUSTRAC has also sponsored a number of countries for Egmont membership.

The Egmont Group works closely and in partnership with FATF and FATF-style regional bodies. Egmont FIUs meet in the margins of the FATF meetings to discuss common and interrelated issues. It is now a FATF requirement (Recommendation 29) that FIUs should apply for membership of the Egmont Group.

Other international involvement

AUSTRAC shares AML/CTF compliance-related information, financial transaction information and intelligence with its international counterparts. This information strengthens the global effort to combat ML/TF and benefits the operational work of FIUs and law enforcement agencies tracking the international movement of the proceeds of crime. In return, AUSTRAC receives valuable financial intelligence from its international partners to assist in its own detection and analysis of illicit transactions.

AUSTRAC regularly liaises with its partner agencies to determine priority jurisdictions for the establishment of exchange instruments and with DFAT on foreign policy matters. AUSTRAC also consults and collaborates with the Attorney-General's Department, AFP and DFAT to ensure technical assistance and training programs reflect broader Australian Government priorities. AUSTRAC makes regular exchanges with regional partners in South-East Asia as well as with the 'Five Eyes' countries.

Over the past 12 months, AUSTRAC has had ongoing discussions with its US counterparts, the Financial Crimes Enforcement Network (FinCEN) and the US Treasury Office of Foreign Assets Control (OFAC) about their interest in Australia-based remitters that may be enabling the violation of US sanctions regarding Iran. AUSTRAC, FinCEN and OFAC have exchanged information at both an operational and strategic level to identify suspicious transactions and activity of interest linked to Australia-based remitters.

In November 2013, AUSTRAC attended the first International Supervisors Forum in Ottawa. The forum is made up of AML/CTF regulators from the USA, UK, Canada, New Zealand and Australia and is designed to provide a venue to share information, operational practices, and to develop common performance indicators with a goal to establishing best practices and harmonising our collective processes whenever possible.

10. The need for any legislative or administrative reform

The review of the AML/CTF Act, Rules and regulations provides the Government with an opportunity to comprehensively examine the operation of Australia's AML/CTF regime and in particular, to consider comment and feedback from stakeholders, including regulated businesses and government agencies, concerning their engagement with the regime and how it may be strengthened to improve its efficiency and effectiveness. The review will also consider the recommendations from the 2014 mutual evaluation of Australia's AML/CTF regime by FATF.

The Attorney-General's Department, in collaboration with AUSTRAC, released an issues paper, terms of reference and guiding principles available on the Attorney-General's Department website: <www.ag.gov.au/Consultations/Pages/StatReviewAntiMoneyLaunderingCounterTerrorismFinActCth2006.aspx>.

The issues paper, released on 4 December 2013, is the first engagement with stakeholders and invites submissions on a range of key issues concerning the framework and operation of the AML/CTF regime. The review aims to identify opportunities to improve the effectiveness and efficiency of the AML/CTF framework in compliance with international standards on combating ML/TF. The issues paper uses guiding questions to facilitate stakeholder engagement and consideration of the following key issues:

- the objects of the AML/CTF Act
- the risk-based approach and better regulation
- regime scope including designated non-financial businesses and professions; that is, lawyers, accountants, real estate agents, trust and company service providers and dealers in precious metals and stones, in accordance with the international standards
- harnessing technology to improve regulatory effectiveness
- industry supervision and monitoring
- enforcement
- reporting obligations
- the efficiency and effectiveness of secrecy and access provisions concerning the use and application of AUSTRAC financial intelligence information
- privacy and record keeping
- international cooperation.

Closing

In summary, AUSTRAC, Australia's FIU and AML/CTF regulator, combats the threat of ML/TF through:

- gathering and sharing financial intelligence to identify vulnerabilities and understand current and emerging money laundering methods
- collaborating to investigate and prevent money laundering activities
- developing and enforcing AML/CTF regulation to identify, mitigate and manage risks
- engaging with industry and the community to create an environment more hostile to money laundering.

AUSTRAC provides a risk-based approach to the supervision of reporting entities with higher amounts of regulatory effort directed towards entities that provide services and products identified as having a higher exposure and vulnerability to ML/TF risk.

AUSTRAC's regulatory activities are designed to assist reporting entities to strengthen their AML/CTF systems and controls to protect against their services being used for criminal purposes. AUSTRAC also seeks to improve the quantity and quality of information received to assist law enforcement and other partner agencies in the detection and prevention of ML/TF and other major crimes.

AUSTRAC is concerned to reduce the regulatory burden for the entities that it regulates, wherever possible. To assist small businesses captured by the AML/CTF Act, AUSTRAC has developed tailored guidance and education to assist entities to comply.

AUSTRAC collaborates with various Commonwealth, state and territory agencies to support investigations and intelligence operations to provide government agencies with additional capabilities to prevent and detect organised crime in Australia.

AUSTRAC has assisted its partners uncover a range of serious offences and is actively involved in major national operations and task forces including:

- Project Wickenby
- National Criminal Intelligence Fusion Capability led by the ACC, incorporating the Financial Intelligence Assessment Team
- AFP-led Criminal Asset Confiscation Taskforce and Terrorism Financing Investigation Unit
- Taskforce Galilee (detecting and combating serious and organised investment fraud)
- Taskforce Attero (ACC-led taskforce on Rebels outlaw motorcycle gang members)
- Taskforce Eligo (ACC/AFP/AUSTRAC coordinating national response to high-risk remitters).

AUSTRAC will continue to be actively involved in major national operations and task forces, including those focused on money laundering, criminal assets, tax evasion and people smuggling, and provide financial intelligence to support significant law enforcement operations.

Other types of investigations where AUSTRAC information is currently assisting include significant drug trafficking, transnational organised crime, money laundering, proceeds of crime, illegal firearms, and child sex offences and pornography.

In 2012-13 AUSTRAC information and intelligence directly contributed to: 1,428 ATO cases resulting in $572 million in additional tax assessments raised; 298 cases and $4.4 million annualised savings for Centrelink (Department of Human Services); and 305 major investigations conducted by AUSTRAC's law enforcement, human services and revenue partner agencies.

Growing profiling capability flowing from AUSTRAC's new Money Laundering Criminal Targeting section is also producing operational outcomes for AUSTRAC's partners, including the detection of 'real time' suspicious financial activities.

In 2012-13, AUSTRAC disseminated:

- 56,986 SMRs and SUSTRs to partner agencies to assist them in their investigations
- 1,341 detailed financial intelligence reports
- 248 exchanges of financial intelligence with international FIUs.

AUSTRAC also shares financial intelligence on sanction-related matters with DFAT and through them, the United Nations Security Council's relevant subgroups (for example, sanctions on Iran).

AUSTRAC released its seventh typologies and case studies report in 2013. The report details how the efforts of law enforcement agencies, combined with AUSTRAC's analysis of transaction reports provided by reporting entities, led to asset seizures and the arrest and conviction of criminals in Australia and overseas.

Forty-one Australian Government and state agencies spanning law enforcement, border and national security, revenue and social justice agencies can access AUSTRAC information and AUSTRAC financial intelligence products under the AML/CTF Act.