Australian Government
Attorney-General's Department

Attorney-General's Department Submission

Parliamentary Joint Committee on Law Enforcement Inquiry into Financial Related Crime

May 2014

Contents

Scope of submission

This submission is made by the Attorney-General's Department (AGD) in response to the terms of reference for the inquiry into financial-related crime adopted by the Parliamentary Joint Committee on Law Enforcement (PJCLE) on 5 March 2014.

Financial crime represents a broad range of activity including money laundering, tax crime, foreign bribery, corporate crime, fraud, scams and corruption. In order to address the request of the PJCLE to examine the effectiveness of current Commonwealth law enforcement legislation and administrative arrangements that target serious financial related crime, this submission focusses on Australia's anti-money laundering regime. This regime sits at the heart of detecting a range of financial and other serious crimes and provides the crucial financial intelligence to allow investigators and prosecutors to "follow the money".

The submission also addresses issues of identity security, given the role of identity crime as an enabler of financial crime and AGD's responsibilities as the lead agency for the National Identity Security Strategy (NISS).

Terrorism financing is not referenced directly in the report; however, the anti-money laundering measures discussed are internationally recognised as being measures which are appropriate for detecting and deterring terrorism financing.

Introduction

Organised crime is big business. A recent United Nations Office of Drugs and Crime report estimates the annual income of organised crime in Asia and the Pacific at nearly 90 billion USD[1]. Legitimising the proceeds of crime and the instruments of crime (the means by which crime is committed) is crucial for organised crime groups, enabling criminals to purchase assets and invest in further criminal enterprises. The Australian Crime Commission (ACC) has stated that 'the capacity to legitimise the proceeds of crime is a major component of virtually all criminal activity and money laundering will be a continuing feature of serious and organised crime.'[2] Money laundering poses an ongoing risk to the Australian community.

---

[1] *Transnational Organized Crime in East Asia and the Pacific: A Threat Assessment*, UNODC, 2013, p1

[2] ACC submission to the Parliamentary Joint Committee on the Australian Crime Commission Inquiry into the Future Impact of Serious and Organised Crime on Australian Society, 2007, p8.

Money laundering is not a victimless, 'white collar' crime. It is an essential component of the ability of criminals to profit from highly damaging crimes like fraud, drugs and firearms trafficking, identity theft and cyber-crime. Money laundering has the potential to threaten the integrity of our financial system, funds further criminal activity including terrorism, and ultimately impacts on community safety and wellbeing.

Effective anti-money laundering and counter-terrorism financing (AML/CTF) laws are critical to the ongoing fight against organised crime and terrorism. The international community and domestic governments have a critical role to play in establishing standards, systems and processes to monitor the flow of illicit funds and create a global environment that is hostile to money laundering and terrorist financing.

Identity crime is now one of the most prevalent crime types in Australia. It is also a key enabler of financial crime as well as serious and organised crime, including money laundering. The NISS provides a framework for cooperation between Australian governments and businesses to combat identity crime and promote identity security as an enabler of the digital economy.

What is money laundering

Money laundering is the name given to the process by which illegally obtained funds are given the appearance of having been legitimately obtained.

Every year, huge amounts of funds are generated from illegal activities (mostly in the form of cash). The criminals who generate the funds need to bring them into the legitimate financial system without raising suspicion. The conversion of cash into other forms makes it more useable. It also distances the criminal activities from the illicit funds.

There are several reasons why criminals launder money. These include:

- **Hiding wealth** – criminals can hide illegally accumulated wealth to avoid its seizure by authorities.
- **Avoiding prosecution** – criminals can avoid prosecution by distancing themselves from the illegal funds.
- **Evading taxes** – criminals can evade taxes that would be imposed on earnings from the funds.

- **Increasing profits** – criminals can increase profits by reinvesting the illegal funds in businesses or further criminal activity.

The money laundering process is typically segmented into three stages:

1) **Placement:** At this stage, illegal funds or assets are brought into the financial system. This 'placement' makes the funds more liquid. For example, if cash is converted into a bank deposit, it becomes easier to transfer and manipulate. Money launderers place illegal funds using a variety of techniques, which include depositing cash into bank accounts and using cash to purchase assets.
2) **Layering:** To conceal the illegal origin of the placed funds and thereby make them more useful, the funds must be moved, dispersed and disguised. The process of distancing the placed funds from their illegal origins is known as 'layering'. At this stage money launderers use many different techniques. These include using multiple banks and accounts, having professionals act as intermediaries, and transacting through corporations and trusts. Funds may be shuttled through a web of many accounts, companies and countries in order to disguise their origins.
3) **Integration:** Once the funds are layered and distanced from their origins, they are made available to criminals to use and control as apparently legitimate funds. This final stage in the money laundering process is called 'integration'. The laundered funds are made available for activities such as investment in further criminal activity or legitimate businesses, or the purchase of high-value assets and luxury goods. At this stage the illegal money has achieved the appearance of legitimacy.

Regulatory responses

International

The Financial Action Task Force

In 1989 the Group of Seven (G7) established the **Financial Action Task Force (FATF)** to examine and develop measures to combat money laundering. Following the September 11 terrorist attacks, the FATF expanded its mandate to incorporate efforts to combat terrorist financing.

The main objectives of the FATF are to set global standards and to promote effective implementation of legal, regulatory and operational measures to fight money laundering, terrorist financing and other related threats to the integrity of the international financial system.

In order to achieve these objectives, the FATF has developed a set of recommendations (the *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation* (the FATF standards)) that are recognised as the international standard for combating money laundering and the financing of terrorism and proliferation of weapons of mass destruction. The FATF standards are revised from time to time to ensure that the measures remain effective and current. The most recent revision was finalised in February 2012.

The FATF standards set out the essential measures that jurisdictions should have in place to:

- identify the money laundering/terrorism financing (ML/TF) risks and develop policies to manage those risks
- coordinate domestic efforts
- apply preventative measures for the financial sector and other designated non-financial financial businesses and professions (DNFBPs)
- establish powers and responsibilities for investigative, law enforcement and supervisory authorities
- enhance the transparency and availability of beneficial ownership information, and
- facilitate international cooperation.

To assess compliance with the FATF standards, FATF members conduct periodic 'mutual evaluations' of other members. The current round of mutual evaluations commenced in October 2013, and represents the first round of evaluations under the revised FATF standards. It will be the first time that evaluations will assess not only a jurisdiction's technical compliance with the standards, but the overall effectiveness of a jurisdiction's AML/CTF regime.

FATF membership is currently limited to 36 members[3] representing most of the major financial centres in the world. In order to achieve global reach of the standards, the

[3] Argentina, Australia, Austria, Belgium, Brazil, Canada, China, Denmark, European Commission, Finland, France, Germany, Greece, Gulf Co-operation Council, Hong Kong (China), Iceland, India, Ireland, Italy, Japan,

FATF has developed a global network of eight 'FATF style regional bodies' (FSRBs)[4], which operate as separate entities, but promote and assess compliance with the FATF standards.

The FSRB model is the key way in which FATF can promote global compliance but maintain membership numbers which make policy development possible. Over 180 jurisdictions have committed to the FATF standards through membership of the FATF or an FSRB.

The FATF standards play an important role in ensuring that an internationally coordinated approach prevents criminals from engaging in jurisdictional arbitrage - exploiting vulnerabilities arising from differences between the laws of different jurisdictions.

The work of the FATF is endorsed and advanced by a wide range of international agencies, including the United Nations Office on Drugs and Crime, the International Monetary Fund and the World Bank. FATF's work has been encouraged by the G8 and the G20, most recently in the context of initiatives to address the global financial crisis.

The FATF operates under a finite life-span, requiring a specific decision of its members to continue. The current mandate of the FATF was adopted by Finance Ministers in 2012 and is due for reconsideration in 2020.

Australia's FATF engagement

Australia has been heavily involved in establishing and promoting the international framework for combating money laundering. Australia is a founding member of the FATF. Attorney-General's Department Secretary, Mr Roger Wilkins AO, is the current Vice-President of FATF and will take over the Presidency in July 2014 for a one year term.

Republic of Korea, Luxembourg, Mexico, Netherlands, Kingdom of, New Zealand, Norway, Portugal, Russian Federation, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States.

[4] Asia/Pacific Group on Money Laundering (APG), Caribbean Financial Action Task Force (CFATF), Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), Eurasian Group (EAG), Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), Financial Action Task Force on Money Laundering in South America (GAFISUD), Inter Governmental Action Group against Money Laundering in West Africa (GIABA) Middle East and North Africa Financial Action Task Force (MENAFATF).

Australia is also a member and permanent Co-Chair of the Asia-Pacific Group (APG) on Money Laundering. The APG is the Asia-Pacific region's FSRB and is housed by the Australian Federal Police (AFP) in Sydney. AUSTRAC leads Australia's delegation at all APG meetings.

Domestic

Financial Transaction Reports Act 1988

Australian anti-money laundering legislation developed as a direct response to two Royal Commissions in the 1980s[5] which exposed the links between money laundering, major tax evasion, fraud and organised crime. The Royal Commissions identified the need for legislative strategies to address these issues.

While initially focusing largely on suspect transactions and large cash transactions, Australia's anti-money laundering legislation was later extended to include the reporting and monitoring of certain international transactions.

The *Financial Transaction Reports Act 1988* (FTR Act) imposed reporting controls on the financial, bullion and gambling sectors to deter financially motivated criminals and to provide financial intelligence to revenue and law enforcement agencies. It applied to a wide range of businesses within the financial services industry, the insurance industry, the travel industry and the gambling industry.

The FTR Act imposed the following main obligations:

- 'cash dealers' were required to report suspect transactions
- certain domestic currency transactions, and currency transfers to and from Australia, of $10,000 or more had to be reported
- it required reporting of international funds transfer instructions
- it created an offence of opening or operating a bank account or similar account with a cash dealer in a false name, and
- cash dealers were required to verify the identities of account holders or signatories, and to block withdrawals by unverified signatories to accounts exceeding certain credit balance or deposit limits.

---

[5] Costigan Royal Commission into the Federated Ship Painters and Dockers Union of Australia (1980-84); Stewart Royal Commission of Inquiry into Drug Trafficking (1980-1983)

The FTR Act continues in force and operates parallel to the AML/CTF Act. The FTR Act applies to 'cash dealers' who are not 'reporting entities' under the AML/CTF Act.

Anti-Money Laundering and Counter-Terrorism Financing Act 2006

The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (the AML/CTF Act) established a robust regulatory regime to detect and deter money laundering and terrorism financing. The AML/CTF Act was a major step in bringing Australia into line with the FATF standards and was developed in close consultation with industry and other interest groups.

An entity becomes a 'reporting entity' under the AML/CTF Act when it provides a 'designated service'. In broad terms the AML/CTF Act designates the services provided by financial institutions, gambling service providers, bullion dealers and remittance dealers. The AML/CTF Act sets out five key obligations for reporting entities:

1) **Enrolment:** all regulated entities need to enroll with AUSTRAC and provide enrolment details prescribed in the AML/CTF Rules.
2) **Conducting customer due diligence**: Regulated entities must verify a customer's identity before providing the customer with a designated service. Regulated entities must carry out ongoing due diligence on customers, and enhanced customer due diligence on high-risk customers.
3) **Reporting:** Reporting entities must report suspicious matters, certain transactions above a threshold and international funds transfer instructions.
4) **Developing and maintaining an AML/CTF Program**: Reporting entities must have and comply with AML/CTF programs which are designed to identify, mitigate and manage the money laundering or terrorist financing risks a reporting entity may face.
5) **Record keeping:** Reporting entities must make and retain certain records (and other documents given to them by customers) for seven years.

The AML/CTF Act sets out general principles and obligations. Details of how these obligations are to be carried out are set out in the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)* (the AML/CTF Rules).

The AML/CTF Act and the AML/CTF Rules establish a risk-based approach. Regulated businesses are required to identify the risk of money laundering associated with the

provision of certain services, and implement appropriate measures to address those risks.

The AML/CTF Act, AML/CTF Rules and FTR Act (collectively the AML/CTF regime) serve a twofold purpose:

1) "Target hardening" - deterring money launderers by requiring businesses to undertake enhanced scrutiny of financial and business transactions, thereby reducing opportunities for laundering to occur, and
2) Financial intelligence - providing law enforcement, national security, revenue, regulatory and social justice agencies, as well as state and territory law enforcement revenue agencies and international counterparts with the financial intelligence they require to detect, investigate and prosecute criminal activity.

Criminal Code Act 1995 (Cth) - Money laundering offence.

Money laundering is criminalised under Division 400 of the *Criminal Code Act 1995* (Cth) (the Criminal Code), and applies to all serious offences. The money laundering offences are broad and apply to both proceeds (ie, money or property that is derived or realised, directly or indirectly, from the commission of an indictable offence – an offence with a jail term of more than 12 months) and instruments of crime (ie, money or property used in or to facilitate the commission of an indictable offence).

The definitions of 'proceeds of crime' and 'property' as set out under s 400.1 of the Criminal Code are expansive, extending to any money or other property that is wholly or partly derived or realised, directly or indirectly, by any person from the commission of an offence that may be dealt with as an indictable offence. Property is defined as real or personal property of every description, whether situated in Australia or elsewhere and whether tangible or intangible, and including an interest in any such real or personal property.

The offences are structured in increments, with six categories of offences broken down by the amount of money laundered: any value, $1,000, $10,000, $50,000, $100,000 and over $1,000,000. Within each category there are 3 offences based on mental state – intent (or actual knowledge), recklessness and negligence.

Penalties are determined through a combination of the amount laundered and the mental state of the offender. Penalties range from a maximum of one year to a maximum of 25 years imprisonment, and the court can also impose a fine.

There are also two offences dealing with property 'reasonably suspected' of being proceeds of crime which are separated by the amount laundered ($100,000 or more and less than $100,000). These offences have penalties of 3 years and 2 years respectively, which reflects the lower standard of proof.

The Criminal Code also makes clear that the prosecution does not need to establish that an offence has been committed in relation to the money or property in order for those assets to be considered proceeds of crime. However, the prosecution must still prove beyond a reasonable doubt that the assets are either the proceeds of a crime, or are intended to become, or are at risk of becoming, an instrument of crime.

Identity-related financial crime

A significant proportion of financial crime, including money laundering, credit card and other frauds, is enabled by the fraudulent use of identity related information. In the United Kingdom, it has been recently estimated that 60% of all fraud involves some form of identity crime, whether this be the use of stolen or fictitious identity information.[6] A recent project to measure the nature and extent of identity crime in Australia estimates the annual economic impact of identity crime (including financial related identity crime) was at least $1.6 billion.

While there are no universally agreed definitions of identity crime and identity fraud, the following definitions were developed as part of the 2007 Intergovernmental Agreement to a National Identity Security Strategy[7]:

- **identity crime** is a generic term to describe activities/offences in which a perpetrator uses a fabricated identity, a manipulated identity, or a stolen/assumed identity to facilitate the commission of crime; and

[6] Credit Industry Fraud Avoidance Service (CIFAS), (2014), Fraudscape: Depicting the UK's fraud landscape, United Kingdom, https://www.cifas.org.uk/secure/contentPORT/uploads/documents/CIFAS%20Reports/External-CIFAS-Fraudscape-2014-online.pdf

[7] 2007 Intergovernmental agreement to a National Identity Security Strategy http://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Inter%20Government%20Agreement%20to%20a%20National%20Identity%20Security%20Strategy%20[94.2KB%20PDF].pdf

- **identity fraud** is the gaining of money, goods, services or other benefits or avoiding obligations through the use of a fabricated identity, a manipulated identity, or a stolen/assumed identity.

The legal framework for identity crime is set out in the Criminal Code and corresponding legislation. The Criminal Code (s372) outlines specific identity crime offences such as:

- dealing in identification information
- possession of identification information, and
- possession of equipment used to make identification information, where this is involved in the commission of a Commonwealth indictable offence.

A number of states and territories have also enacted specific identity crime offences in their criminal codes.

There are also a range of other related offences in Commonwealth, state and territory legislation that may apply to activities involved in the commission of identity related crimes. These identity crime-related offences include fraud, forgery, and impersonation.

Commonwealth legislation in other portfolios also contains offences relating to the fraudulent use of evidence of identity documents or identity information. For example, the *Migration Act 1958* (s234) contains offences relating to false documents and false or misleading information regarding non-citizens.

Nature and extent of identity crime in Australia

It is difficult to estimate the true amount of identity related crime in Australia due to a number of factors including the under-reporting of identity crime by victims, and the tendency of law enforcement and other agencies to record identity-related crime using broader categories of fraud or other crime types.

Data from the Australian Payments Clearing Association shows that the total value of credit card fraud has increased from $42 million in 2005-06 to $121 million in 2012-13. A major contributing factor is the rise in card-not-present fraud (where a fraudulent transaction is made using only the credit card details and not the physical card). In 2012-13, card-not-present fraud accounted for around two-thirds ($82 million) of all credit card fraud. This represents an increase in the value of card-not-present fraud of

600 per cent in the last eight years. However, despite these increases, credit card fraud represents only a small proportion of all credit card transactions – only around 0.02 per cent in 2012-13[8].

Surveys by the Australian Institute of Criminology (AIC)[9] and Australian Bureau of Statistics (ABS)[10] indicate that around 4 - 5% of Australians report being a victim of identity crime each year and lose money as a result. The AIC survey indicated that victims reported an out-of-pocket loss of between $1 and $310,000, at an average of $4,101 per incident. However, just over half of respondents (55%) who reported losing money managed to recover or be reimbursed for some of their losses, at an average of $2,481 per incident, while the remaining 45 per cent did not receive any reimbursement or recover any losses. Overall, losses were relatively small, with 50 per cent of victims losing less that $250 and 75 per cent losing less than $1000.

The AIC survey also indicated that the three types of personal information misused most often were:

- credit and debit card information (in 52% of cases)
- name (in 40% of cases), and
- bank account information (in 31% of cases).

Data from the Commonwealth Director of Public Prosecutions (CDPP) and the ABS indicate that each year in Australia there are around 40,000 convictions for fraud offences and 7,000 convictions for identity crimes (such as forgery, identity theft and manufacturing counterfeit credentials). Of the 40,000 fraud offences, AGD has estimated that somewhere between 15,000 and 20,000 are enabled through the use of a stolen, manipulated or fabricated identity.

The findings of a recent report by AGD on a project to measure the nature and extent of identity crime in Australia indicates that identity crime is now one of the most prevalent crime types in Australia. This supports the assessment by the ACC that identity crime is

---

[8] Australian Payments Clearing Association, 2013, http://www.apca.com.au/payment-statistics/fraud-statistics/2013-financial-year

[9] Australian Institute of Criminology (AIC), (2014), *Identity crime and misuse in Australia: Results of the 2013 online survey*, Research and Public Policy Series 128, Canberra: http://aic.gov.au/publications/current%20series/rpp/121-140/rpp128.html

[10] Australian Bureau of Statistics (ABS), (2012), *Personal Fraud, 2010-2011*, ABS Cat. No. 4528.0, Canberra: http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/by%20Subject/4530.0~2012-13~Main%20Features~Victims%20of%20personal%20crime~4

a key enabler of other serious and organised crime, including money laundering. Further work is needed on reporting processes and systems for recording identity crime and other crime types enabled by identity crime to assess the extent of identity crime as an enabler of financial crime. For example, incidents were revealed where prosecutions for offences such as money laundering (which involved the use of fraudulent identities to facilitate the offence) did not provide any indication that these were identity-related crimes when recorded and reported.

A companion body of work is underway to develop strategies for improving agency data collection and reporting systems for identity crime and other crime types enabled by identity crime.

Australia's identity system and the National Identity Security Strategy

Those seeking to commit identity crime can take advantage of the opportunities presented by Australia's complex system of national 'identity infrastructure'. Around 20 government agencies across Australia manage over 50 million documents and credentials, such as driver licences and passports that are used as evidence of a person's identity. This is in addition to a comparable number of other credentials, such as credit cards, that are issued by organisations in the financial and other industry sectors.

Literally millions of these identity credentials are issued, renewed and revoked each year as people are born, become adults, get married, migrate interstate and internationally and die. Detecting and preventing the use of false or fraudulent identity credentials in such a dynamic system poses significant challenges for the organisations involved.

AGD is coordinating efforts between the Commonwealth and the States and Territories under the National Identity Security Strategy (NISS) to improve the integrity of Australia's identity infrastructure and processes. The strategy was first agreed by the Council of Australian Governments in 2007 and was revised in 2012 to ensure it remained ready to meet the opportunities and challenges presented by the digital economy and the evolving nature of identity crime in Australia.

Document Verification Service

Verification of the identities of people seeking to access high value or high risk services, such as many financial transactions, is a key part of efforts under the NISS to combat identity crime.

A key initiative in this regard is the national Document Verification Service (DVS). The DVS is a secure, online system that provides for automated checks of the accuracy and validity of information on the key government documents commonly presented as evidence of identity. The DVS enables its user organisations to check the information on identity credentials against the records of the issuing agency. These checks are conducted in real time to inform decisions that rely upon the confirmation of a person's identity. It provides a key tool for organisations that are seeking to prevent the enrolment or registration of customers, clients and even staff who may be using fraudulent identities.

The DVS has been available for use by government agencies since 2009. In early 2014 the DVS became available for use by certain private sector organisations with a requirement or authority to verify a person's identity under Commonwealth legislation. This includes financial sector and other organisations covered by the AML/CTF Act.

There has been strong private sector interest in the DVS, particularly from providers of financial services. As at 29 April 2014, 160 private sector applications had been approved and the service had 23 active private sector users. On 5 May 2014, the Attorney-General, Senator the Hon George Brandis QC, launched the DVS commercial service.

The DVS helps businesses protect themselves against identity crime, and will make it easier for businesses to comply with their regulatory obligations for verifying customers' identities. Privacy considerations are at the forefront of the DVS design. The system is not a database; it does not store any personal information. All DVS checks must be done with the informed consent of the person involved.

AGD is working with the States and Territories, as joint owners of the DVS, to further expand the range of private sector organisations that are able to access the service.

National Identity Proofing Guidelines

The verification of information on identity documents is only one part of processes to verify a person's identity. Equally important is the ability to establish a 'social footprint' that shows the operation of an identity in the community over time. So too is the ability to link a physical person to their claimed identity, something traditionally done through photo identity documents.

Under the NISS, AGD is also developing new national guidelines to update guidance for government agencies on this threefold approach to verifying a person's identity (biographic; social footprint; biometrics). These new guidelines adopt a risk-based approach, aligned with international standards, in which agencies can choose between different sets of identity proofing requirements. This provides a more robust, yet flexible approach to the traditional '100 point' check.

The guidelines are designed for government agencies that issue documents or credentials that are most commonly relied upon as evidence of a person's identity. However they will also be made available to private sector organisations which may choose to adopt elements of the guidelines as a 'better-practice' guide to help meet any regulatory obligations or business needs to verify a person's identity.

Any implementation of the guidelines by private sector organisations will need to be done in accordance with the *Privacy Act 1988*.

Biometrics

Traditional approaches to verifying a person's identity for higher-risk or value transactions have relied upon the use of a face-to-face or in-person interaction. As a greater number of these transactions are conducted online, new approaches to identity verification will be developed that make use of the opportunities presented by technologies such as biometrics while also maintaining appropriate privacy and security safeguards.

Biometrics (or biometric information) refers to any measurable biological or behavioural characteristics of an individual that can be used to identify or verify the identity of the individual. The most commonly used biometrics include fingerprints, facial images and voice prints.

Biometric systems are the technologies that automate the identification of individuals using one or more types of biometric information. These systems are currently used by a range of government agencies in support of their national security, law enforcement, border management and service delivery functions. It is now common practice for people to provide biometric data to travel internationally, to apply for a driver licence or other forms of photo identification. The use of biometric technology is also becoming more prevalent amongst the private sector, for example fingerprint scanners in smartphones and other electronic devices. Over time, this may see the use of biometric systems become more accepted in the community.

By providing greater levels of assurance in a person's identity, biometric systems can help to protect individuals, businesses and government agencies against identity crime. At the same time, biometric systems can offer greater convenience and efficiencies in service delivery, particularly in online services, by reducing the reliance on face-to-face transactions to verify a person's identity.

The utility of biometric systems can be enhanced through the ability to match or verify biometric data within and between the holdings of government agencies, where this is permitted under the *Privacy Act 1988*. With this in mind, a National Biometric Interoperability Framework has been developed under the auspices of the National Identity Security Strategy. AGD is working with relevant Commonwealth, State and Territory agencies to explore opportunities to enhance the interoperability of their biometric systems.

This work includes pilot projects for sharing biometric information between relevant agencies, to aid in the detection of identity crime and/or to improve the efficiency of service delivery, where this is required or authorised under relevant legislation. AGD has also commissioned a feasibility study into technical options to promote interoperability between facial biometric systems operated by Commonwealth, state and territory agencies.

In the future, this work could potentially be expanded to include private sector organisations, including those in the financial sector. The use of biometrics by banks, for example, could help improve the prevention and detection of identity related financial crime.

Any current and future work to promote biometric interoperability needs to be conducted with robust privacy and other safeguards, in accordance with the *Privacy Act 1988* and other relevant legislation. This includes the new Australian Privacy Principles under which biometrics are classified as sensitive information. This requires a person's informed consent to the collection of their biometric information, and any use or disclosure of this information must be related to the purpose for which it was originally collected, unless certain law enforcement or other exceptions apply.

Policy and coordination

The role of the Attorney-General's Department

Under the Administrative Arrangement Orders, AGD is responsible for the AML/CTF Act and the FTR Act. This places AGD as the lead agency for developing AML/CTF policy. In this context, AGD has two main roles:

1) AGD traditionally leads Australia's engagement with the FATF, ensuring that the international standards, best practice and guidance issued by the FATF are appropriate.
2) AGD coordinates policy development for Australia's domestic AML/CTF regime.

AUSTRAC collects the financial data provided by reporting entities and analyses it to produce financial intelligence. That financial intelligence is used by law enforcement, national security, revenue, regulatory and social justice agencies, as well as state and territory law enforcement revenue agencies and international counterparts.

In order to effectively coordinate policy development, AGD convenes and chairs the Anti-Money Laundering Interdepartmental Committee (AML IDC), which addresses both domestic and international AML/CTF policy and operational issues. Established in 2010 it meets three times a year to coordinate AML/CTF priorities across agencies. The IDC comprises the major Commonwealth agencies with central AML/CTF policy, operational and prosecutorial roles – AGD, AUSTRAC, ACC, AFP, ACBPS, ATO, CDPP, DFAT and Treasury. PM&C and other agencies attend as required.

The IDC strengthens links between policy, legislative development, and operational activity, as well as ensuring that legislation and domestic or foreign policy with AML/CTF

implications is considered by relevant agencies. It provides a feedback loop for operational and intelligence findings to be considered at a high level to inform policy and legislative change.

AGD works very closely with AUSTRAC on AML/CTF issues to ensure coordination between policy and operational issues on financial intelligence and regulatory matters. AGD also participates in the regular stakeholder forums convened by AUSTRAC.

Policy Development

Australia is recognised internationally as having a robust AML/CTF regime. The AML/CTF regime provides a comprehensive legal framework designed to ensure that Australia's financial system is hostile to money laundering, and helps to protect Australia, its people and financial institutions against abuse from criminal activity.

However, by its nature money laundering is an evolving crime. Criminals continue to search for gaps in the existing AML/CTF framework, and seek alternative ways to process and disguise the funds associated with their criminal activities. The AML/CTF regime must be subject to ongoing critical evaluation and amendment to ensure that it remains effective.

Review of the AML/CTF regime and FATF mutual evaluation

Section 251 of the AML/CTF Act requires that a review of the AML/CTF Act, Rules and Regulations be initiated within seven years of the Act's commencement.

On 4 December 2013, the Minister for Justice, the Hon Michael Keenan MP, announced a review of Australia's AML/CTF regime. The review will cover a range of issues including: the objects of the AML/CTF Act; the risk-based approach and better regulation; regime scope; harnessing technology to improve regulatory effectiveness; industry supervision and monitoring; enforcement; reporting obligations; secrecy and access; privacy and record keeping; and international cooperation. The Terms of Reference and Issues Paper are available on the AGD website. Submissions closed on 28 March 2014. Submissions are also available on the Department's website.[11]

---

11 http://www.ag.gov.au/Consultations/Pages/StatReviewAntiMoneyLaunderingCounterTerrorismFinActCth2006.aspx

The review will overlap with Australia's fourth round mutual evaluation against the revised FATF standards. As part of the mutual evaluation process Australia will receive an onsite visit by FATF evaluators in July-August 2014. The 2014 mutual evaluation will provide valuable information on compliance with international standards and areas for improvement in effective implementation. It is proposed that this information will be considered as part of the broader AML/CTF regime review. The FATF mutual evaluation process will conclude in February 2015 when the FATF considers the evaluation of Australia.

Emerging issues

Money Laundering Methodologies

As technology changes, so too do money laundering methodologies. Electronic payment systems and new payment methods have become an integral part of the globalised economy. Criminals also exploit these systems for money laundering purposes.

It is now possible to establish systems to remit funds across the globe via the internet which have no geographical nexus with Australia. Internet based payment systems offering services in Australia may have infrastructure physically located in a jurisdiction with lax AML/CTF requirements. This creates policy challenges in terms of capturing those services under Australia's regime, but also significant challenges for downstream regulation and enforcement.

Similarly virtual currencies such as Bitcoin afford users anonymity and make cross-border currency movements very straightforward and largely outside the current AML/CTF regime. As AUSTRAC notes in its submission to the inquiry, digital currencies that are not backed, either directly or indirectly, by precious metal or bullion are not regulated by the AML/CTF Act.[12] Virtual currency is discussed in more detail in AUSTRAC's submission. These qualities make virtual currency attractive to criminal groups and vulnerable to exploitation by money launderers. Although there is limited evidence of large-scale usage of virtual currency by criminal groups, this emerging area will require close attention to ensure an appropriate regulatory and law enforcement response to any exploitation of virtual currency by money launderers.

[12] AUSTRAC submission to PJCLE Inquiry into Financial Crime, 2014, p17

Designated Non-Financial Businesses and Professions

Criminal intelligence has identified that there are a number of vulnerabilities in Australia's AML/CTF regime, particularly regarding sectors that fall outside the scope of the AML/CTF Act. Designated non-financial businesses and professions (DNFBPs), including lawyers, accountants, real estate agents, trust and company service providers and dealers in precious metals and stones, have been identified by FATF as industries particularly vulnerable to abuse for money laundering. AUSTRAC notes that "it is becoming more common for organised crime to engage a range of professionals to provide advice, establish and, in some cases, administer … complex structures which disguise illicit money flows" and that Australian-based and overseas-based crime groups use professionals such as lawyers, accountants, financial advisers and real estate agents to help undertake transactions designed to obscure ownership, conceal proceeds of crime, legitimise illicit funds and avoid regulatory controls and detection efforts.[13] The Australian Crime Commission has made similar findings in relation to the use of professional facilitators and money laundering through the real estate sector.[14]

The review of the AML/CTF Act provides an opportunity to examine whether the Act should now be extended to capture services conducted by DNFBPs. Industry, partner agencies and other interested parties were invited to make submissions to the review. These submissions are receiving consideration.

Information sharing

Australian Governments have acknowledged that sharing intelligence, data and information between jurisdictions and agencies is crucial in the fight against serious and organised crime.

Streamlined and efficient arrangements for sharing intelligence, data and information between the Commonwealth, States and Territories are particularly important in light of developments in both the nature of the organised crime threat and the strategies law enforcement agencies employ to meet that threat.

---

[13] *Money Laundering in Australia*, AUSTRAC, 2011, p28-29 (http://www.austrac.gov.au/files/money_laundering_in_australia_2011.pdf)
[14] See *Commonwealth Summary of Intelligence: Financial Crime Impacting Australia*, Australian Crime Commission, 2014

Over recent years, the Commonwealth, States and Territories have done a range of work to enhance arrangements for intelligence, data and information sharing between jurisdictions. For example, in late 2013 the Government established the National Anti-Gang Squad. The National Anti-Gang Squad brings together officers from the AFP, local law enforcement agencies and the Australian Taxation Office (ATO). By embedding ATO officers within the National Anti-Gang Squad, these officers can provide local law enforcement with greater coordination and access to information held by the ATO, which may not otherwise be readily available.

There is, however, further work to be done to achieve optimal intelligence, data and information sharing between jurisdictions and agencies. The Department will continue to explore opportunities to improve information sharing on serious and organised crime at both a Commonwealth and national level, in consultation with relevant agencies

Identity security

In future, we may see a greater role for financial and other private sector organisations as providers of digital identities or identity verification services; functions that have traditionally been the role of government. Some other countries have begun to embrace this approach. The Canadian Government has established a Cyber Authentication Renewal Initiative in which citizens can choose to use either digital identity credentials provided by banks or a government-issued credential to access online government services. Other countries are pursuing similar joint public-private partnership approaches that would see government agencies as 'consumers' of private sector identity credentials and services, for example the US *National Strategy for Trusted identities in Cyberspace* and the UK's *Identity Assurance Programme*. New Zealand has established its *RealMe* program in which the government is the provider of a digital identity credential that citizens can use to access private sector services.

For the foreseeable future, the digital identities that Australians will use to access higher risk/value transactions online will need to be grounded in the more traditional identity documents produced by government agencies.

Conclusion

Money laundering has severe economic and social consequences. It has the potential to threaten the integrity of our financial system, funds further criminal activity including terrorism, and ultimately impacts on community safety and wellbeing. Laundering

money to make illicit funds appear legitimate is an essential component of serious and organised crime.

Effective AML/CTF laws are critical to the ongoing fight against organised crime and terrorism. Australia has a robust regulatory regime to detect and deter money laundering and terrorism financing. However, the constantly changing nature of financial crime, including money laundering, means that Australia must remain vigilant, identify and rectify weaknesses in the current regime, and be responsive to new and emerging trends in money laundering.

AGD is playing a key role establishing the foundations of secure digital identities to promote trust and reduce the risk of financial crime enabled by identity crime to increase online. Strong identity verification processes, using the DVS and supported by the national identity proofing guidelines, will be important foundations.