Australian Government
Attorney-General's Department

APRIL 2016

REPORT ON THE STATUTORY REVIEW OF THE ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING ACT 2006 AND ASSOCIATED RULES AND REGULATIONS

ISBN 978-1-925290-60-8 (print)

ISBN 978-1-925290-61-5 (online)

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the It's an Honour website (www.itsanhonour.gov.au).

Contact us

For enquiries regarding the licence and any use of this report please contact:

Director, Governance Office
Attorney-General's Department
3–5 National Circuit
BARTON ACT 2600

Telephone: 02 6141 6666
Email: copyright@ag.gov.au

For enquiries regarding the content of this report and the statutory review of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* please contact:

Transnational Crime Branch
Attorney-General's Department
3–5 National Circuit
BARTON ACT 2600

Telephone: 02 6141 6666
Email: AMLreview@ag.gov.au

Minister's Foreword

I am pleased to present the report of the statutory review of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) and the associated Rules and Regulations.

Money laundering and terrorism financing are major global problems. They threaten Australia's national security and the integrity of Australia's financial system.

Money laundering is a key enabler of organised crime. Every year, criminals generate huge amounts of funds from illicit activities such as drug trafficking, tax evasion, people smuggling, theft, fraud and corruption. To enjoy the profits of their illicit activity without raising suspicion, criminals must find ways to place these funds into the legitimate financial system and obscure their origins.

Funds for terrorism can come from a range of sources, legitimate and illegitimate. Relatively small amounts of money placed in the hands of terrorists and terrorist organisations can be disastrous, funding attacks on Australian soil or supporting terrorist activities overseas.

Countries that become a soft touch for money launderers and terrorist financiers jeopardise their national security and undermine the credibility of their financial institutions and economies. They also pose a threat to the international financial system and the international community.

The AML/CTF Act commenced operation on 12 December 2006 and established a regime designed to make the Australian financial system hostile to money laundering and terrorism financing threats. In doing so, the Act bolsters national security, enhances Australia's international reputation as a destination for foreign business and investment, and protects the reputation of Australian business in highly competitive overseas markets.

The AML/CTF Act provides the foundation of Australia's commitment to meet global standards for combating money laundering and terrorism financing developed by the Financial Action Task Force (FATF). The FATF is the lead inter-governmental body that develops and promotes implementation of international anti-money laundering and counter-terrorism financing (AML/CTF) standards.

Since 2006, Australia's AML/CTF regime has been strengthened through amendments to the AML/CTF Act and the making of Rules and Regulations. The regime has also been complemented by other policy and operational measures that strengthen our capabilities to address our money laundering and terrorism financing risks.

The statutory review provides an opportunity to shape a modern AML/CTF regime that positions Australia to address current and future challenges. This modern regime will involve closer collaboration with the private sector and harness cutting edge technology to mitigate risks and threats to Australia's financial system to achieve better regulatory outcomes for government and industry.

The review has overlapped with an evaluation by the FATF of Australia's compliance with the international AML/CTF standards. The FATF published the report of this evaluation in April 2015, providing valuable information for consideration as part of this review.

The finalisation of this review comes at a time when countries around the world are looking to strengthen measures to combat terrorism financing in the wake of recent terrorist attacks in Lebanon, Egypt, Paris, Indonesia, Belgium and Pakistan. These deplorable acts of violence remind us that continued vigilance is essential. They also highlight the importance of remaining flexible and responsive to evolving threats to national and global security.

I would like to thank the industry groups, businesses, agencies, organisations and individuals who participated in the consultation process for the statutory review. Your comments and suggestions have instigated some robust discussions on the future of Australia's AML/CTF regime.

The private sector in Australia was closely involved in the design of the regime established under the AML/CTF Act and has continued to work collaboratively with government. This genuine dialogue between government and industry will help deliver a much simpler and streamlined regulatory framework that addresses contemporary challenges in the financial, criminal and national security environments and leverages innovation and creativity.

The Hon. Michael Keenan MP
MINISTER FOR JUSTICE

Table of Contents

Terms of reference and guiding principles

Purpose

To review the operation of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act), the *Anti-Money Laundering and Counter-Terrorism Financing Regulations 2008,*[1] and the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)* (collectively the 'AML/CTF regime') in accordance with section 251 of the AML/CTF Act.

Objectives

The statutory review will examine:

- the operation of the AML/CTF regime
- the extent to which the policy objectives of the AML/CTF regime remain appropriate, and
- whether the provisions of the AML/CTF regime remain appropriate for the achievement of those objectives.

The review will culminate in a report to the Government which may include recommendations for reform of the AML/CTF regime.

Guiding principles

The statutory review will be guided by the following principles as they relate to AML/CTF:

- Create a financial environment hostile to money laundering, the financing of terrorism, serious and organised crime and tax evasion, through industry regulation and the collection, analysis and dissemination of financial intelligence.
- Ensure Australia fulfils its international obligations and addresses matters of international concern (including the Financial Action Task Force standards, the Egmont Group, Group of 20 Nations, United Nations Security Council Resolutions, the United Nations Convention against Corruption and the United Nations Convention on Transnational Organised Crime).
- Support the better regulation agenda to simplify the regulatory burden on reporting entities (in particular, small businesses), while maintaining an AML/CTF regime which represents the most appropriate, efficient and effective means of achieving government objectives.
- Foster and enhance international cooperation and collaboration.
- Work in partnership with industry, the states and territories to promote a national effort to maintaining the AML/CTF regime.
- Ensure the AML/CTF regime produces information necessary to assist the Australian Government and law enforcement agencies to combat money laundering, the financing of terrorism and serious and organised crime.
- Ensure privacy considerations are appropriately addressed.

[1] On 15 April 2014, the *Anti-Money Laundering and Counter-Terrorism Financing Regulations 2008* ceased operation and were replaced by the *Anti-Money Laundering and Counter-Terrorism Financing (Iran Countermeasures) Regulation 2014*. This was replaced by the *Anti-Money Laundering and Counter-Terrorism Financing (Prescribed Foreign Countries) Regulation 2016* on 26 February 2016.

Executive summary

This statutory review examines the operation of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (the AML/CTF Act) and the associated Rules and Regulations.[2]

The AML/CTF Act was developed in consultation with industry to establish a strong and modern regulatory regime for combating money laundering and terrorism financing (ML/TF), as well as other serious crimes. The central components of this regime require regulated businesses to:

- establish, implement and maintain an anti-money laundering and counter-terrorism financing (AML/CTF) compliance program
- conduct customer due diligence (CDD), and
- lodge specified transaction and suspicious matter reports with the Australian Transaction Reports and Analysis Centre (AUSTRAC).

The regime established under the AML/CTF Act and the associated Rules and Regulations (the AML/CTF regime) represents an important partnership between government and industry. Information reported to AUSTRAC by industry establishes an audit trail for transactions, allowing AUSTRAC to generate financial intelligence that assists partner agencies to detect and disrupt serious and organised crime and terrorism.

A wide range of industry stakeholders and government agencies were consulted during the review, providing feedback on what is working well and identifying areas where reforms may be required.

Industry stakeholders strongly supported the aims of the AML/CTF regime, but generally considered that the legal framework for obligations is unduly complex and often poorly understood by regulated businesses, particularly smaller businesses. These stakeholders asked for obligations to be simplified, streamlined and clarified, and the regulatory burden reduced, where possible. They also sought more guidance and assistance from AUSTRAC on how to understand their ML/TF risks and comply with their obligations.

Partner agencies considered that the AML/CTF regime is generally working well and indicated that the financial intelligence generated by AUSTRAC is extremely useful from an operational perspective. These partner agencies supported greater access to AUSTRAC information, a broadening of the regime to capture other services that pose a high ML/TF risk, and enhanced audit, information-gathering and enforcement powers to further strengthen industry compliance.

The feedback provided by industry stakeholders and government agencies has been invaluable, informing discussions and shaping ideas for future reforms.

The review has also taken into account the relevant findings in the Financial Action Task Force's (FATF) mutual evaluation report (MER) on Australia.[3] The MER, which was publicly released in April 2015, evaluates Australia's technical compliance with the FATF's international standards for combating ML/TF and assesses the effectiveness of Australia's AML/CTF regime.[4]

The MER identified a number of deficiencies in the scope of Australia's AML/CTF regime and the preventive measures that apply to regulated entities. These deficiencies have been considered and options explored to improve compliance.

---

[2] Section 251 of the AML/CTF Act outlines the requirements for the statutory review of the AML/CTF Act, Rules and Regulations.
[3] The FATF is an inter-governmental body that develops and promotes policies to combat money laundering, terrorist financing and the proliferation of weapons of mass destruction. The FATF has developed 40 Recommendations that are recognised as the international standard for combating these threats.
[4] Financial Action Task Force, *Australia, Mutual Evaluation Report*, April 2015, http://www.fatf-gafi.org/topics/mutualevaluations/documents/mer-australia-2015.html.

The report on the review concludes that the AML/CTF regime remains relevant and appropriate, but determines that there is scope to strengthen the regime and achieve greater regulatory efficiencies. To this end, the report makes a number of recommendations intended to deliver a simpler and streamlined AML/CTF regime that:

- makes better use of the risk-based approach to provide regulatory relief
- minimises red tape, duplication and unnecessary regulatory burden
- better supports industry to understand and comply with AML/CTF obligations by improving the readability and accessibility of the AML/CTF Act and Rules
- captures services that pose a high ML/TF risk and remains responsive to new and emerging threats
- readily facilitates access to, and the use of, AUSTRAC information by government agencies involved in detecting and disrupting serious and organised crime, and terrorism
- supports enhanced collaboration between government agencies involved in detecting and disrupting serious and organised crime, and terrorism
- recognises the pivotal role of the private sector in the detection and prevention of criminality and seeks to leverage this expertise by building trusted partnerships for the sharing of financial intelligence
- strengthens the audit, information-gathering and enforcement framework used by AUSTRAC and its partner agencies to build a culture of compliance among regulated businesses, and
- aligns more closely with best practice approaches that are consistent with the FATF standards.

A summary of the key findings and recommendations is provided below.

The report also considers the lessons learnt from recent terrorist attacks overseas. These attacks have highlighted the challenges associated with combating and disrupting terrorism financing activity. They have also sparked a renewal of global efforts to better understand the changing nature of terrorism financing risks and strengthen measures to address those risks.

As Australia's AML/CTF regulator, AUSTRAC will respond to feedback gathered during the course of the review that relates to its operations. This will include several measures to assist regulated entities to better understand and comply with their AML/CTF obligations.

The Government will consult closely with relevant industry and government stakeholders about any proposed reforms arising from this report. Any changes to AML/CTF obligations will be carefully prioritised and managed to minimise the impacts on regulated entities and avoid regulatory fatigue.

Summary of key findings and recommendations

The review makes a number of findings and sets out recommendations to improve and strengthen the operation of the AML/CTF Act, Rules and Regulations.

Key findings

- **Industry is supportive of Australia's AML/CTF regime and the risk-based approach**
  Industry stakeholders and partner agencies acknowledged the benefits of a robust AML/CTF regime and are broadly supportive of the objectives underpinning the AML/CTF Act. The majority of industry stakeholders also supported the use of the risk-based approach to enable regulated entities to efficiently use and allocate resources proportionate to the level of assessed risk.
- **The AML/CTF Act and Rules are too complex**
  Industry stakeholders and partner agencies commonly raised concerns about the complexity of the

AML/CTF Act and the Rules. This complexity generates significant uncertainty, impeding industry's ability to understand and comply with their obligations. The length, legalistic style and fragmented structure of the Rules are major issues for some regulated businesses, particularly smaller businesses, who generally find the Rules inaccessible.

- **Industry requires more assistance to understand and comply with their obligations**
  Industry stakeholders asked for more sector-specific guidance to support them in understanding their AML/CTF obligations. Smaller regulated businesses tend to struggle to identify and understand their ML/TF risks, and develop AML/CTF systems to manage and mitigate those risks. These businesses are seeking more prescription in the AML/CTF Act and Rules, and greater guidance from AUSTRAC, about the extent of their obligations. Larger regulated businesses are more comfortable with the risk-based approach and applying it to their business.
- **More exemptions could be provided for services that pose a low ML/TF risk**
  Industry stakeholders considered that there are opportunities to provide considerable regulatory relief for regulated businesses by providing exemptions or extending the use of simplified obligations for services that pose a low ML/TF risk.
- **The framework for combating terrorism financing requires strengthening**
  The international community is examining ways to address the unprecedented threats posed by terrorist organisations such as the Islamic State of Iraq and the Levant (ISIL). With the nature of terrorism financing risks constantly evolving, Australia's framework for combating terrorism financing should be strengthened so these risks can be addressed and terrorism financing activity effectively detected and disrupted.
- **Other services that pose a high ML/TF risk should be captured under the AML/CTF regime**
  Submissions to the review generally supported extending AML/CTF regulation to other services that pose high ML/TF risks. These include new payment types and systems (such as digital currencies) and a range of services provided by lawyers, accountants, conveyancers, real estate agents, high-value dealers, trust and company service providers, and offshore-based businesses.
- **Transaction reporting thresholds should be reviewed**
  Partner agencies supported the retention of existing reporting thresholds, but industry stakeholders considered the value of the thresholds should be reviewed and possibly increased to take into account inflation and reduce regulatory burden.
- **Reporting obligations are onerous and should be streamlined**
  Industry stakeholders considered that reporting requirements should be streamlined to reduce duplication and minimise red tape.
- **AML/CTF programs requirements should be consolidated and streamlined**
  Industry stakeholders considered that the requirements for AML/CTF programs are too complex. They also asked that regulated businesses be permitted to develop AML/CTF programs at the corporate group level, including corporate groups with foreign branches and subsidiaries.
- **The record-keeping retention period should be reviewed**
  Industry stakeholders considered that the record-keeping retention period should be reviewed and lowered to align with the FATF standards and reduce regulatory burden.
- **Regulatory measures for remitters should be strengthened**
  Stakeholders representing the remittance sector and partner agencies considered that the AML/CTF regulation of remitters should be strengthened to reduce the ML/TF risks associated with remittance services.

- **The secrecy and access provisions are overly complex and impede information-sharing**
  Partner agencies raised concerns about the complexity of the secrecy and access provisions under the AML/CTF Act that provide for the collection, use and disclosure of AUSTRAC information. This complexity generates considerable uncertainty, impeding the flow of financial intelligence for operational purposes and preventing the sharing of AUSTRAC information for other legitimate purposes.
- **Enforcement measures should be strengthened**
  Partner agencies considered that the offences regime under the AML/CTF Act could be strengthened to better encourage a culture of compliance among regulated businesses. They supported a wider use of infringement notices for a range of minor offences and giving partner agencies that have information-gathering powers under the AML/CTF Act the power to apply sanctions. They also suggested giving AUSTRAC responsibility for supervising compliance with Australian sanction laws.
- **AML/CTF reporting obligations under two Acts is inefficient**
  With the introduction of the AML/CTF Act in 2006, certain parts of the *Financial Transaction Reports Act 1988* (FTR Act) were repealed or became inoperative. Others parts of the FTR Act continue to impose reporting obligations on cash dealers and solicitors. This creates two AML/CTF reporting regimes, with no apparent regulatory gain.

Key recommendations

This report makes 84 recommendations to strengthen Australia's AML/CTF regime and implement a more efficient and effective regulatory framework. These recommendations are set out in full in *Chapter 20: Table of Recommendations*.

The recommendations arising from this review are designed to bolster measures to protect the Australian community and financial system, while not imposing unnecessary costs on regulated businesses.

Measures are proposed that will simplify obligations and use the risk-based approach in a more targeted way to minimise the regulatory burden. The report also proposes measures that will strength regulation and better position law enforcement agencies to respond to new and emerging threats, including dynamic terrorism and terrorism financing threats.

A summary of the general recommendations and key specific recommendations is set out below.

General recommendations

- **Simplify the AML/CTF Act**
  The AML/CTF Act should be simplified and become more principles-based, with some detail provided in the Rules and the remaining detail provided in guidance.
- **Simplify and rationalise the AML/CTF Rules**
  The AML/CTF Rules should be simplified, rationalised, drafted in plain language, presented in a user-friendly format, and supported by guidance.
- **Co-design future reforms in partnership with industry and partner agencies**
  Reforms to the AML/CTF Act and Rules arising from this review should be co-designed with industry and partner agencies.
- **Embed the principle of technology neutrality**
  The AML/CTF regime should not favour one technology at the expense of another and should anticipate the future use of technology as much as possible.
- **Provide regulated businesses with enhanced feedback**
  AUSTRAC should provide targeted feedback to regulated businesses about supervisory and

compliance activity, and transaction reporting to assist them to understand and comply with their AML/CTF obligations.

- **Review Australia's counter-terrorism financing measures**
  A government working group should be established to consider international developments in combating terrorism financing and consider the appropriateness of these measures for the Australian context.

Specific recommendations

- **Broaden the objects of the AML/CTF Act**
  The objects of the AML/CTF Act should be broadened to articulate the benefits of a robust AML/CTF regime from a national perspective.
- **Capture high ML/TF risk services**
  New payment types and systems that pose a high ML/TF risk, such as digital wallets and digital currencies, should be subject to AML/CTF regulation. Models for AML/CTF regulation of non-financial businesses and professions designated for coverage by the FATF standards, such as lawyers, accountants, conveyancers, real estate agents, high-value dealers and trust and company service providers, should be developed and a cost-benefit analysis conducted. The ML/TF risks posed by other services recognised as having ML/TF vulnerabilities should also be assessed, such as:
    - cheque cashing facilities, and
    - offshore-based businesses that provide services regulated under the AML/CTF Act to customers in Australia.

  Where such services are assessed as posing a high ML/TF risk, options for regulating these services should be explored as appropriate. The continued appropriateness of the thresholds applicable to the stored value cards designated services should also be re-assessed in light of the emerging ML/TF risks posed by these cards.
- **Re-consider the AML/CTF regulation of specific services that pose a low ML/TF risk**
  Services provided by cash-in-transit operators pose a low ML/TF risk and should not be regulated under the AML/CTF regime. The ML/TF risks associated with traveller's cheques should be reassessed with a view to removing traveller's cheques from the AML/CTF regime if they are found to pose a low ML/TF risk.
- **Minimise the regulatory burden associated with complying with CDD obligations**
  The regulatory burden associated with CDD obligations should be minimised by:
    - simplifying the CDD obligations in the AML/CTF Act and Rules
    - expanding the application of simplified CDD procedures where there is a proven low ML/TF risk, and
    - enhancing the ability of business to rely on the CDD conducted by other regulated businesses.
- **Simplify and streamline transaction reporting requirements to minimise regulatory burden and more closely align them with the FATF standards**
  Reporting requirements should be amended to remove regulatory inefficiencies, provide greater clarity and improve compliance with the FATF standards. This process should include considering:
    - extending the funds transfer chain definition to providers of designated remittance arrangements

    - reviewing the utility of requiring transaction reports to be submitted by two entities involved in the one transaction, and
    - reviewing the utility of requiring both threshold transaction reports and international funds transfer instructions to be reported as part of one transaction.
- **Assess whether the international funds transfer reporting obligations accurately reflect ML/TF risks**
  While threshold-free reporting of international fund transfer instructions should be retained, options should be explored to better calibrate these reporting obligations to high and low risk transactions.
- **Simplify, streamline and clarify AML/CTF program obligations**
  The obligation for regulated businesses to develop, implement and maintain an AML/CTF program that is effective in managing and mitigating risks should be simplified and streamlined. This should include consolidating program requirements, allowing programs to be implemented at the group level, clarifying the role and functions of the AML/CTF compliance officer, and clarifying the obligations that apply to foreign branches and subsidiaries.
- **The record-keeping obligations should be aligned with the FATF standards and the seven-year mandatory retention period for records should be retained**
  Businesses should be required to retain sufficient records to reconstruct individual transactions to align record-keeping requirements with the FATF standards. The mandatory retention period for records should be retained at seven years.
- **Simplify and rationalise compliance reporting**
  AUSTRAC should develop a new compliance reporting tool that better meets the information needs of AUSTRAC and removes any unnecessary reporting.
- **Simplify and align correspondent banking obligations with the FATF standards**
  The correspondent banking obligations should be simplified and modified to better align with the FATF standards. This includes broadening the definition of a correspondent banking relationship, requiring mandatory due diligence and ongoing due diligence assessments, and requiring specific due diligence in relation to payable-through accounts.
- **Enhance the registration framework for remitters**
  The Government should work with industry to develop proposals to enhance the registration framework for the AML/CTF regulation of remitters. The AML/CTF Act should also be amended to strengthen the AUSTRAC CEO's ability to regulate remitters.
- **Strengthen the cross-border reporting regime**
  The AML/CTF Act should be amended to establish a consolidated requirement to report all cross-border movements of cash and bearer negotiable instruments (BNI) worth AUD10,000 or more. The definitions of cash and BNI should also be broadened to capture other objects or instruments that can be transported across borders and pose a high ML/TF risk.
- **Simplify the secrecy and access provisions to improve the sharing of AUSTRAC information**
  A simplified framework should be developed to govern access to, and the sharing of, AUSTRAC information under the AML/CTF Act. This new framework should:
    - clarify obligations
    - expand the permissible uses of AUSTRAC information, including to assist future public-private partnership initiatives
    - facilitate effective and efficient information-sharing between domestic and international partner agencies

- provide for safeguards, protections and controls to apply to all confidential and sensitive information held by AUSTRAC subject to prescribed exemptions, and
- permit regulated businesses to disclose suspicious matter report information to related foreign entities.

- **Strengthen and standardise the enforcement powers under the AML/CTF Act**
  The AML/CTF Act should be amended to adopt the model regulatory powers set out in the *Regulatory Powers (Standard Provisions) Act 2014*, while maintaining existing AML/CTF-specific powers. AML/CTF Act enforcement powers should also be strengthened by:
  - exploring options for compliance testing
  - expanding the scope of remedial directions
  - expanding the use of infringement notices to other minor regulatory offences, and
  - allowing specified AUSTRAC partner agencies to issue an infringement notice or apply to the Federal Court for a civil penalty order where a regulated business fails to comply with a notice issued by that agency.
- **Clarify and expand the functions of the AUSTRAC CEO**
  The AML/CTF Act should be amended to give the AUSTRAC CEO standard powers to perform his or her functions. The functions of the AUSTRAC CEO should also be more closely linked with the objects of the Act, and the feasibility of giving the AUSTRAC CEO responsibility for supervising compliance with Australian sanction law explored.
- **Simplify and streamline the application process for exemptions and adopt a more proactive approach to considering potential exemptions**
  AUSTRAC should adopt a proactive and systematic approach to reviewing the ML/TF risks posed by specific services, transactions and customer types, and granting exemptions where low ML/TF risks are identified. The process for industry to apply for exemptions under the AML/CTF Act should be streamlined, simplified and supplemented by additional guidance and templates.
- **Repeal the FTR Act**
  The FTR Act should be repealed and AML/CTF-related reporting obligations consolidated under the AML/CTF Act to establish a single reporting regime.

1. Introduction

Background to Australia's AML/CTF regime

Money laundering and terrorism financing are criminal offences in Australia. This criminal justice response to the threat posed by these serious offences is complemented by a regulatory response that establishes a framework for collecting valuable information from the private sector about the movement of money and other assets.

Regulatory responses to combating ML/TF in Australia began in 1988 with the introduction of the *Cash Transaction Reports Act 1988* (CTR Act). The CTR Act was the outcome of several Royal Commissions which uncovered links between tax evasion, fraud, organised crime and money laundering.[5] It created reporting requirements for cash dealers, imposed obligations on customers' accounts and established the predecessor to AUSTRAC – the Cash Transaction Reports Agency.

The introduction of the CTR Act was closely followed by the creation of the Financial Action Task Force (FATF) in 1989. Australia is one of the 15 founding members of the FATF. This international policy-making body promotes the effective implementation of legal, regulatory and operational measures for combating ML/TF and other related threats to the integrity of the international financial system. The FATF assesses formal compliance with its standards through 'mutual evaluations' of member countries. This involves a peer assessment of whether a country complies with the standards and whether its AML/CTF regime is effective.

In April 1990, the FATF issued its first set of 'Forty Recommendations' for implementing effective anti-money laundering measures. These measures, some of which were already implemented by the CTR Act, were designed to increase the transparency of the financial system and give countries the capacity to successfully take action against money launderers. In response, the CTR Act was overhauled in 1992 and renamed the *Financial Transaction Reports Act 1988* (FTR Act). The Cash Transaction Reports Agency was also renamed the Australian Transaction Reports and Analysis Centre (AUSTRAC) and focused primarily on developing and providing financial intelligence to partner agencies.

In response to the terrorist attacks on the United States on 11 September 2001, countering terrorism financing was added to the mandate of the FATF. Revised standards were developed and released in 2003, which included 'Nine Special Recommendations' to deal with terrorism financing. In 2009, the FATF commenced another review of the FATF standards, which resulted in the adoption of a single set of forty revised recommendations in 2012.[6] These revised standards include new standards, new requirements under existing standards and a framework for assessing the effectiveness of AML/CTF measures.[7]

The AML/CTF Act

In 2005, the FATF evaluated Australia's compliance with the FATF's 2003 Forty Recommendations on Money Laundering and Nine Special Recommendations on Terrorism Financing. At that time, Australia was already reviewing its AML/CTF regime. These two reviews culminated in the passage of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act).

---

[5] The Royal Commission of Inquiry into Drugs (Williams 1980), Royal Commission of Inquiry into Drug Trafficking (Stewart 1983) and Royal Commission on the Activities of the Federated Ship Painters and Dockers Union (Costigan 1984).

[6] Financial Action Task Force, *The FATF Recommendations*, February 2012, http://www.fatf-gafi.org/topics/fatfrecommendations/documents/fatf-recommendations.html.

[7] Financial Action Task Force, *Methodology for assessing technical compliance with the FATF Recommendations and the Effectiveness of AML/CFT systems*, February 2013, http://www.fatf-gafi.org/topics/fatfrecommendations/documents/fatfissuesnewmechanismtostrengthenmoneylaunderingandterroristfinancingcompliance.html.

The AML/CTF Act was developed in close consultation with industry in order to co-design an appropriate, cost-effective framework that would meet the needs of industry, the public and law enforcement. The policy goals of the legislation are to implement a regulatory framework that:

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

The AML/CTF Act establishes the principal obligations for individuals and businesses regulated under the regime (called reporting entities). Those obligations are to:

- enrol with AUSTRAC
- register with AUSTRAC if the reporting entity provides remittance services
- develop and maintain an AML/CTF program to identify, mitigate and manage ML/TF risks associated with their services
- identify customers and undertake ongoing customer due diligence (CDD)
- lodge transaction, suspicious matter and compliance reports with AUSTRAC, and
- comply with various AML/CTF-related record-keeping obligations.

The AML/CTF Act is complemented by the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)* (AML/CTF Rules). The AML/CTF Rules are issued by the AUSTRAC CEO and provide the detail for the broader obligations set out in the AML/CTF Act. The Rules are an enforceable legal instrument, which can be allowed or disallowed by Parliament.

AUSTRAC develops the AML/CTF Rules in consultation with relevant government agencies, industry and other stakeholders.

The Governor-General may make Regulations on matters covered by the AML/CTF Act.[8] The regulation-making power provides a tool to respond in a timely manner to technical or mechanical issues or to give effect to a specific provision in the Act. The regulation-making power has been used sparingly to date to amend items related to designated services and give effect to countermeasures regarding Iran and the Democratic People's Republic of North Korea (DPRK / North Korea).[9]

The AML/CTF Act was implemented in a staggered manner from 2006 with all provisions fully operational from 12 December 2008. In 2006, the then Minister for Justice issued Policy Principles under section 213 of the AML/CTF Act to give effect to a Government undertaking that the AUSTRAC CEO would only take civil penalty action against a reporting entity, rather than criminal enforcement activity, where that reporting entity has failed to take reasonable steps towards compliance with its obligations under the Act during a 15 month period following commencement of the obligations under the Act.

The introduction of the AML/CTF Act significantly expanded the operation and regulatory coverage of Australia's AML/CTF regime. From fewer than 4,000 cash dealers under the FTR Act, the regime expanded to a regulated population of over 14,040 reporting entities in the financial, remittance, gambling and bullion sectors. AUSTRAC was also given stronger compliance and enforcement powers to use in supervising the larger regulated population.

[8] Section 252 of the AML/CTF Act.
[9] *Anti-Money Laundering and Counter-Terrorism Financing (Prescribed Foreign Countries) Regulation 2016.*

Over the past seven years, the volume of transaction reporting from industry has significantly grown, rising from 18 million reports in 2007-08 to over 96 million reports in 2014-15.[10] The number of government agencies that can access and use this information has also increased.

The FTR Act remains in operation and contains residual reporting obligations for cash dealers (as defined under section 3 of the FTR Act). If a service offered by a cash dealer under the FTR Act falls within the definition of a designated service under the AML/CTF Act, the FTR Act obligations under the do not apply in relation to that service.

Australia has sought to respond to new and emerging risks and changes in international best practice in order to ensure that the AML/CTF regime remains robust. In 2011, the regulation of remitters was significantly strengthened by the introduction of a rigorous registration process. In June 2014, new AML/CTF Rules came into force that introduced more stringent CDD requirements consistent with the FATF standards.

The risk-based approach

The risk-based approach is a key pillar of Australia's AML/CTF regime and central to the effective implementation of the FATF standards.

By adopting a risk-based approach, reporting entities can implement compliance measures that are proportionate to their assessed level of ML/TF risk. This approach recognises that the reporting entity is in the best position to assess the ML/TF risks posed by its customers, delivery channels, products and services and allows reporting entities to allocate resources in an efficient way.

The role of AUSTRAC

AUSTRAC is Australia's AML/CTF regulator and financial intelligence unit (FIU). It was established in 1989 under the FTR Act and continues in existence under section 209 of the AML/CTF Act.

AUSTRAC's purpose is to protect the integrity of Australia's financial system and contribute to the administration of justice through expertise in countering ML/TF. As part of its regulatory role, AUSTRAC promotes compliance with the obligations of the AML/CTF Act by providing guidance and assistance to reporting entities. AUSTRAC also assesses reporting entities' compliance with AML/CTF obligations and undertakes enforcement action where non-compliance is identified.

In performing its regulatory functions, AUSTRAC must ensure that the AML/CTF regime supports economic efficiency and competitive neutrality.

AUSTRAC also analyses and enhances the financial information provided by reporting entities and disseminates intelligence products to its law enforcement, national security, human services and revenue partner agencies in accordance with the secrecy and access requirements of the AML/CTF Act. This financial intelligence has become a crucial element in the detection and investigation of serious and organised crime, ML/TF and tax evasion. AUSTRAC also collects and assesses transaction reports by cash dealers and solicitors under the FTR Act and exchanges intelligence with international counterparts to support global efforts to combat transnational crime.

The increase in the number of transaction reports provided to AUSTRAC since the introduction of the AML/CTF Act has improved law enforcement's access to financial intelligence. In 2014-15, AUSTRAC:

- disseminated 93,137 suspicious matter reports (SMRs) and suspicious transaction reports (SUSTRs) to partner agencies to assist them in their investigations
- disseminated 943 detailed financial intelligence reports, and

[10] AUSTRAC, *AUSTRAC Annual Report 2014-15,* http://www.austrac.gov.au/sites/default/files/austrac-ar-14-15-web.pdf.

- conducted 857 exchanges of financial intelligence with international FIUs.[11]

In 2014-15, AUSTRAC's information and intelligence directly contributed to the following partner agency outcomes:

- 16,038 Australian Taxation Office (ATO) cases, resulting in AUD466 million in additional tax assessments raised, and
- 373 cases and AUD5.5 million of annualised savings for the Department of Human Services.[12]

Fourth Round Mutual Evaluation of Australia

Australia was one of the first countries to be assessed against the revised 2012 standards under the FATF's fourth round of mutual evaluations.

The FATF publicly released the mutual evaluation report (MER) in April 2015.[13] The MER highlights Australia's progress since 2005, acknowledging the strengths of Australia's AML/CTF regime. This includes Australia's understanding of the primary ML/TF risks and operational cooperation to address those risks. Law enforcement's efforts to combat terrorism financing are commended, as is Australia's framework for international cooperation. The legal framework for implementing targeted financial sanctions is recognised as world's best practice.

Australia rated well on effectiveness across a number of areas in the MER. This means that aspects of Australia's AML/CTF regime are producing the expected outcomes.

The MER includes recommendations to enhance the AML/CTF Act's technical compliance with the FATF standards. Some of these recommendations relate to known gaps in Australia's AML/CTF regime. Others are new requirements introduced by the revised 2012 standards. The recommendations in the MER to improve technical compliance with the FATF standards that would require amendment of the AML/CTF Act, Rules and Regulations are considered as part of this review.

Conduct of the review

Section 251 of the AML/CTF Act requires a review of the operation of the AML/CTF Act, Rules and Regulations. This review must commence before the end of the period of seven years after the commencement of that provision and a report about the review prepared and tabled by the Minister for Justice in each House of Parliament within 15 sitting days of the report's completion.

The statutory review of the AML/CTF Act commenced on 4 December 2013 with the publication of Terms of Reference and Guiding Principles, and the release of an issues paper for public comment. More than 80 submissions were received from the private sector, the public and government agencies in response to the issues paper.[14] A series of roundtable discussions were also held between September 2014 and May 2015 with industry groups, private sector representatives, not-for-profit organisations and government agencies to discuss the issues raised in submissions and better understand concerns about the operation of the AML/CTF regime.[15]

[11] AUSTRAC, *AUSTRAC Annual Report 2014-15,* http://www.austrac.gov.au/sites/default/files/austrac-ar-14-15-web.pdf.
[12] *bid*.
[13] Financial Action Task Force, *Australia, Mutual Evaluation Report*, April 2015, http://www.fatf-gafi.org/topics/mutualevaluations/documents/mer-australia-2015.html.
[14] A list of the public submissions received is available on the Attorney-General's Department's website: http://www.ag.gov.au/Consultations/Pages/StatReviewAntiMoneyLaunderingCounterTerrorismFinActCth2006.aspx, (accessed 15 January 2016).
[15] A list of these meetings is provided at *Appendix 1.*

Scope of the review

This review examined the operation of the AML/CTF regime, the extent to which the policy objectives of the AML/CTF regime remain appropriate, and whether the provisions of the AML/CTF regime remain appropriate for the achievement of those objectives.

Changes to the AML/CTF Rules introduced in June 2014 to strengthen CDD obligations and the new industry contribution arrangements to fund AUSTRAC's regulatory and intelligence functions that apply from the 2014-15 financial year onwards have not been considered as part of the review.[16]

Other policy considerations

Over the past few years, the Government has actively pursued reforms to cut unnecessary red tape and implement well-designed regulation to reduce the cost incurred in complying with Commonwealth regulation. The AML/CTF regime was reviewed taking into account the principles of this 'better regulation' agenda.

The regulation of small business under the AML/CTF regime poses a range of specific challenges in terms of achieving better regulatory outcomes, as the ML/TF risks posed by the services offered by these small businesses need to be addressed without unduly hampering the efficient conduct of business. The risk-based approach adopted under the AML/CTF Act provides some assistance to meet this challenge by giving businesses the flexibility to comply with their obligations in a way that addresses their specific risks. This approach minimises compliance costs.

The AML/CTF regime also provides mechanisms to exempt reporting entities from regulatory obligations. The use of these mechanisms has been examined under this review with a view to achieving better regulatory efficiencies for business and government.

The review has also considered the role that AML/CTF measures in addressing national security threats, including serious and organised crime. Australia's National Organised Crime Response Plan 2015-18[17] is one of the three key elements of the Australian Government's approach to serious and organised crime that promotes a coordinated national approach to combating these threats. The plan outlines how the Commonwealth, states and territories will work together over the next three years to address a number of key threats from serious and organised crime, including the increasing prevalence of drugs such as ice and gun-related crime and violence. Developing a strengthened national approach to financial crime, tackling the criminal proceeds of organised crime and reducing barriers to information-sharing between agencies are all priorities under the plan. Initiative 5A of the plan specifically relates to the enhancing of measures to address ML/TF.

[16] Attorney-General's Department, *Review of the AML/CTF Act – Issues Paper,* December 2013, p. 6, http://www.ag.gov.au/Consultations/Documents/issues-paper-review-aml-ctf-regime-20131202.pdf.
[17] See the Attorney-General's Department's website for further information: https://www.ag.gov.au/CrimeAndCorruption/OrganisedCrime/Pages/default.aspx, (accessed 15 January 2016).

2. Overarching issues

Industry stakeholders and partner agencies raised a number of issues that have broader implications for the AML/CTF regime. These overarching issues relate to:

- the complexity of the legislative framework for the AML/CTF regime
- the ability to use technology to meet AML/CTF obligations
- the tension between the risk-based approach and a prescriptive approach to AML/CTF regulation
- the need for more guidance and feedback from AUSTRAC as the AML/CTF regulator
- the timing for any reforms that may arise from the review, and
- the need for AUSTRAC and partner agencies to be adequately equipped to combat and disrupt terrorism financing nationally and internationally.

This report makes a number of general recommendations to address these issues that centre on:

- simplifying the AML/CTF Act and Rules
- adopting technology neutrality
- clarifying the risk-based approach
- consulting closely with industry in the reform process, and
- exploring options for strengthening preventative measures for combating and disrupting terrorism financing.

Simplifying the AML/CTF Act and Rules

The AML/CTF regime is overly complex, spanning 344 pages of primary legislation and 309 pages of legislative rules. All industry stakeholders and partner agencies indicated that this complexity impedes the ability of reporting entities to understand and comply with their AML/CTF obligations. The scale, structure and density of the AML/CTF Rules, in particular, was considered to be a major problem, rendering the Rules hard to follow and largely inaccessible, particularly for small business.

The feedback from industry indicates that there is a pressing need to simplify the AML/CTF Act and Rules, and streamline AML/CTF obligations. This could be achieved by establishing a more principles-based AML/CTF regime under the Act and providing some of the details surrounding the content of obligations in the Rules. The remaining details surrounding obligations could be provided in guidance. As part of this process, the AML/CTF Rules should be rationalised, drafted in plain language and presented in a user-friendly format.

While simplifying the AML/CTF Act and Rules would not involve changing existing AML/CTF obligations for reporting entities, the process is likely to generate significant regulatory efficiencies.

In 2005 the United Kingdom's Financial Services Authority (now Financial Conduct Authority) consulted with industry on a proposal to simplify its AML Handbook and Rules. This led to an agreement to move away from prescriptive rules to high level rules that emphasised the need for a firm's senior management to take responsibility for complying with AML/CTF obligations.[18] The simplification project resulted in the

[18] Financial Services Authority, *Reviewing our Money Laundering Regime,* 2005, http://www.fsa.gov.uk/pubs/policy/ps06_01.pdf.

replacement of 57 pages of detailed rules in the AML Handbook and Rules with two pages of high-level principles, and is associated with delivering savings in excess of GBP250 million in administrative costs.[19]

Adopting the technology neutrality principle

Industry stakeholders emphasised during consultations the importance of retaining technology neutrality in the AML/CTF Act and Rules. Reporting entities should be able to use their technology tools of choice to meet their AML/CTF obligations.

The 2014 Financial System Inquiry's report echoed this view, recommending that the principle of technology neutrality be embedded into development processes for future regulation.[20] The Government agreed with this recommendation, noting that technology-specific regulation can impede innovation and competition by preventing the adoption of the best technology or the most innovative business models.[21]

While the AML/CTF Act and Rules have aimed to be technology neutral, the AML/CTF framework has not always anticipated new technologies.[22] Any future reforms to the AML/CTF Act and Rules should adhere to this principle and be able to accommodate new technologies.

Clarifying the risk-based approach through enhanced AUSTRAC feedback and guidance

Industry stakeholders expressed differing views about how best to assist reporting entities to understand their AML/CTF obligations.

Smaller and medium-sized reporting entities tend to favour increased prescription of obligations in the AML/CTF Act and Rules, complemented by guidance. These reporting entities preferred to be 'told exactly what to do', rather than design their own AML/CTF programs based on the specific ML/TF risks they face.

Larger reporting entities are comfortable with using the risk-based approach to design and implement their AML/CTF programs, supported by guidance.

There are two key concerns associated with a more prescriptive approach to AML/CTF regulation. First, a high level of prescription does not allow reporting entities to adopt a flexible set of AML/CTF measures to target their resources efficiently and apply preventive measures that are commensurate to the level of assessed risk.[23] Second, a high level of prescription tends to encourage reporting entities to apply resources for AML/CTF measures uniformly without regard to risk, or target these resources on the basis of factors other than risk. This may lead to a 'tick the box' approach to meeting the minimum prescribed requirements, rather than taking steps to genuinely understand and mitigate ML/TF risks.[24]

A better approach to assisting reporting entities to understand, manage and mitigate their ML/TF risks and comply with their AML/CTF obligations is to provide enhanced guidance. Stakeholders strongly supported the development of more guidance, particularly industry-specific guidance, to build on AUSTRAC's existing guidance.

---

[19] Financial Services Authority, *Simplification Plan*, December 2006, p. 3, http://www.fsa.gov.uk/pubs/other/simplify_plan.pdf.
[20] Recommendation 39, Financial System Inquiry, *Final Report*, 7 December 2014, http://fsi.gov.au/publications/final-report/.
[21] Australian Government, *Improving Australia's financial system: Government response to the Financial System Inquiry*, 20 October 2015, http://www.treasury.gov.au/PublicationsAndMedia/Publications/2015/Govt%20response%20to%20the%20FSI.
[22] See, for example, the consideration of digital currencies in *Chapter 4.3: Regime scope – Payment types and systems.*
[23] Financial Action Task Force, *Guidance on the risk-based approach to combating money laundering and terrorist financing: High level principles and procedures*, June 2007, paragraph 1.7, http://www.fatf-gafi.org/media/fatf/documents/reports/High%20Level%20Principles%20and%20Procedures.pdf.
[24] *Ibid*.

In September 2014, AUSTRAC replaced its regulatory guide with the AUSTRAC compliance guide.[25] The compliance guide consolidates AUSTRAC's guidance using a question and answer format and also includes worked examples, diagrams and hyperlinks to the legal framework. The compliance guide may address some of the issues raised by stakeholders during consultation, but AUSTRAC will continue to review and update the guide to meet the information needs of reporting entities. AUSTRAC should also develop guidance on high-risk customers and scenarios that will address a minor deficiency identified in the MER for Australia.[26]

Industry stakeholders asked for more qualitative and timely feedback from AUSTRAC following compliance and supervisory visits for reporting entities at the individual level and for industry on a sector-wide basis.

Enhanced feedback on the quality and usefulness of transaction and suspicious matter reporting was also specifically requested, particularly feedback on the value of transaction reporting for law enforcement agencies in terms of disrupting and investigating ML/TF and serious criminal activity.

Providing targeted engagement and feedback for the regulated population is a challenge for AUSTRAC because of the number of reporting entities under the AML/CTF Act. The size, scale and scope of regulated entities also varies considerably, with approximately 70 per cent categorised as a small to medium-size business (that is, with 20 or fewer employees). However, AUSTRAC should continue to explore, enhance and expand the mechanisms available for improved and enhanced feedback.

Consulting with industry

Industry stakeholders urged the Government to consult closely with industry when implementing any recommendations arising from the review. A particular concern was the potential cost to industry of any significant reforms that may require changes to reporting entities' systems and programs. Industry also requested that time frames for implementing any AML/CTF reforms take into account other reform processes that may be impacting on the regulated sector and for any AML/CTF reforms to be introduced as one reform package, rather than as waves of reform, to avoid regulatory fatigue.

The establishment of the AML/CTF Act in 2006 was marked by significant and extensive consultation with industry to co-design the AML/CTF regime. This collaborative approach to regulatory reform should continue, with industry and government working together to co-design any changes to the AML/CTF Act and Rules, where appropriate.

Strengthening preventive measures for countering terrorism financing

The wave of terrorist attacks experienced in 2015 and 2016 has renewed global efforts to strengthen measures for detecting, disrupting and preventing these appalling acts of violence. This includes measures to prevent and disrupt the flow of funds to support terrorists and terrorist activity.

In November 2015, Australia co-hosted with Indonesia a Counter-Terrorism Financing Asia-Pacific Summit in Sydney. The Summit brought together a range of stakeholders representing governments, law enforcement agencies, national security agencies and the private sector from Australia and the region to consider ways to work together to identify, understand and counter threats posed by terrorism financing

[25] AUSTRAC, *AUSTRAC compliance guide*, http://www.austrac.gov.au/businesses/obligations-and-compliance/austrac-compliance-guide, (accessed 15 January 2016).

[26] FATF Recommendation 34 (Guidance and feedback). The MER expressed concern that there is only limited guidance available to assist the regulated sector in identifying high-risk customers or situations and observed that none of the guidance published applies to most designated non-financial businesses and professions. See *Chapter 4.2.Regime scope – Designated non-financial businesses and professions* for consideration of this issue.

and foreign terrorist fighters. A key outcome of the Summit was a commitment to develop regional undertakings to collaborate and share financial and other intelligence, and contribute to global strategies to strengthen intelligence-sharing approaches to combat the financing of terrorist groups.[27]

In December 2015, the FATF convened an extraordinary Plenary meeting that focussed on combating the financing of the Islamic State in Iraq and the Levant (ISIL), their affiliates and other terrorist groups. The FATF agreed to focus and accelerate efforts to understand and counter the unprecedented risks posed by ISIL, and ensure that measures to counter terrorism financing are responsive to the changing nature of terrorism financing risks. This includes considering options for strengthening the existing measures and enhancing operational information-sharing.[28]

The French Government announced a package of reforms for combating terrorism financing in the wake of two separate terrorist attacks in Paris in 2015. These include measures to:

- strengthen controls of non-banking payment methods in line with the risk they present, such as pre-paid cards
- investigate the financial activities of suspected persons on law enforcement and national security agency watch-lists
- enable its financial intelligence unit to freeze the bank accounts of suspect persons
- restrict the sale of antiquities and other cultural assets used to finance ISIL, and
- establish a register of bank accounts.[29]

Industry stakeholders and partner agencies were consulted during the review about certain proposals to strengthen Australia's capacity to counter terrorism financing. This includes reassessing the ML/TF risks posed by stored value cards, regulating other services that pose a high ML/TF risk, enhancing Australia's cross-border movement of physical currency and bearer negotiable instruments reporting regime, enhancing the regulation of remitters and developing a modern information-sharing framework that supports collaborative approaches to combating ML/TF and serious crime, at the domestic and international level. These proposals are discussed in detail elsewhere in this report.

The recent attacks overseas have highlighted the need for countries to take urgent action to review the adequacy of counter-terrorism financing measures and enhance their capacity to deny terrorists and terrorist groups access to funds that support their activities. The FATF has reviewed the implementation of counter-terrorism financing measures globally and urged countries with serious problems to table urgent laws to address them. The FATF has also asked countries to focus on the effective implementation of counter-terrorism financing laws.[30]

In light of these international developments, Australia should explore opportunities to enhance its capacity to combat and disrupt terrorism financing in consultation with relevant stakeholders. While Australia has a good understanding of its terrorism financing risks and a comprehensive legal framework to combat terrorism financing, this framework should evolve to respond to the changing nature of terrorism financing risks.

---

[27] Counter-Terrorism Financing Summit, *The Sydney Communique,* November 2015, http://www.austrac.gov.au/sites/default/files/ctf-sydney-communique-FINAL-PRINT.pdf.
[28] Financial Action Task Force, *The Financial Action Task Force leads renewed global effort to counter terrorist financing*, 14 December 2015, http://www.fatf-gafi.org/publications/fatfgeneral/documents/fatf-leads-renewed-global-effort-to-counter-terrorist-financing.html.
[29] Ministère des Finances et des Comptes Publices, *Countering terrorist financing*, November 2015, http://www.gouvernement.fr/sites/default/files/locale/piece-jointe/2015/12/countering_terrorist_financing.pdf.
[30] Financial Action Task Force, *Terrorist Financing: FATF Report to G20 Leaders – actions being taken by the FATF,* 16 November 2015, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/terrorist-financing-fatf-report-to-g20.html.

Recommendations

Recommendation 2.1

The AML/CTF Act should be simplified to enable reporting entities to better understand and comply with their AML/CTF obligations.

Recommendation 2.2

The AML/CTF Rules should be simplified, rationalised and presented in a user-friendly format to improve accessibility and understanding of obligations.

Recommendation 2.3

The AML/CTF Act and Rules should adopt the technology neutrality principle.

Recommendation 2.4

AUSTRAC should consider further opportunities to provide greater guidance and publish feedback on compliance outcomes and the value of financial intelligence.

Recommendation 2.5

Reforms to the AML/CTF Act and Rules that have a regulatory impact should be co-designed by government and industry.

Recommendation 2.6

A government working group should be established to consider international developments in combating terrorism financing and consider the appropriateness of these measures for the Australian context.

3. Objects of the Act

The objects of an Act fulfil a number of functions, providing a general understanding of the intent of the legislation and setting some high level principles to assist understanding of the legislation itself. Importantly, the objects also play a role in assisting the interpretation of the legislation by the courts.[31]

The objects of the AML/CTF Act are set out in section 3. They have an international focus, relating to fulfilling Australia's international obligations, addressing matters of international concern and affecting Australia's relationships with foreign countries and international organisations beneficially.[32] This includes, but is not limited to, Australia's international obligations to combat money laundering, terrorism financing, corruption, transnational crime and terrorism.

Consultation

Industry stakeholders and partner agencies discussed a range of proposals for amending the objects of the AML/CTF Act.

There was strong support for the inclusion of objects that extend beyond Australia's international obligations and articulate the benefits of a robust AML/CTF regime from a national perspective. In particular, stakeholders and partner agencies supported objects that referred to:

- combating money laundering, terrorism financing and other serious crimes
- collecting the information necessary to detect, deter and disrupt money laundering, terrorism financing and other serious crimes, and
- protecting the integrity of the Australian financial system.

Partner agencies also considered the objects should include combating the financing of the proliferation of weapons of mass destruction (WMDs) (proliferation financing) and supporting the implementation of other United Nations Security Council and Australian autonomous sanctions.

Other stakeholders suggested the inclusion of new objects that relate to the implementation of the AML/CTF Act, rather than the purpose of the legislation. These include enhancing public awareness and understanding of ML/TF, guarding against unnecessary and inefficient regulation that is too complex and measuring effectiveness.

There was also some support for the inclusion of principles to guide the administration of the Act, including principles related to:

- the risk-based approach
- minimising regulatory burden, and
- protecting the privacy of individuals and their personal and financial information.

[31] Section 15AA of the *Acts Interpretation Act 1901* states that "In the interpretation of a provision of an Act, a construction that would promote the purpose or object underlying the Act (whether that purpose or object is expressly stated in the Act or not) shall be preferred to a construction that would not promote that purpose or object."
[32] Section 3 of the AML/CTF Act.

Discussion

Objects

Australia continues to be an active member of the FATF and a signatory to a range of United Nations conventions and resolutions that centre on tackling corruption, terrorism and serious and organised crime. This cooperation at the international level remains integral to combating and disrupting transnational crime. In view of this, compliance with the FATF standards and other international obligations continues to be an important foundation of the AML/CTF Act.

While industry stakeholders and partner agencies acknowledged this foundation, they strongly supported the inclusion of new objects with a domestic focus. These objects relate to:

- detecting, deterring and disrupting money laundering, terrorism financing, and other serious crimes
- providing intelligence, regulatory, investigative and law enforcement agencies with the information and intelligence they need to prevent, detect, deter and disrupt money laundering, terrorism financing and other serious crimes, and
- promoting public confidence in Australia's financial system at the national and international level.

The objects of the AML/CTF Act should be broadened to reflect these matters to guide understanding of the policy intent of the legislation and better assist with the interpretation of specific provisions.

In 2012 the FATF responded to the threat of illicit proliferation of WMDs by revising its mandate to include the development of measures to combat proliferation financing.[33] This recognises the role that AML/CTF regulation and the collection and dissemination of financial intelligence play in combating proliferation financing. The objects should be broadened to reflect this development.

The FATF also issued a new standard in 2012 to specifically target proliferation financing. The FATF standards now require countries to implement targeted financial sanctions (TFS) to comply with the United Nations Security Council Resolutions (UNSCRs) relating to the prevention, suppression and disruption of proliferation of WMDs and their financing.[34] This complemented the existing FATF requirement to implement terrorism and terrorism financing TFS imposed by other UNSCRs.[35] Other UNSCRs imposing TFS and other sanctions measures are also binding on Australia under international law.

Australia implements the UNSC TFS regimes under the *Charter of United Nations Act 1945* and the *Autonomous Sanctions Act 2011*, administered by the Department of Foreign Affairs and Trade (DFAT). A proposal for AUSTRAC to supervise reporting entities for compliance with TFS sanctions and related sanctions measures is discussed in *Chapter 15: Audit, information-gathering and enforcement*. If the Government implements this proposal, the objects of the AML/CTF Act should be amended to include this broader policy objective to support the supervision and monitoring of Australian sanction laws.

Principles

The articulation of legislative principles to complement an expanded set of objects could also assist with the interpretation and administration of the AML/CTF Act.

[33] Financial Action Task Force, *Financial Action Task Force Mandate (2012-2020),* April 2012, http://www.fatf-gafi.org/media/fatf/documents/FINAL%20FATF%20MANDATE%202012-2020.pdf.
[34] FATF Recommendation 7 (Targeted financial sanctions related to proliferation).
[35] FATF Recommendation 6 (Targeted financials sanctions relating to terrorism and terrorism financing).

The risk-based approach is already an important cornerstone of the AML/CTF Act. Inserting the risk-based approach as a principle to guide the administration of the Act would embed this regulatory approach within the regime.

Protecting privacy is also an important principle underpinning aspects of the AML/CTF Act's operation. The AML/CTF regime poses a number of privacy risks and impacts, including the unnecessary collection of personal information and the unauthorised use and disclosure of information. Safeguards and controls are already built into the AML/CTF Act to protect the confidentiality and security of personal and confidential information, including:

- controls that govern access to, and the use of, AUSTRAC information, and
- requirements for businesses that are also reporting entities to comply with the *Privacy Act 1988* when handling personal information collected pursuant to AML/CTF Act obligations.

The inclusion of a principle relating to protecting privacy to guide the administration of the Act would emphasise the importance of these safeguards and controls, and the need for AML/CTF obligations to be implemented in a way that minimises and addresses privacy risks and impacts associated with the collection and handling of personal information.

Recommendations

Recommendation 3.1

The AML/CTF Act should be amended to include objects that relate to the following concepts:

- implementing measures to detect, deter and disrupt money laundering, the financing of terrorism, the proliferation of weapons of mass destruction and its financing and other serious crimes
- responding to the threat posed by money laundering, the financing of terrorism, the proliferation of weapons of mass destruction and its financing and other serious crimes by providing regulatory, national security and law enforcement officials with the information they need to detect, deter and disrupt these crimes
- supervision and monitoring of compliance by reporting entities with Australian sanction laws (subject to consideration in Chapter 15 of this report), and
- promoting public confidence in the Australian financial system.

Recommendation 3.2

The AML/CTF Act should be amended to insert general principles for the administration of the Act that provide for the following:

- AML/CTF obligations under the AML/CTF Act, Rules and Regulations should be proportionate to the ML/TF risks faced by reporting entities
- regulatory, national security and law enforcement agencies should have access to the information they need to detect, deter and disrupt money laundering, the financing of terrorism, the proliferation of weapons of mass destruction and its financing, contraventions of Australian sanction laws and other serious crimes (subject to consideration in Chapter 15 of this report), and
- AML/CTF obligations under the AML/CTF Act, Rules and Regulations should be designed and implemented in a way that minimises and appropriately addresses the privacy risks and impacts associated with the handling of personal information.

4. Regime scope

This chapter considers the scope of the AML/CTF regime established by the designated services listed in section 6 of the AML/CTF Act.

Existing designated services are examined and opportunities explored to extend the scope of the regime to regulate other services that pose a high ML/TF risk. These include:

- services provided by designated non-financial businesses and professions
- transactions involving new payment types and systems, such as digital currencies, and
- services provided to customers in Australia by offshore-based entities.

4.1 Regime scope – Existing designated services

The designated services set out in section 6 of the AML/CTF Act determine the scope of regulation under Australia's AML/CTF regime.

Any person that provides a designated service to a customer is a reporting entity for the purposes of the AML/CTF Act, and is subject to AML/CTF compliance and reporting obligations, and supervision and monitoring by AUSTRAC.

Designated services are prescribed across four tables:

- Table 1: financial services
- Table 2: bullion dealing services
- Table 3: gambling services, and
- Table 4: services specified in the regulations.[36]

The scope of some designated services is narrowed by exemptions and the setting of a monetary threshold.[37]

Consultation

Industry stakeholders representing cash-in-transit (CIT) operators considered that designated services associated with collecting and delivering physical currency pose a low ML/TF risk and should be removed from the AML/CTF regime entirely. Other sectors considered that aspects of other designated services should be exempted from the regime due to the low ML/TF risk they pose.[38]

Stakeholder submissions from the CIT sector also submitted that some threshold transaction reports reported by CIT operators may duplicate reports that arise when the service being provided involves a customer (of the CIT operator) and their nominated financial institution.

Other stakeholders indicated that prescribing specific services as the trigger for regulation creates unnecessary legal complexity and confusion, and asked for this approach to be reconsidered. They also

[36] There are currently no services prescribed under Table 4.
[37] For example, issuing a money or postal order is only a designated service for the purpose of the AML/CTF Act where the value of the order equals or exceeds AUD 1,000 (or another amount if specified in the regulations) (item 27, table 1, section 6 of the AML/CTF Act).
[38] See *Chapter 17: Exemption process* for consideration of this issue.

asked for the phrase 'in the course of carrying on a business' to be recast so that it did not capture entities providing a designated service on a sporadic basis.

One partner agency noted the declining use of traveller's cheques, and questioned whether services associated with traveller's cheques should continue to be regulated under the AML/CTF Act. Another partner agency raised concerns that the services described at Items 14 and 15 of Table 1 (providing a cheque book or similar facility) did not sufficiently cover the ML/TF risks associated with the cashing of cheques as bills of exchange.

The findings of the MER

The MER's findings on the range of designated services listed under section 6 of the AML/CTF Act focused on omissions; in particular, the omission of services provided by DNFBPs.[39] The MER also questioned whether the threshold exemptions applicable to the stored value card designated services were appropriate in light of the ML/TF risks posed by such instruments.

Discussion

Designated services model of AML/CTF regulation

The regulatory framework under the AML/CTF Act is service-based and captures businesses according to the nature of the services they provide rather than the nature of the business that provides that service. The main strength of this approach is that businesses cannot evade AML/CTF regulation by changing the way they characterise the nature of their business.

Stakeholders considered that this approach adds a significant layer of technical and legal complexity to the AML/CTF regime, generating uncertainty. This is evident in the number of definitional issues identified by stakeholders, which indicate that stakeholders find a number of the designated services unclear or confusing.[40]

The complexity of the service-based approach has also led to the inadvertent impost of additional obligations on some businesses that have difficulty interpreting the scope of designated services and determining whether a service they provide is captured or not.[41]

Foreign jurisdictions such as the United Kingdom, Ireland and Canada impose AML/CTF regulation on types of business (for example, banks), rather than on the services being provided (for example, opening a bank account). While these models are less complex, they open up the possibility that business could evade AML/CTF regulation by changing how they label their business. These models also do not capture new entrants who provide high-risk ML/TF services as an adjunct to their main business.[42]

The recommendation made in this report to simplify the AML/CTF Act and Rules should include simplifying the designated services under section 6 of the Act. [43] This simplification, and the development of enhanced guidance by AUSTRAC, should introduce greater clarity for businesses in terms of determining whether or not the services they provide are regulated under the AML/CTF regime.

---

[39] See *Chapter 4.2: Regime scope – Designated non-financial businesses and professions* for consideration of this issue.
[40] For example, the 'factoring' and 'forfaiting' designated services. See *Chapter 19: Definitional issues* for consideration of this issue.
[41] For example, the 'designated remittance arrangement' designated services. See *Chapter 11: Remittance sector* for consideration of this issue.
[42] For example, where a company that predominantly provides telecommunications services starts to provide remittance services.
[43] See *Chapter 2: Overarching issues* for consideration of this issue.

Removal of existing designated services

Two classes of designated services were proposed for deletion from section 6 of the AML/CTF Act on the basis that they pose a low ML/TF risk. These are:

- services provided by CIT operators, and
- services relating to the issuing and cashing of traveller's cheques.

CIT operators

CIT operators are currently captured as reporting entities under the AML/CTF regime because they provide designated services associated with collecting and delivering physical currency.[44] Stakeholders representing this industry strongly supported repealing these designated services from the AML/CTF Act or, at the very least, reducing obligations. These stakeholders argued for this regulatory relief on the basis that CIT services pose a low ML/TF risk and CIT operators are already regulated at the state and territory level through licensing schemes.

The AML/CTF regulation of CIT operators in Australia predates the founding of the FATF, with CIT operators captured under the CTR Act in 1988 as cash dealers on the basis that they deliver currency. CIT operators continued to be captured under AML/CTF regulation under the FTR Act and more recently under the AML/CTF Act.

Since the commencement of Australia's AML/CTF regime, the ML/TF risks posed by businesses that transport cash domestically have not been considered to be high at the international level. There are no inherent ML/TF risks associated with the *domestic* transportation of cash from one place to another by a contractor such as a CIT operator as opposed to the domestic transportation of cash by any other business that transports a person or goods. Moving cash within Australia is not, in itself, a money laundering typology and the FATF standards do not require countries to apply AML/CTF regulation to CIT operators. The physical movement of cash *internationally* across borders is however established money laundering typology.[45] The risks associated with the physical movement of cash internationally are addressed through Australia's cross-border cash reporting regime established in Part 4 of the AML/CTF Act.[46]

In view of the lack of an inherent ML/TF risk, the licensing of CIT operators at the state and territory level, and the potential overlap of CDD and reporting requirements between CIT operators and financial institutions, the collection and delivery of cash should be removed as designated services from the AML/CTF Act. Where CIT operators deposit large amounts of cash into accounts on behalf of a customer, the authorised deposit-taking institution accepting the deposit will still have CDD and reporting obligations in relation to the customer and the transaction. Where cash is physically transported across Australia's borders, the Part 4 cross-border reporting requirements will still apply.

Traveller's cheques

The issuing and cashing of traveller's cheques are currently designated services under the AML/CTF Act.[47] The selling of traveller's cheques is captured under the FTR Act.[48]

The use of traveller's cheques has markedly declined in recent years because of the popularity of the global travel (stored value) card and the global reach of credit and debit cards. There is now only one business

[44] Items 51 and 53, table 1, section 6 of the AML/CTF Act.
[45] Financial Action Task Force / Middle East & North Africa Financial Action Task Force, *Money laundering through the physical transportation of cash*, October 2015, http://www.fatf-gafi.org/publications/methodsandtrends/documents/ml-through-physical-transportation-of-cash.html.
[46] See *Chapter 12: Cross-border movement of physical currency and bearer negotiable instruments* for consideration of this issue.
[47] Items 25 and 26, table 1, section 6 of the AML/CTF Act.
[48] See *Chapter 18: The Financial Transaction Reports Act 1988* for consideration of this issue.

which issues traveller's cheques in Australia and the value of traveller's cheques sold in Australia between 2010 and 2013 decreased by 72 per cent.

While traveller's cheques have been assessed as posing a high ML/TF risk in the past, this ML/TF risk profile may have changed commensurate with the marked decrease in use. AUSTRAC should conduct a risk assessment to inform a decision as to what AML/CTF obligations, if any, should apply to issuing, selling and cashing traveller's cheques, noting that the FATF standards currently require countries to apply AML/CTF regulation to the issuing and managing of traveller's cheques.

Reconsideration of existing designated services

Stored value cards

Issuing and increasing the monetary value of stored value cards (SVCs) are designated services where the monetary value of the SVC is AUD1,000 or above (if value can be withdrawn in cash) or AUD5,000 or above (if value cannot be withdrawn in cash).[49]

While these thresholds were based on a ML/TF risk assessment, the risks associated with SVCs may have changed in recent times. There is increasing evidence that pre-paid SVCs and other financial products that provide low-value, high-volume accessibility and anonymity for individuals are being used to finance terrorism. For example, in the November 2015 terrorist attacks in Paris, there are indications that the terrorists had anonymous prepaid SVCs delivered to them in nearby countries to book hotel rooms.

In light of these developments, AUSTRAC should assess the ML/TF risks associated with SVCs to inform a decision as to whether these thresholds should be maintained. This will also help respond to concerns raised by the FATF in the MER about the appropriateness of these thresholds.[50]

Cheque cashing

The use of cheques is an established method of tax evasion and money laundering.[51]

Cheques are used to pay false invoices and fraudulently inflate business expenses to evade tax obligations. Cheque deposits are then cashed out and the funds returned to the issuer of the cheque. These cheques allow criminals to deposit funds anonymously into third-party bank accounts, hiding the source of the funds, obscuring the connection to criminal entities and concealing any further use of the funds.[52]

While the provision of cheques and chequebook services is a designated service under the AML/CTF Act, the cashing of a cheque is not.[53] This may represent a money laundering vulnerability, particularly where cheques involving large amounts are exchanged for cash using a cheque cashing service provided by an entity that is not regulated under the AML/CTF Act. In view of this, AUSTRAC should assess the ML/TF risks associated with exchanging cheques for cash.

'In the course of carrying on a business'

Industry stakeholders submitted that the phrase 'in the course of carrying on a business' within tables 2 and 3 of section 6 of the AML/CTF Act should be qualified (as it is in table 1) because it unduly extends the scope of the AML/CTF regime.

---

[49] Items 21-24, table 1, section 6 of the AML/CTF Act.
[50] See paragraph a2.7 of the MER.
[51] See case studies 4, 11, 17 in AUSTRAC, *Typologies and case studies report 2013*, 2013, http://www.austrac.gov.au/sites/default/files/documents/typ13_full.pdf.
[52] *Ibid*.
[53] Items 14 and 15, table 1, section 6 of the AML/CTF Act.

Under table 1, a number of services are only captured as a designated service where the service is provided in the course of carrying on a business specifically related to that service. For example, item 10 of table 1 captures supplying goods by way of lease under a finance lease, but only where this service is provided in the course of carrying on a finance leasing business.

In contrast, under tables 2 and 3, the service is captured if it is provided in the course of carrying on any business. For example, the buying and selling of bullion is captured under items 1 and 2 of table 2, where the buying and selling is conducted in the course of carrying on any business. 'Business' is defined broadly under the AML/CTF Act as 'a venture or concern in trade or commerce, whether or not conducted on a regular, repetitive or continuous basis'.[54] The broadness of this definition means that, for example, if an antique dealer who usually buys and sells furniture decides to buy and sell gold coins on a sporadic basis, the antique dealer would be required to have fully compliant AML/CTF systems in place.[55]

Businesses that may provide some designated services incidentally, rather than as part of their core business, should not generally be captured under AML/CTF regulations. This position is consistent with the Replacement Explanatory Memorandum for the AML/CTF Act which states that:

> as a general proposition, designated services are limited to services provided to a customer on the course of carrying on the core activity of a business and to not capture activities which are peripheral to the core activity of the business… Some businesses may have more than one core activity and whether an activity is a core activity of the business will be determined by the circumstances of each case.[56]

In view of this, the services currently included in tables 2 and 3 of section 6 of the AML/CTF Act should only apply to services provided by a reporting entity to a customer in the course of carrying on the reporting entity's core activity. The amendments will better target the AML/CTF regime at businesses that routinely provide services that pose a ML/TF risk, and reduce the regulatory burden for businesses that do not. This may reduce the number of reporting entities required to be enrolled with AUSTRAC.

Recommendations

Recommendation 4.1

The AML/CTF Act should be amended to delete the following from table 1 of section 6:

- Item 51 (collecting physical currency, or holding physical currency from or on behalf of a person), and
- Item 53 (delivering physical currency to a person).

Recommendation 4.2

AUSTRAC should conduct an assessment of the ML/TF risks posed by the issuing, selling and cashing/redeeming of traveller's cheques and whether these services should continue to be regulated under Australia's AML/CTF regime.

Recommendation 4.3

AUSTRAC should conduct an assessment of the ML/TF risks posed by stored value cards and the continued appropriateness of the thresholds in the stored value card designated services.

---

[54] Section 5 of the AML/CTF Act.

[55] An antique dealer may, however, be a type of high-value dealer. High-value dealers are proposed for AML/CTF coverage in this review. See *Regime scope – Designated non-financial businesses and professions* for further information.

[56] Sub-clause 6(2), *Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 Replacement Explanatory Memorandum*, http://www.comlaw.gov.au/Details/C2006B00175/Other/Text.

Recommendation 4.4

AUSTRAC should conduct an assessment of the ML/TF risks posed by the services provided by cheque cashing facilities with a view to regulating these services under the AML/CTF Act if they are determined to pose a high ML/TF risk.

Recommendation 4.5

The use of the term 'in the course of carrying on a business' should be qualified for the activities currently within tables 2 and 3 of section 6 of the AML/CTF Act to ensure that only activities routinely or regularly provided by a reporting entity are captured under AML/CTF regulation.

4.2 Regime scope – Designated non-financial businesses and professions

Channels to launder illicit funds and facilitate or disguise criminal activity are not limited to the mainstream financial system.

Transnational and Australia-based crime groups are increasingly making use of professional facilitators or 'gatekeepers' to the financial system, such as lawyers, accountants and trust and company service providers (TCSPs), to set up complex legal structures to disguise and launder criminal wealth.[57] These gatekeepers may be unaware that their services are being exploited by criminals or 'wilfully blind' to the misuse. A small minority of gatekeepers may collude and operate as criminal facilitators.

Criminals can also exploit businesses involved in the buying and selling of high-value assets and goods to conceal the profits of their crime. This includes real estate, artwork, businesses and jewellery.

The FATF has documented the ML/TF risks posed by the services provided by these businesses and professions and require that AML/CTF regulation apply to:

- casinos (when customers engage in financial transactions equal to or above USD/EUR3,000)
- real estate agents (when they are involved in transactions on behalf of clients concerning the buying and selling of real estate)
- dealers in precious metals and stones (when they engage in any cash transaction with a customer equal to or above USD/EUR15,000)
- lawyers, notaries, other independent legal professionals and accountants (when they prepare for or carry out transactions for their client concerning specified activities), and[58]
- TCSPs (when they prepare for or carry out transactions for a client concerning specified activities).[59]

The FATF refers to these businesses and professions collectively as 'designated non-financial businesses and professions' (DNFBPs).[60]

---

[57] Australian Crime Commission, *Organised Crime in Australia 2009*, 2009, p.9, https://www.crimecommission.gov.au/publications/intelligence-products/organised-crime-australia/organised-crime-australia-2009.

[58] The specified activities for which the FATF requires lawyers, notaries, other independent legal professionals and accountants to be subject to AML/CTF regulation are:

- buying and selling of real estate
- managing of client money, securities or other assets
- management of bank, savings or securities accounts
- organisation of contributions for the creation, operation or management of companies
- creation, operation or management of legal persons or arrangements, and
- buying and selling of business entities.

[59] The specified activities for which the FATF requires trust and company service providers to be subject to AML/CTF regulation are:

- acting as a formation agent of legal persons
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons
- providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement
- acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement, and
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

[60] For example, the following FATF publications: *Guidance on the Risk-Based Approach for Accountants*, June 2008, http://www.fatf-gafi.org/documents/riskbasedapproach/fatfguidanceontherisk-basedapproachforaccountants.html; *Money*

Coverage of DNFBPs under Australia's AML/CTF regime

The AML/CTF Act currently imposes obligations on two categories of DNFBPs:

- businesses providing gambling services (which includes casinos), and
- bullion dealers (which are dealers in precious metals).

Gambling services providers in Australia include casinos, gaming machine venues, wagering and sports betting providers and bookmakers. Gambling service providers must apply CDD to customers that hold accounts with the gambling provider and engage in transactions equal to or above AUD10,000, adopt and maintain an AML/CTF program, and report threshold transactions and suspicious matters to AUSTRAC. Gambling service providers licensed by state or territory gaming regulators that operate no more than 15 gaming machines are exempt from most obligations under the AML/CTF regime.

Bullion dealers must perform CDD measures for transactions of AUD5,000 or more, adopt and maintain an AML/CTF program, and report threshold transactions and suspicious matters to AUSTRAC.

Other categories of DNFBPs are only covered when they provide one or more of the designated services listed in section 6 of the AML/CTF Act. This occurs essentially where they are acting in the capacity of a financial institution. However, a number of exemptions apply to solicitors providing some designated services.[61]

Under the FTR Act, solicitors, solicitor corporations and partnerships of solicitors have obligations to submit significant cash transaction reports (SCTRs) to AUSTRAC.[62]

Draft legislation to amend the AML/CTF Act to regulate DNFBPs was released for public comment in August 2007. This was followed by a series of industry roundtables in 2008 and 2009. Further consultation scheduled for 2010 was delayed on the basis that the proposed reforms needed to be balanced against the very immediate needs of business amidst the financial climate of the global financial crisis. The FATF had also commenced the process of revising the FATF standards, which was finalised in 2012.

Coverage of DNFBPs worldwide

In recent years, the coverage of DNFBPs under AML/CTF regulation globally has increased, particularly within the member states of the European Union and in Asia. [63]

Table 1 below provides an overview of the extent to which DNFBPs are regulated under AML/CTF regimes in a selection of countries.

Laundering Using Trust and Company Service Providers, October 2010, http://www.fatf-gafi.org/publications/methodsandtrends/documents/moneylaunderingusing trustandcompanyserviceproviders.html; *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals*, June 2013, http://www.fatf-gafi.org/documents/documents/mltf-vulnerabilities-legal-professionals.html.

[61] For example, a solicitor who, in the course of carrying on a law practice, accepts or makes available money or property transferred under a 'designated remittance arrangement' is currently exempted from the reporting requirements under section 45 of the AML/CTF Act relating to IFTIs.

[62] See *Chapter 18: The Financial Transaction Reports Act 1988* for consideration of this issue.

[63] This follows the implementation of the *Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing*.

TABLE 1: REGULATION OF DNFBPS IN SELECTED COUNTRIES

FATF DNFBP	Australia	United Kingdom	United States	Canada	New Zealand	Hong Kong	Singapore	Malaysia
Casinos	✓	✓	✓	✓	✓	✓	✓	✓
Real estate agents	-	✓	-	✓	✓ (limited)	✓	✓	✓
Lawyers	-	✓	-	-	✓ (limited)	✓	✓	✓
Accountants	-	✓	-	✓	✓ (limited)	✓	✓	✓
Notaries	-	✓	-	✓	-	✓	✓	✓
TCSPs	-	✓	-	✓	✓	✓	✓	✓
Dealers in precious metals and stones	✓ (limited to bullion dealers)	✓	✓	✓	-	-	✓ (limited to pawn-brokers)	✓ (except for jewellers in East Malaysia)

Consultation

The majority of industry stakeholders and partner agencies consulted supported regulating all DNFBPs under the AML/CTF Act to strengthen Australia's AML/CTF regime, relieve the AML/CTF compliance burden shouldered by financial institutions, improve compliance with the FATF standards and better protect the integrity and transparency of the Australian financial system.

The Law Council of Australia (LCA) strongly opposed the AML/CTF regulation of lawyers, arguing that aspects of AML/CTF regulation are inconsistent with the unique role of lawyers. Representatives from the accountancy profession supported the extension of the regime to cover DNFBPs in principle, contingent on there being genuine and thorough consultation with stakeholders, appropriate and reasonable transitional timetables being agreed on, and on the proposals for extending the regime being effective, practical and cost-effective.

Industry representatives from other DNFBP sectors (real estate, jewellers and TCSPs) did not lodge submissions to the review. However, during industry roundtables conducted in 2008 and 2009, a key concern for many of these sectors was the compliance cost that AML/CTF regulation would place on sole practitioners and small businesses. At that time, these sectors sought assurances that staggered implementation and a 'grace period' would apply to the implementation of the reforms, and that regulatory relief would be provided for services with low ML/TF risk.

The findings of the MER

The MER strongly criticised Australia's failure to impose AML/CTF obligations on all DNFBPs (other than casinos and bullion dealers),[64] concluding that the non-regulation of these sectors was having an adverse impact on the overall effectiveness of Australia's AML/CTF regime across several core areas.[65]

The MER recommended that Australia establish comprehensive AML/CTF obligations for the remaining DNFBPs as a matter of priority. The MER also noted that the FATF assessment team was concerned about

[64] The lack of sufficient coverage of DNFBPs led to Australia receiving ratings of 'non-compliant' for FATF Recommendations 22 (Designated non-financial businesses and professions: Customer due diligence) and 23 (Designated non-financial businesses and professions: Other measures).

[65] For example, paragraph 2.20 of the MER noted the use of complex company structures as a major typology for laundering the proceeds of high-risk drug crimes in Australia and the difficulties Australian law enforcement faces in following the money trail and confiscating criminal wealth when these structures are used.

the extent to which non-regulated DNFBPs understood their ML/TF risks. Some DNFBP representatives who met with the FATF assessment team during the on-site visit asserted that the ML/TF risk posed by their respective sectors is low.[66] This assertion was at odds with the findings of the FATF assessment team and is inconsistent with the FATF's wider assessment of the ML/TF risks posed by services provided by the DNFBP sector globally.

Discussion

ML/TF risks and regulatory issues for professionals and corporate service providers

Over the past few years, the FATF has observed a 'trend toward the involvement of various legal and financial experts, or gatekeepers, in money laundering schemes', noting that:

> [t]he most significant [money laundering] cases each involve schemes of notable sophistication, which were possible only as a result of the assistance of skilled professionals to set up corporate structures to disguise the source and ownership of the money.[67]

The FATF considers that these gatekeepers are in a unique position to collect and report information that may be critical in assisting law enforcement to identify ML/TF, and consequently requires they be subject to AML/CTF regulation.

The Australian Crime Commission (ACC) has also observed that organised criminals are exploiting professional services to advise on, and establish, networks of businesses, proprietary companies, partnerships and trusts to facilitate the laundering of illicit income and support criminal activity.[68] The ACC's *Organised Crime in Australia 2015* report notes that organised crime groups are becoming innovative in infiltrating legitimate industries to generate and launder significant criminal profits.[69] This has included setting up businesses within the transport, resources or investment sectors.[70] Using professionals to advise on, establish and conduct transactions relating to these businesses provides the appearance of legitimacy to financial activity linked to criminal controlled enterprises and distances criminals from their illicit activities and funds. This makes tracing illicit funds difficult and time consuming for law enforcement agencies.

The lack of coverage of DNFBPs under the AML/CTF Act has attracted the attention of a number of Parliamentary Committees.[71] The Parliamentary Joint Committee on Law Enforcement recommended in September 2015 that the review consider the extension of AML/CTF regulation to cover DNFBPs as part of its inquiry into financial related crime.[72] The report of the Queensland Organised Crime Commission of Inquiry considered in October 2015 that the AML/CTF Act should be amended to regulate DNFBPs.[73]

---

[66] See paragraph 5.28 of the MER.
[67] Financial Action Task Force, *Laundering the Proceeds of Corruption*, July 2011, p. 19, http://www.fatf-gafi.org/media/fatf/documents/reports/Laundering%20the%20Proceeds%20of%20Corruption.pdf.
[68] Australian Crime Commission, *Organised Crime in Australia 2009*, 2009, p.9, https://www.crimecommission.gov.au/publications/intelligence-products/organised-crime-australia/organised-crime-australia-2009, (accessed 29 July 2015).
[69] Australian Crime Commission, *Organised Crime in Australia 2015,* 2015, https://www.crimecommission.gov.au/sites/default/files/FINAL-ACC-OCA2015-180515.pdf.
[70] *Ibid*, p. 7.
[71] See the discussion on 'real estate' below for consideration of the House of Representatives Standing Committee on Economics' *Report on Foreign Investment in Residential Real Estate.*
[72] Parliamentary Joint Committee on Law Enforcement, *Inquiry into financial related crime*, September 2015, http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/Financial_related_crime/Report.
[73] Queensland Organised Crime Commission of Inquiry, *Report* ,October 2015, https://www.organisedcrimeinquiry.qld.gov.au/__data/assets/pdf_file/0017/935/QOCCI15287-ORGANISED-CRIME-INQUIRY_Final_Report.pdf.

Lawyers

In Australia, the increasing complexity and sophistication of money laundering schemes has seen organised crime groups employing the services of lawyers.[74] In particular, criminals may seek out lawyers:

- to complete a certain transaction (for example, the buying or selling of real estate or a business), or
- where specialised legal and notarial skills and services are required (for example, to create a trust or company).

In 2013, the FATF released a typologies report outlining the general ML/TF vulnerability of lawyers based on the specific services they provide.[75] The findings in this report are consistent with AUSTRAC's strategic analysis brief *Money laundering through legal practitioners*, released in June 2015.[76] AUSTRAC's brief examined domestic and international case studies and identified five main methods of money laundering using services provided by lawyers:

- conducting transactions on behalf of clients
- using lawyers' trust or investment accounts
- recovering fictitious debts
- facilitating the buying and selling of real estate, and
- establishing corporate structures.[77]

The buying and selling of real estate, for example, is an established money laundering method that usually involves the services of a conveyancer or solicitor. Where criminals engage a solicitor for these transactions, the criminals can use other services provided by the solicitor to further conceal the illicit funds, including:

- establishing complex loan and other credit arrangements in relation to the property
- transferring the ownership of property to nominees or third parties
- establishing and maintaining domestic or offshore legal entity structures, for example, trusts or companies, to own the property, or
- receiving and transferring large amounts of cash.[78]

Lawyers' trust accounts have also been identified as being vulnerable to misuse for ML/TF purposes, as criminals can pass their illicit funds through trust accounts and into the financial system and attract less scrutiny from financial institutions, as case study 1 demonstrates.[79]

The AML/CTF regulation of lawyers aims to ensure that lawyers are aware of and understand the ML/TF risks posed by the services they provide and take steps to manage and mitigate those risks. The information lawyers gather under this regulation can assist law enforcement to identify ML/TF, particularly where a lawyer has lodged a report to the authorities because the information provided by his or her customer, or aspects of a transaction or business relationship, raises suspicions.

---

[74] Australian Crime Commission, *Professional Facilitators of Crime*, July 2013, https://www.crimecommission.gov.au/publications/intelligence-products/crime-profile-fact-sheets/professional-facilitators-crime.
[75] Financial Action Task Force, *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals*, June 2013, http://www.fatf-gafi.org/topics/methodsandtrends/documents/mltf-vulnerabilities-legal-professionals.html.
[76] AUSTRAC, *Money laundering through legal practitioners,* June 2015, http://austrac.gov.au/money-laundering-through-legal-practitioners.
[77] *Ibid.*
[78] AUSTRAC, *Money laundering through real estate*, 2015, http://www.austrac.gov.au/sites/default/files/sa-brief-real-estate.pdf.
[79] AUSTRAC, *Money laundering through legal practitioners,* 2015, http://www.austrac.gov.au/sites/default/files/sa-brief-legal-practitioners.pdf.

The LCA strongly opposes AML/CTF regulation of the legal profession in Australia on a number of grounds, arguing that:

- some AML/CTF obligations are fundamentally incompatible with the role of legal practitioners within the justice system and would particularly impact on legal professional privilege
- the cost and burden of additional further regulation is undesirable and unjustifiable, particularly on smaller law practices and sole practitioners, and
- making legal practitioners less susceptible to inadvertent or unintentional involvement in ML/TF activities is best achieved through the existing regulatory scheme for legal practitioners and by raising awareness and providing guidance.[80]

The LCA noted in its submission to the review that the legal profession in Australia is already subject to a regulatory system and has core professional obligations, including a professional obligation not to break or facilitate breaching of the law. The LCA considers that the existing regulatory scheme is functioning well, and distinguishes the legal profession from other DFNBPs:

> As officers of the court with special privileges (such as client legal privilege) and special responsibilities to the administration of justice, the courts, clients and the profession as a whole, the role of lawyers is unique. Lawyers distinctively must counsel clients fearlessly and frankly about legitimate behaviours in any aspect of the law, but may not induce clients to breach the law or to facilitate breaching the law. A lawyer who does so is liable to criminal prosecution as well as the full force of the legal professional regulatory sanctions. These obligations and requirements mirror the heart of the policy intent of the AML/CTF scheme. The imposition of an additional regulatory structure is not warranted or necessary, given the broad equivalence of the existing regulatory sub-structure with Australia's FATF obligations.[81]

However, it will not always be apparent to a lawyer that their services are being misused to facilitate breaching of the law, as their regulatory obligations do not require them to 'look behind' a transaction or a service. Lawyers are not required to identify and verify their clients, conduct CDD, question the source of funds or monitor transactions in line with the FATF standards. Under the FTR Act, solicitors are required to collect information about the customer when submitting a significant cash transaction report and guidance from various professional bodies advises lawyers to collect key information about clients. However, there is no broad requirement for them to verify key information about customers (even if, under specific circumstances, they may be required to collect it).

Without taking these steps, a lawyer may never know the true identity of their clients or whether there is something unusual or untoward about a transaction or a service. This impedes the ability of law enforcement to 'follow the money trail' as they investigate ML/TF and other serious offences that may involve the use of services provided by lawyers to obscure the illicit origins of funds.

Lawyers in England and Wales are subject to AML/CTF obligations and supervised for compliance with these AML/CTF obligations by the Solicitors Regulation Authority (SRA), an independent regulatory body created by the United Kingdom Law Society. Between October 2013 and September 2014, lawyers lodged 3,610 suspicious activity reports with the SRA.[82]

The following case studies published by the SRA illustrate the role lawyers play in detecting money laundering by monitoring transactions for 'red flags' and lodging suspicious activity reports.

---

[80] Law Council of Australia, *Statutory review of the Anti-money laundering and counter-terrorism financing regime in Australia*, April 2014, http://www.ag.gov.au/Consultations/Pages/StatReviewAntiMoneyLaunderingCounterTerrorismFinActCth2006.aspx.
[81] *Ibid,* p. 4.
[82] National Crime Agency, *2014 SARs Annual Report,* July 2015, http://www.nationalcrimeagency.gov.uk/publications/464-2014-sars-annual-report/file.

CASE STUDY 1: CLIENT ASKS WHETHER TO ACCEPT CASH PAYMENT FOR PROPERTY[83]

Mrs A was a sole practitioner acting on behalf of a client who was the vendor in a property transaction. The client had been using Mrs A's services for property matters for more than 20 years and called Mrs A to ask her if he was able to accept GBP50,000 cash as part payment for a house. The client explained that the buyer had made an offer of GBP150,000. This included GBP100,000 that he had in savings, but he had also won a large sum of money on a horse race and so was able to pay GBP50,000 in cash. Mrs A advised her client not to accept this payment, as she knew that cash payment was a key money laundering red flag. She also told her client that it contravened regulations for the cash payment to be held in her client account. The client did not continue with the sale and Mrs A made a suspicious activity report.

Some months later, the individual who had tried to purchase the property was convicted of drug related crimes, and it emerged he had been trying to launder proceeds through the purchase of property.

CASE STUDY 2: SUSPICIOUS PAYMENTS IDENTIFIED IN BANK STATEMENT REVIEW[84]

Firm B was acting for a client in a purchase of an apartment. To check source of funds, the firm had requested six months of bank statements as part of their 'know your client' procedures. When Mr C, an associate at Firm B, checked the statements, he noticed that the client had no money coming into his account at all for two months, and then very large regular deposits coming in the following months. The large deposits were from a company, XYZ Biz. Mr C could not find any details of XYZ Biz when he did an internet search. The client had not previously mentioned XYZ Biz and had given no indication that there would be anything irregular in the statements.

Mr C reported the irregularity to Firm B's money laundering reporting officer who examined the bank statements himself and subsequently made a suspicious activity report, detailing the payments and the lack of information available on XYZ Biz. Soon after the report, the police contacted Firm B requesting the client's file. It later emerged that the client had bought a number of properties as premises in which to grow cannabis. XYZ Biz was a shadow company set up by the client to try to disguise the proceeds of his criminal activity as payment for legitimate work.

In 2012, the SRA spoke to 100 randomly-selected conveyancing firms in 2012 and found that one in four had experienced attempted money laundering or fraud.[85] The majority of these instances were uncovered when a customer attempted to avoid or cheat identity checks.[86]

A primary concern for the legal profession worldwide is the impact that AML/CTF obligations may have on client confidentiality and legal professional privilege. Legal professional privilege is a rule of law protecting a class of communications between lawyers and their clients relating to civil and criminal proceedings from disclosure.

In Australia, industry stakeholders representing the legal profession contend that any obligation for lawyers to report suspicious matters to AUSTRAC could compel lawyers to compromise their legal professional privilege obligations. The profession maintains this view notwithstanding that section 242 of the AML/CTF Act provides that the Act does not affect the law relating to legal professional privilege.[87] However, there will be circumstances where a communication between a lawyer and client is clearly confidential, but does not fall within the ambit of legal professional privilege. Under AML/CTF regulation, these communications would be subject to the AML/CTF Act.

[83] Solicitors Regulation Authority, *Cleaning up: Law firms and the risk of money laundering*, 2014, p. 14, http://www.sra.org.uk/risk/resources/risk-money-laundering.page.
[84] *Ibid,* p. 15.
[85] Solicitors Regulation Authority, *Conveyancing thematic study: Full report*, March 2013, http://www.sra.org.uk/sra/how-we-work/reports.page.
[86] *Ibid.*
[87] This protection is consistent with the FATF standards, which provide that legal practitioners are not required to report suspicious transactions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege.

Outside the scope of legal professional privilege, a suspicious matter reporting obligation for a lawyer regulated under the AML/CTF Act is likely to arise in circumstances where performance of the requested service or transaction for the customer involved may be at odds with the codes of conduct and ethical standards for lawyers.[88] This includes a solicitor's paramount duty to the court and the administration of justice, the duty not to engage in dishonest and disreputable conduct and other fundamental ethical duties.

The interaction between legal professional privilege and AML/CTF obligations has presented challenges for some jurisdictions. In February 2015, the Canadian Supreme Court ruled that provisions of Canada's AML/CTF legislation establishing search and seizure powers were unconstitutional to the extent that these provisions applied to lawyers.[89] In particular, the court ruled that these provisions contravened section 8 of the Canadian *Charter of Rights and Freedoms* that provides protection against unreasonable search and seizure.

In this case, the court concluded that the search and seizure powers authorised sweeping searches of law offices which inherently risked breaching solicitor-client privilege. Where such searches occur, a client may not be aware that his or her privilege is threatened and unable to claim privilege. This effectively transferred the burden of protecting solicitor-client privilege to lawyers with no protocol for independent legal intervention. However, the Canadian Supreme Court did suggest that AML/CTF obligations could be imposed if sufficient protections were put in place for legal professional privilege, and the right against self-incrimination.[90]

England and Wales have dealt with the challenge posed by the interface between AML/CTF obligations and legal professional privilege through self-regulation by a legal professional body.

Conveyancers

The process of transferring ownership of a legal title of real estate from one person or entity to another (conveyancing) poses significant ML/TF risks, as real estate is a high-value, growth asset commonly purchased by criminals to benefit from the proceeds of their crimes. The FATF standards recognise these risks and require lawyers and other independent legal professionals who are conveyancers to comply with AML/CTF obligations when they prepare for or carry out transactions for their clients that involve the buying and selling of real estate.[91]

In Australia, a conveyancer is a licensed and qualified professional that does not necessarily have to be a lawyer. In view of this, any proposed AML/CTF regulation of lawyers that provide conveyancing services should include conveyancers that are not lawyers.

Accountants

Accountants' specialised skills and services are vulnerable to misuse by money launderers because of their involvement in conducting and facilitating transactions, managing accounts, client money and assets, creating, operating or managing corporate structures and buying or selling real estate.

Case study 3 highlights the intelligence gap created when accountants, acting as gatekeepers, do not have AML/CTF obligations.

---

[88] Law Council of Australia, *Australian Solicitor's Conduct Rules,* June 2011, https://www.lawcouncil.asn.au/lawcouncil/images/LCA-PDF/a-z-docs/AustralianSolicitorsConductRules.pdf.
[89] *Canada (Attorney General) v. Federation of Law Societies of Canada*, 2014 SCC 7, http://scc-csc.lexum.com/scc-csc/scc-csc/en/14639/1/document.do.
[90] *Ibid*, at [112].
[91] See the discussion of AML/CTF coverage of real estate agents below for further information on the ML/TF risks associated with real estate.

CASE STUDY 3: FALSE IDENTITY USED IN TRUST[92]

In 2014, the Australian Taxation Office (ATO) flagged a set of amended activity statements lodged by an accountant A on behalf of the X Trust, which had resulted in GST refunds being paid. The ATO auditor attempted to contact the principal behind the X Trust but, after making enquiries, the auditor was unable to contact the principal and determined that the principal's identity was probably fabricated. This led to scrutiny of A, being the only known individual associated with the refund claims.

Ultimately, the ATO decided not to proceed with a criminal investigation and a Tax Practitioners Board investigation cleared A of any breach of his obligations as a tax agent.

As accountants do not currently have AML/CTF obligations, A was not legally required to undertake CDD and identify and verify the principal's identity. If A had attempted to perform CDD, A may have discovered that the principal's identity was fabricated, disrupting the principal's potentially illicit activities and protecting A's business from misuse.

As a result of his association with the X Trust, A and his other clients are now on an ATO watch list.

The above case study also illustrates how trust structures can be used to obscure the ultimate beneficial owner of assets, particularly where professionals conducting transactions on behalf of the trust have no legal obligation to conduct CDD or report suspicious transactions.

During industry consultations conducted in 2008 and 2009, the Institute of Chartered Accountants of Australia[93] and CPA Australia expressed concerns about how the imposition of AML/CTF obligations on accountants would impact on the professional relationship between accountants and their clients, particularly in relation to client confidentiality. However, the principle of client confidentiality is observed by many industries, including those already subject to the AML/CTF Act. Banks and other financial institutions are subject to the full range of AML/CTF obligations and have developed systems that enable them to comply with their reporting obligations with minimal impact on client confidentiality.

Trust and company service providers

TCSPs assist in the creation, operation and management of corporate and trust structures, providing an important link between financial institutions and their clients. The use of TCSPs to launder illicit funds is an internationally established money laundering method, as they have a number of characteristics that make them vulnerable to misuse for ML/TF purposes.[94] Information on the sources and uses of client funds and legal beneficial ownership information can be concealed with relative ease using TCSPs through the establishment of multiple accounts and the conduct of complex transactions on behalf of clients.[95]

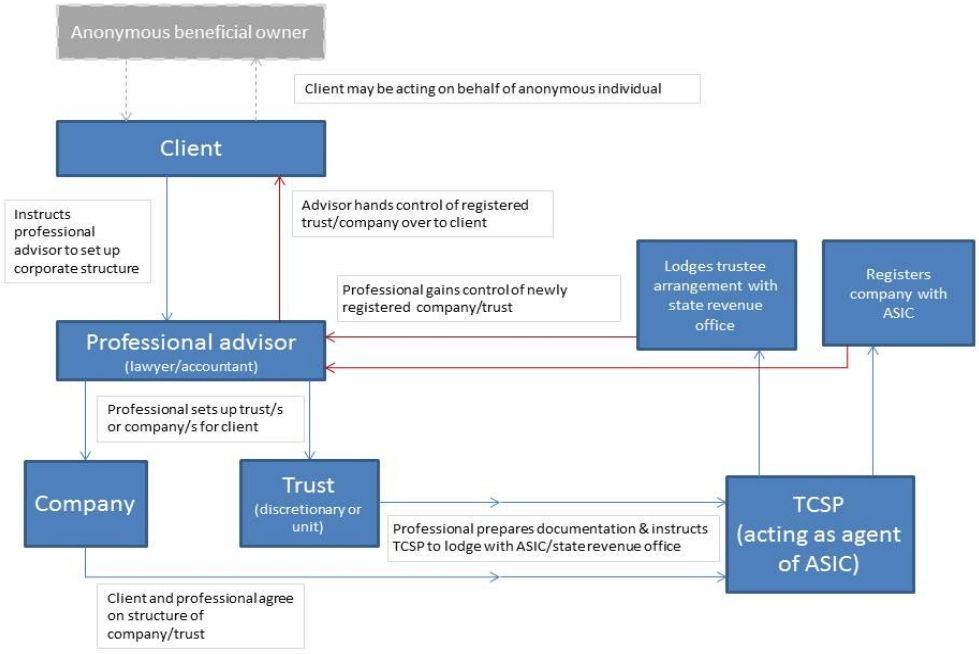
In Australia, the majority of companies that are registered with the Australian Securities and Investments Commission (ASIC) are established through TCSPs specialising in company registration and the establishment of trusts. The clients of these TCSPs are often not the companies themselves, but lawyers and accountants acting on the behalf of their clients. Once registered, companies can still rely on TCSPs to fulfil the ASIC obligations. While this registration process, and other state and territory registration processes,[96] allow for basic information to be collected, these processes do not ensure that accurate and up-do-date information on the beneficial owners of companies is readily available.

[92] Source: Australian Taxation Office.
[93] Renamed Chartered Accountants Australia New Zealand in 2013.
[94] Financial Action Task Force, *Money laundering using trust and company service providers*, October 2010, http://www.fatf-gafi.org/topics/methodsandtrends/documents/moneylaunderingusingtrustandcompanyserviceproviders.html.
[95] *Ibid*, p. 36.
[96] For example, registers are maintained by state and territory authorities in relation to the creation of incorporated and limited partnerships, incorporated associations and cooperatives.

Even less information is available about legal arrangements such as trusts and the beneficial owners of these legal arrangements.[97]

Diagram 1 below demonstrates the chain of services that can distance the TCSP from the actual customer.

DIAGRAM 1: EXAMPLE OF A TCSP CHAIN OF SERVICE



AML/CTF regulation of TCSPs in Australia would ensure that accurate and up-to-date information is readily available to law enforcement on:

- the beneficial owner of assets
- the source of assets, and
- the business objective of the company or a trust within a structure.

AML/CTF regulation would also allow TCSPs to report to AUSTRAC any suspicions that funds from criminal activities were being 'layered' within the financial system. This includes, for example, transactions where:

- complex and opaque legal entities and arrangements are used
- prospective clients use nominee agreements to hide from the TCSP the beneficial ownership of client companies
- a trust account is opened and then receives multiple cash deposits
- a trust account is opened with large amounts, inconsistent with the client's profile
- a trust account is opened with funds originating from foreign banks
- multiple trusts accounts are opened with the same beneficiary, and
- a natural person opens multiple trust accounts with different businesses declared upon each opening.

[97] See *Chapter 5: Customer due diligence* for consideration of this issue.

ML/TF risks and regulatory issues for dealers in high-value goods and assets

High-value dealers

The buying and selling of high-value goods (such as jewellery, art and luxury cars) is recognised internationally as a major avenue for money laundering activity. These goods can be readily purchased and sold, often using cash. Criminals can use these goods to improve their lifestyle and later sell them for a capital gain as they improve their value over time.

The money gained from this process can then be reinvested elsewhere, obscuring the origins of the illicit cash used for the original transaction.

Small, high-value goods such as jewellery and designer handbags are particularly easy to purchase for cash, move around and later sell without attracting attention. Cars and boats are also attractive to criminals as their high-value allows large amounts of proceeds of crime to be laundered. These goods are also desirable to consumers.[98] The ML/TF risks posed by the buying and selling of real estate as a high-value good are discussed separately below.

AUSTRAC's has rated high-value goods as posing a high ML/TF threat.[99] In 2014-15, the AFP's Criminal Assets Confiscation Taskforce restrained over AUD247 million worth of illicit assets, of which over AUD213 million worth was real estate and other high-value commodities.[100]

Case study 4 below provides an example of an investigation conducted by the New South Wales Crime Commission that uncovered the purchase of high-value goods with illicit funds.

CASE STUDY 4: HIGH-VALUE GOODS (OPERATION SCHOALE)[101]

In 2006, the New South Wales Crime Commission commenced an investigation into the suspected involvement of two men in the importation and distribution of between 300 and 500 kilograms of cocaine in 2005 and 2006. During the course of the investigation, New South Wales Police and the Crime Commission executed a number of search warrants, during which 17 firearms, two kilograms of cocaine and around AUD18 million cash were recovered.

Financial analysis relating to one of the offenders and his wife identified serious discrepancies between the couple's reported taxable income and their expenditure on high-value goods. In the six years prior to her arrest, for instance, the wife declared income averaging AUD66,247 per annum, yet funded the acquisition of a large property for AUD1.3 million and a Mercedes Benz for approximately AUD300,000, and spent AUD607,511 cash on home decorations (including AUD900 on a gold-plated toilet roll holder), AUD470,640 in cash for designer jewellery and AUD45,340 on two watches. Extensive landscape gardening at the property was also funded with crime-derived cash.

At the conclusion of the investigation, the Crime Commission sought and received confiscation orders for the property. The wife was convicted on charges of dealing with the proceeds of crime (totalling around AUD4.6 million), perverting the course of justice, conducting financial transactions so as to avoid reporting obligations, and knowingly giving false evidence before the Crime Commission.

While the FATF standards only require dealers in precious metals and stones to be subject to AML/CTF regulation, FATF member countries have imposed AML/CTF regulation on dealers of other high-value goods

[98] Motor vehicle dealers currently have limited AML/CTF obligations under the FTR Act. See *Chapter 18: The Financial Transaction Reports Act 1988* for consideration of this issue.
[99] AUSTRAC. *Money laundering in Australia 2011*, 2011, http://www.austrac.gov.au/publications/corporate-publications-and-reports/money-laundering-australia-2011.
[100] Australian Federal Police, *Annual report 2014-15,* 2015, http://www.afp.gov.au/~/media/afp/pdf/a/afp-annual-report-2014-2015.pdf.
[101] Source: New South Wales Crime Commission.

because of the ML/TF risks posed by the services they provide. The extent of this coverage varies from jurisdiction to jurisdiction.[102] Australia already regulates bullion dealers under the AML/CTF Act.[103]

Real estate

Real estate can be an attractive channel for criminals wishing to launder illicit funds for a number of reasons. Criminals can purchase a property using large sums of cash, live in the property, renovate the property (using illicit cash) to improve its value and sell the property at a later date for a capital gain. The ultimate beneficial ownership of real estate can also be easily concealed.[104]

The increase in value of the Australian real estate market in recent years has increased the attractiveness of Australia as a location in which to invest illicit wealth, with high-value properties offering ideal opportunities to launder large volumes of illicit funds. This is particularly the case in the aftermath of the global financial crisis as Australia, with its relatively stable economy, is seen as a country in which it is 'safe' to invest or hide criminal wealth.

AUSTRAC released a strategic brief in 2015 that highlights some common methods of money laundering through real estate, including:

- the use of third parties to buy properties
- the use of loans and mortgage (for example, criminals take out a mortgage to buy a property and pay back the mortgage using lump sum cash payments)
- manipulating property values (that is, criminals buy and sell real estate at a price above or below market value)
- structuring cash deposits to buy real estate (that is, criminals deposit cash below the reporting threshold of AUD10,000 at different banks and then use these deposits to obtain a bank cheque to buy a property)
- buying and leasing properties, but providing the tenant with illicit funds to pay the rents
- buying a property using illicit funds with the intention of conducting further criminal activity at the property, and
- using illicit funds to renovate properties.[105]

Instances have been identified in Australia where real estate agents have taken large cash payments for tenancies over properties (some of which have later been used for criminal purposes, such as drug laboratories or for the storage of guns or drugs), as deposits for the sale of property, or as cash bonuses to the vendor in exchange for a lower contract sale price. The latter involves real estate agents facilitating stamp duty fraud. Stamp duty fraud can also be facilitated when the purchaser secretly pays additional funds to the vendor after the sale of the property has been settled, as case study 5 demonstrates.

[102] For example, the United Kingdom defines a high-value dealer as a business which accepts cash payments of EUR15,000 or more (or equivalent in any currency) in exchange for goods. The United Kingdom considers the following businesses are likely to be high-value dealers: motor dealers, jewellers, antique and fine art dealers, boat dealers, builders, bathroom and kitchen suppliers and auctioneers and brokers. See HM Revenue & Customs' website for further information: https://www.gov.uk/money-laundering-regulations-high-value-dealer-registration, (accessed 15 January 2016).
[103] See Table 2, section 6 of the AML/CTF Act.
[104] AUSTRAC, *Strategic analysis brief: Money laundering through real estate*, 2015, http://www.austrac.gov.au/sites/default/files/sa-brief-real-estate.pdf.
[105] *Ibid*, pp. 7-10.

CASE STUDY 5: MISSING STAMP DUTY LED AUTHORITIES TO UNCOVER LARGE-SCALE COCAINE IMPORTATIONS[106]

Law enforcement initiated a joint-agency investigation into cocaine distribution. Agencies were made aware that a key suspect had recently purchased a home for more than AUD1 million, from two known associates. The purchase was partially financed through a series of structured cash deposits totalling approximately AUD385,000.

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

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

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

A total of 13 people were arrested and charged with offences relating to possession of drugs, firearms and money laundering. In addition, AUD13.5 million in cash, two kilograms of cocaine, 17 firearms, a number of prestige cars and a house were seized. Seven of the 13 persons arrested were sentenced to jail for periods ranging from five to 30 years. Four persons, who assisted the key syndicate members in laundering the proceeds of crime, received good behaviour bonds.

There are other conditions that make the investment of illicit funds in Australian real estate attractive, including the lack of AML/CTF regulation of DNFBPs that facilitate real estate transactions, which lowers the risk that the identity of the client or the source of the funds will be questioned, and eliminates the risk that the transaction will be reported to AUSTRAC.[107]

Recently there has been significant attention on the purchase of real estate in Australia by foreign purchasers seeking to conceal their identity. The House of Representatives Standing Committee on Economics examined this issue in 2014 and recommended that the Government consider the purchase of residential property by foreign investors as a possible area of investigation for this review.[108]

Addressing the ML/TF risks posed by DNFBPs

The non-regulation of DNFBPs under the AML/CTF Act generates a significant gap in Australia's AML/CTF regime that provides opportunities for criminals to misuse DNFBP services to launder illicit funds, as case study 6 demonstrates.

---

[106] AUSTRAC, *Typologies and case studies report 2012,* 2012, case study 9, www.austrac.gov.au/typologies-2012-case-studies-account-deposit-taking#Case09, (accessed 15 January 2016).

[107] A national regulatory framework has been developed for electronic conveyancing. This framework consists of the Electronic Conveyancing National Law, which commenced on 1 January 2013 in New South Wales, and has been replicated in the other participating jurisdictions. The electronic conveyancing system has provision for CDD processes which may overlap with proposals for conveyancers to be subject to CDD requirements as part of AML/CTF obligations. See the Australian Registrars National Electronic Conveyancing Council's website for further information: http://www.arnecc.gov.au/home, (accessed 18 August 2015).

[108] Recommendation 11, House of Representatives Standing Committee on Economics, *Report on Foreign Investment in Residential Real Estate,* 2014, http://www.aph.gov.au/Parliamentary_Business/Committees/House/Economics/Foreign_investment_in_real_estate/Tabled_Reports.

CASE STUDY 6: USE OF A RANGE OF DNFBPS BY A CRIME SYNDICATE TO LAUNDER ILLICIT FUNDS[109]

A crime syndicate made significant profits by purchasing bulk amounts of cannabis in one state and then selling the drugs in another state. As a cover for its illicit activities, the syndicate established what appeared to be a transport company and used a company truck to traffic the cannabis interstate.

The syndicate used four methods to launder its illicit profits.

- They employed a company that specialised in processing wages to pay them a wage from their new transport company. The cash proceeds from the cannabis sales were deposited into the transport company's account and transferred to the wage processing company for payment as wages.
- They created trust accounts and investment companies, giving an accountant AUD100,000 of illicit funds to purchase shares in the name of the trust accounts and investment companies.
- One syndicate member purchased a property worth more than AUD700,000 in a family member's name, financing the purchase using a mortgage. Over a two-month period the syndicate member paid more than AUD320,000 in 16 illicit cash deposits to their solicitor (who provided conveyancing services and acted on behalf of the syndicate member in the transaction) to pay off the mortgage on the property.
- Syndicate members invested their criminal profits to purchase high-value goods and support a lavish lifestyle.

Reporting entities submitted two reports to AUSTRAC detailing the suspicious activities of the syndicate. These reports identified one member of the syndicate making multiple cash deposits into their account in amounts just below the AUD10,000 cash transaction reporting threshold. On occasions these deposits occurred on the same day but at different bank branches. The syndicate member explained to bank staff the funds were to purchase a home but could not explain the source of the funds. AUSTRAC referred the reports to law enforcement and also prepared a financial intelligence report detailing the wider financial transactions undertaken by members of the syndicate and associated companies and trust accounts, which supported existing law enforcement intelligence. Law enforcement confiscated approximately AUD600,000 worth of assets that were proceeds of crime. Two members of the syndicate pleaded guilty to multiple money laundering and drug trafficking charges and both were sentenced to six years imprisonment.

The extension of the AML/CTF regulation to the remaining DNFBPs would deliver a number of substantial benefits:

- a current regulatory 'blind spot' would be removed and a broader range of information collected and reported to AUSTRAC, and shared with law enforcement
- suspicions about transactions would be reported earlier in the transaction chain than occurs currently, providing earlier opportunities for law enforcement to disrupt criminal activity, and
- more accurate information about the beneficial ownership of funds and assets would be collected when complex legal structures are first established.

This extended information base would allow AUSTRAC to generate financial intelligence to better assist law enforcement to 'follow the money', tackle serious and organised crime and protect Australia's national security. Australia would also become more hostile to ML/TF threats, enhancing the integrity and credibility of Australia's financial institutions and financial system, bolstering the attractiveness of Australia as a place to conduct business and more strongly aligning the AML/CTF regime with the FATF standards.

Any business added as a reporting entity under the AML/CTF Act would need to bear the initial costs associated with implementing AML/CTF systems and controls, and ongoing costs to maintain those systems and controls. However, extending regulation would relieve some of the regulatory burden on current reporting entities, who could rely on CDD conducted by DNFBPs.[110]

[109] Source: AUSTRAC.

[110] See *Chapter 5: Customer due diligence* for further information on the concept of 'reliance'.

The AML/CTF regulation of DNFPBs would also have a significant impact on AUSTRAC's resources, as the regulated population under the AML/CTF regime would increase substantially. This would requiring AUSTRAC to monitor and supervise tens of thousands more businesses, and pose potential privacy risks and impacts, as numerous DNFBPs would be collecting and handling additional personal information.[111]

In view of these impacts, options for regulating lawyers, accountants, high-value dealers, real estate agents and TCSPs under the AML/CTF Act should be explored in consultation with industry.

Options could include:

- applying all existing AML/CTF obligations under the AML/CTF Act to DNFBPs
- applying some of the existing AML/CTF obligations under the AML/CTF Act to DNFBPs (that is, 'light touch' regulation), or
- establishing self-regulation of DNFBP sectors by relevant industry bodies.

The costs and benefits of adopting these options should be carefully considered to ensure any proposed regulatory measures strike an appropriate balance between mitigating ML/TF risks and supporting the efficient conduct of business. The implementation of any AML/CTF obligations for these businesses should also be staggered to assist affected businesses with the transition towards becoming a reporting entity.

Recommendations

Recommendation 4.6

The Attorney-General's Department and AUSTRAC, in consultation with industry, should:

a) develop options for regulating lawyers, conveyancers, accountants, high-value dealers, real estate agents and trust and company service providers under the AML/CTF Act, and

b) conduct a cost-benefit analysis of the regulatory options for regulating lawyers, accountants, high-value dealers, real estate agents and trust and company service providers under the AML/CTF Act.

[111] Paragraph 5.5 of the MER notes that there are approximately 56,000 legal practitioners, 35,019 real estate agents and 300 company formation agents in Australia.

4.3 Regime scope – Payment types and systems

The global payments landscape has changed significantly since the passage of the AML/CTF Act in 2006. This rate of change will continue, and probably accelerate, as new payment types and systems become more innovative and grow in popularity and uptake.

Despite these changes at the global level, mainstream payment systems continue to dominate Australia's payments landscape. These include:

- cash
- cheque
- direct entry (that is, electronic funds transfers)
- credit, debit and stored value cards,[112] and
- international payments (wire transfers/SWIFT).

The use of cash remains widespread but has begun to plateau in recent years due to the rise of contactless payment systems for credit and debit cards. While the use of cheques as a payment system has significantly decreased over the last ten years, there has been a significant increase in the use of both debit and credit cards. Direct entry payment systems, such as direct debits from a customer's bank account and payments sent to customers' bank accounts, now account for a greater value of transactions in Australia than all the other payment systems combined. There has also been a steady increase in international payments year-on-year.[113]

The introduction of the New Payments Platform (NPP) in 2017-18 will be a significant change. The NPP is aimed at low value payments and will provide the ability to make near real-time direct credit payments, with immediate application in inter-bank fund transfers.[114]

While the AML/CTF Act was drafted with the intention of being flexible and responsive to these new and emerging technologies, there are some gaps relating to coverage of new payment types and systems under the AML/CTF regime.

Consultation

Industry stakeholders and partner agencies strongly supported the inclusion of all new payment types and systems that pose a level of ML/TF risk under AML/CTF regulation, particularly digital wallets and digital currencies. Stakeholders consider that it was critical that the AML/CTF regime applied equal treatment to all providers of similar products or services to maintain a high degree of competitive neutrality and ensure a 'level playing field'.[115]

[112] Issues in relation to the definitions of credit, debit and stored value cards are discussed in *Chapter 19: Definitional issues*. Issues in relation to the stored value card designated services are discussed in *Chapter 4.1: Regime scope – Existing designated services*.
[113] Reserve Bank of Australia*, The Changing Way We Pay: Trends in Consumer Payments*, June 2014, http://www.rba.gov.au/publications/rdp/2014/2014-05.html.
[114] See *Chapter 6: Reporting obligations* for further information.
[115] See *Chapter 2: Overarching issues* for consideration of technology neutrality.

The findings of the MER

The MER found Australia to be largely compliant with the FATF standard for identifying and assessing the risks of new technologies, as Australia demonstrated that it had assessed ML/TF risks associated with new products and technologies.[116]

The MER also noted that while reporting entities are required to generally identify, mitigate and manage their ML/TF risks, there is no specific obligation to consider the risks posed by new technologies. See *Chapter 7: AML/CTF programs* for a more detailed discussion of this issue.

Discussion

There is significant diversity among emerging payment types and systems, including the digitisation of payment systems and value exchange mechanisms. Digital wallets have been developed to store value and undertake transactions online. Crypto-currencies have also generated significant attention, particularly since the emergence of Bitcoin in 2009.

The dynamic nature and rapid developments associated with new payment types and systems offer opportunities for criminals to exploit these systems for ML/TF and other criminal purposes.

Front-end applications

Front-end applications ('apps') provide a new way for customers to initiate a payment. They typically take the form of a mobile app and provide a user interface that allows customers to make payments through established payment systems, such as bank accounts or card schemes.

Apps do not need to be specifically regulated under the AML/CTF Act because they link to payment systems already regulated under the AML/CTF Act (for example, a bank account). However, as apps develop and evolve, some may play a greater role in providing customers with accounts, rather than just facilitating payments. These accounts could be misused for ML/TF purposes. In view of this, AUSTRAC should monitor developments in this area.

Digital wallets

Digital wallets provide a similar service to transaction accounts provided by financial institutions. They are a virtual holding of value through a unique account that stores a user's personal credentials and financial information electronically to enable commercial transactions (for example, purchasing items online or in-store using a smartphone with near-field communication technology, such as PayWave). They allow funds to be transacted into and out of other wallets or established mechanisms (that is, to/from bank accounts or credit/debit cards).

While various forms of stored value other than transaction accounts have existed for some time (for example, stored value cards), they are typically limited in value and are associated with a physical card.

While the types of accounts and account services that are regulated under the AML/CTF Act are mostly traditional financial products provided by authorised deposit-taking institutions, banks, building societies and credit unions, some digital wallets are considered 'accounts' under the AML/CTF Act and some digital wallet account providers are reporting entities that have AML/CTF obligations. [117]

[116] FATF Recommendation 15 (New technologies).
[117] Account is defined under section 6 of the AML/CTF Act and the designated services relating to accounts are set out in items 1-3, table 1, section 6 of the AML/CTF Act.

Future technological advances may inspire a new class of digital wallet providers that are not captured under the AML/CTF Act, despite providing a service similar to traditional account providers currently captured under the AML/CTF regime (for example, wallets that store digital currency).[118]

To prevent any future regulatory gap from developing, the AML/CTF Act should be amended to clearly bring digital wallets and digital wallet providers under the AML/CTF regime. The definitions of 'purchase payment facility' and 'holder of the stored value' in section 9 of the *Payment Systems (Regulation) Act 1998* provide a useful guide on how this could be achieved.

Digital currencies

Terminology

There is currently no internationally accepted definition of the terms 'digital currency', 'virtual currency' or 'e-currency'.[119] The current practice in Australia is to refer to online currencies as 'digital currencies' so this report will use that terminology.[120]

Digital currencies are an electronic means of transferring, storing and trading value. In contrast to the traditional physical currencies issued by national governments ('fiat currency'), digital currencies are currently only issued by individuals or commercial enterprises and are not recognised as legal tender. However, at least one country (Ecuador) has implemented its own digital currency ('dinero electronicó') and more may follow.[121]

Bitcoin is a type of digital currency and one of the most prominent to emerge globally. Bitcoin is an example of a 'crypto-currency' as it is backed by cryptographic algorithms rather than a physical substance like gold or mainstream currency. It is a decentralised peer-to-peer currency traded digitally. Transactions are facilitated and verified by the network of users, rather than a central issuer (for example, a central bank), and are recorded on a public online ledger (called the 'blockchain').

Digital currencies like Bitcoin can be exchanged for fiat currency and are considered 'convertible digital currencies'. Other electronic payment systems, such as those used in online games or frequent flyer and loyalty programs, cannot be exchanged and are types of 'non-convertible digital currencies'.

Current AML/CTF regulation of digital currencies

The AML/CTF Act does not currently clearly regulate all types of digital currencies or digital currency businesses.

Section 5 of the AML/CTF Act defines money to include 'e-currency', which is defined to be an internet-based, electronic means of exchange that is backed either directly or indirectly by precious metal, bullion or a thing prescribed by the AML/CTF Rules and is not issued by or under the authority of a government body.

The definition of e-currency under the AML/CTF Act does not cover all digital currencies, particularly decentralised crypto-currencies such as Bitcoin, because crypto-currencies are backed by an algorithm

---

[118] See discussion of 'digital currency' below for further information.
[119] For example, the FATF uses the term 'virtual currency'. Financial Action Task Force, *Guidance for a risk-based approach to virtual currencies*, June 2015, http://www.fatf-gafi.org/topics/fatfrecommendations/documents/guidance-rba-virtual-currencies.html.
[120] See, for example, the Senate Economics References Committee inquiry into digital currencies (http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency) and the Productivity Commission report on *Business Set-up, Transfer and Closure* (http://www.pc.gov.au/inquiries/completed/business/report/business.pdf).
[121] Banco Central del Ecuador, B*anco Central expide resolución sobre dinero electrónico,* 2 June 2014, http://www.bce.fin.ec/index.php/boletines-de-prensa-archivo/item/659-banco-central-expide-resolucion-sobre-dinero-electronico.

rather than a physical thing. This means if a reporting entity was to sell over AUD10,000 worth of bullion in exchange for Bitcoin there would be no obligation to submit a threshold transaction report.

There is currently no specific designated service for e-currencies. Other designated services do not clearly cover digital currency businesses either, such as the designated services of exchanging one currency for another (as currency is not defined to include e-currency), or the designated services for transferring money or property as a non-financier as part of a designated remittance arrangement. [122] [123]

Despite these gaps, Australia does have oversight of digital currency transactions when digital currency is exchanged for fiat currencies or vice versa, as these transactions generally intersect with the regulated financial sector. AUSTRAC can receive the following reports from reporting entities:

- international funds transfer instruction reports detailing transfers of fiat currencies between Australian accounts and foreign accounts for the purchase/sale of digital currencies
- threshold transaction reports for cash deposits/withdrawals of AUD10,000 or more to or from the bank accounts of digital currency businesses, and
- suspicious matter reports submitted where reporting entities consider financial activity involving a digital currency business to be suspicious.

Consultation

Industry stakeholders and partner agencies focused primarily on the application of the AML/CTF Act to Bitcoin to illustrate the gaps in the AML/CTF Act's regulation of digital currencies. Stakeholders and partner agencies considered that Bitcoin should be regulated under the AML/CTF Act and made the following suggestions:

- creating a new designated service to include digital currency exchange providers
- creating new designated services to include any business involved in the transfer of digital currencies
- broadening the e-currency definition to include Bitcoin and other digital currencies
- the creation of a new report type to capture all digital currency transactions irrespective of value, and
- requiring digital currency exchanges to be registered similarly to the current requirements for remitters.

The regulation of Bitcoin has been considered in a number of fora in Australia. In August 2015, the Senate Economics References Committee released the report from its inquiry into digital currencies.[124] The Committee supported applying AML/CTF regulation to digital currency exchange providers and recommended the review consider this issue.[125] The Committee noted that some digital currency businesses had already tried to implement AML/CTF obligations, despite not being required to.

The Productivity Commission's report on its inquiry into barriers to business entry and exit considered payment systems regulation in Australia.[126] The Commission recommended that AUSTRAC regulate digital

[122] Item 50, table 1, section 6 of the AML/CTF Act.
[123] Items 31-32A, table 1, section 6 of the AML/CTF Act.
[124] Senate Economics Reference Committee, *Digital currency-game changer or bit player,* 4 August 2015, http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency/Report.
[125] *Ibid,* Recommendation 4.
[126] Productivity Commission, *Business Set-up, Transfer and Closure*, 30 September 2015, http://www.pc.gov.au/inquiries/completed/business/report/business.pdf.

currency businesses for AML/CTF purposes, given the high growth potential of digital currencies, the ML/TF risks and the likely low costs of including them within the regulatory framework.[127]

As part of its FinTech priority statement, the Australian Government noted that applying AML/CTF regulation to digital currencies may facilitate future developments or use of these currencies in the future.[128]

The ATO has also released guidance on the tax treatment of crypto-currencies in Australia, specifically targeted at Bitcoin.[129]

Discussion

Benefits and risks of digital currencies

Digital currencies offer the potential for cheaper, more efficient and faster payments, particularly for transfers around the world. As no transaction fee is involved, transactions can be significantly cheaper. Without a need for a central intermediary (such as a bank) to oversee the process and verify the transaction, the transaction process can be significantly more efficient. Digital currency transactions can occur almost instantaneously around the world, 24 hours a day.

Digital currencies also pose ML/TF risks:

- They allow for greater anonymity than traditional non-cash payment methods. Decentralised systems like Bitcoin do not attach customer names or other customer identification to individual transfers, and the system has no central server or service provider.
- The Bitcoin protocol does not require or provide identification and verification of participants or generate historical records of transactions that are necessarily associated with real world identities.
- Transactions are made on a peer-to-peer basis, avoiding regulated financial systems.
- AML/CTF software to monitor and identify suspicious transactions is only in its nascent stage of development.
- Different components of a digital currency system may be located in different places round the world with different standards of AML/CTF regulation.[130]

These risks are significantly higher for convertible digital currencies. Convertible digital currencies are able to be exchanged and thus transfer value between individuals. Non-convertible digital currencies and exchange mechanisms (for example, frequent flyer and loyalty programs) have limited intersection with the financial system and are limited in their functionality to transfer value. This means it is more difficult for money launderers or terrorism financiers to misuse them.

While digital currencies have undoubted legitimate uses, the transfer of convertible digital currencies can occur without passing through the formal financial sector. This provides another tool for criminals and terrorist financiers to move and store illicit funds beyond the reach of law enforcement and other authorities, and purchase illicit goods and services.

This capacity for misuse by illicit actors was confirmed by AUSTRAC's report *Terrorism Financing in Australia 2014*, which assessed that the potential for anonymity offered by digital currencies made them

---

[127] *Ibid,* Recommendation 9.3.
[128] The Treasury, *Australia's FinTech priorities*, http://fintech.treasury.gov.au/australias-fintech-priorities/, accessed 5 April 2016).
[129] Australian Taxation Office, *Tax treatment of crypto-currencies in Australia – specifically bitcoin*, 18 December 2014, https://www.ato.gov.au/general/gen/tax-treatment-of-crypto-currencies-in-australia---specifically-bitcoin/, (accessed 15 January 2016).
[130] Financial Action Task Force, *FATF Report: Virtual Currencies – Key Definitions and Potential AML/CFT Risks*, June 2015, pp. 9-10, http://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html

attractive for terrorism financing, particularly when the payment system or currency exchange is based in a jurisdiction with a comparatively weaker AML/CTF regime.[131]

Case study 7 demonstrates the use of digital currencies in criminal activity.

CASE STUDY 7: SUSPECT USES DIGITAL CURRENCY FOR DRUG TRAFFICKING[132]

Law enforcement intercepted a number of packages sent to Australia from overseas via the postal system containing cocaine and MDMA. The packages were addressed to the suspect. AUSTRAC information identified that the suspect had sent funds from Australia via banks to a digital currency exchange to purchase digital currency.

The suspect had registered an online account with a black market website, which allowed users to purchase and sell illicit goods and conduct transactions using digital currency. The suspect used this online account to purchase, import and sell illicit drugs.

The suspect was convicted of two charges of importing a marketable quantity of a border controlled drug and one charge of trafficking a controlled drug and possessing a controlled weapon. The suspect was sentenced to three years and six months imprisonment.

International approaches to digital currencies

International approaches to AML/CTF regulation of digital currencies vary across jurisdictions. Some countries consider that digital currencies already fall within their AML/CTF regimes or are seeking to include digital currencies within their AML/CTF regimes. Others have sought to ban digital currencies altogether.[133]

In March 2013, the US Financial Crime Enforcement Network (FinCEN) released interpretive guidance stating that all virtual currency exchanges and administrators are money service businesses and are therefore subject to its AML/CTF registration, reporting, and recordkeeping requirements.[134] This applies to offshore virtual currency exchanges and administrators that do business wholly or substantially in the US. The US has taken enforcement action against virtual currency firms for breaching these obligations.[135]

The New York State Department of Financial Services has released a 'BitLicense' regulatory framework for New York-based digital currency businesses, which includes AML/CTF obligations.[136] The AML/CTF obligations include the requirement to have an AML/CTF program, CDD procedures and suspicious transaction reporting.

In June 2014, Canada amended its AML/CTF law to treat dealers in digital currencies as money service businesses.[137] The amendments mean dealers in digital currency will be subject to requirements relating to AML/CTF programs, record keeping, verification procedures, PEPs, suspicious transaction reporting and registration. The amendments capture entities that have a place of business in Canada and entities that have a place of business outside Canada but who provide services to persons or entities in Canada.

---

[131] AUSTRAC, *Terrorism Financing in Australia 2014*, 2014, http://www.austrac.gov.au/publications/corporate-publications-and-reports/terrorism-financing-australia-2014.

[132] AUSTRAC*, Typologies and case studies report 2014,* 2014, case study 1, http://www.austrac.gov.au/typologies-2014-case-studies-account-deposit-taking#case1, (accessed 15 January 2016).

[133] See the FATF's *Guidance for a risk-based approach to virtual currencies* for further information on how jurisdictions around the world have approached virtual currencies. Financial Action Task Force, *Guidance for a risk-based approach to virtual currencies*, June 2015, http://www.fatf-gafi.org/topics/fatfrecommendations/documents/guidance-rba-virtual-currencies.html.

[134] Financial Crimes Enforcement Network*, Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies, FIN-2013-G001*, 18 March 2013, http://fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf.

[135] See for example, Financial Crimes Enforcement Network, 5 May 2015, *FinCEN fines Ripple Labs Inc. in first civil enforcement action against a virtual currency exchanger,* http://www.fincen.gov/news_room/nr/pdf/20150505.pdf, (accessed 15 January 2016).

[136] New York State Department of Financial Service, 3 June 2015 *NYDFS announces final BitLicense framework for regulating digital currency firms*, http://www.dfs.ny.gov/about/speeches/sp1506031.htm, (accessed 15 January 2016).

[137] Division 19 (Money laundering and terrorist financing) of *Economic Action Plan 2014 Act, No. 1*, http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=6684616&File=347.

In March 2015, the United Kingdom Government proposed regulation of digital currencies to support innovation and prevent criminal use. The United Kingdom intends to apply AML/CTF regulation to digital currency exchanges in the United Kingdom and will further consult with stakeholders on the proposed regulatory approach.[138]

In June 2015, the FATF released guidance on how countries can apply a risk-based approach to address the ML/TF risks associated with virtual[139] currency payment products and services.[140] The guidance suggests that countries should consider applying the FATF standards to convertible virtual currency exchanges, and any other types of institution that act as nodes where convertible virtual currency activities intersect with the regulated financial system. This includes:

- requiring convertible virtual currency exchanges to conduct CDD, keep transaction records, make suspicious transaction reports and include the required originator and beneficiary information when conducting wire transfers
- applying registration/licencing requirements to domestic entities providing convertible digital currency exchange services between virtual currencies and fiat currencies, and
- subjecting domestic entities providing convertible virtual currency exchange services to adequate supervision and regulation.

Conclusion

The ML/TF risks posed by convertible digital currencies such as Bitcoin are significant as the features of digital currencies make them attractive to individuals and businesses who wish to utilise them for both legitimate and illegitimate purposes.

To address these risks, convertible digital currencies should be regulated under the AML/CTF Act. Such regulation would bring Australia in line with other key international jurisdictions and assist the use of legitimise digital currency by businesses concerned about the risks associated in dealing with digital currency businesses.

Accordingly, the AML/CTF Act should be amended to expand the definition of e-currency to include convertible digital currencies not backed by a physical thing. Closed or non-convertible systems should be excluded from this expanded definition. However, these types of systems should be monitored for any future developments or changes in the level of ML/TF risk.

The AML/CTF Act should also be amended to regulate certain activities related to convertible digital currencies including:

- exchanging convertible digital currencies for fiat currency, other digital currencies or physical currency
- providing wallets and account services for convertible digital currencies, and
- providing ATM services for convertible digital currencies.

These new designated services largely represent the nodes where the regulated financial sector intersects with digital currencies. They also represent the digital currency activities that are similar to the services offered by the regulated financial sector which already have AML/CTF obligations. For example, ATM

---

[138] HM Treasury, *Digital Currencies: response to the call for information,* March 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf.

[139] The FATF uses the term 'virtual currencies' to refer to 'digital currencies'. They are assumed to be synonymous for the purposes of this report.

[140] Financial Action Task Force, *Guidance for a risk-based approach to virtual currencies*, June 2015, http://www.fatf-gafi.org/topics/fatfrecommendations/documents/guidance-rba-virtual-currencies.html.

services in Australia are largely only made available to account holders who have been subject to CDD requirements. Similar requirements should be applied to digital currency ATMs.

It is important to note that future regulation must be proportionate to the risks faced and balanced with the potential benefits of digital currencies. If regulation and associated compliance costs are perceived as too great, providers may move offshore to jurisdictions with weaker AML/CTF controls. The proposed reforms should be developed in consultation with the digital currency industry to ensure an appropriate balance is achieved. Future regulation of new payment types and systems will also result in the additional collection and handling of personal information, posing additional privacy risks and impacts.

The application of AML/CTF obligations to offshore digital currency exchange providers is considered in *Chapter 4.4: Scope of the regime – Offshore service providers of designated services ('geographical link').*

Recommendations

Recommendation 4.7

AUSTRAC should closely monitor the ML/TF risks associated with new payment types and systems (including front-end applications), to ensure gaps do not develop in Australia's AML/CTF regime.

Recommendation 4.8

The AML/CTF Act should be amended to ensure that digital wallets are comprehensively captured by AML/CTF regulation.

Recommendation 4.9

The AML/CTF Act should be amended to expand the definition of e-currency to include convertible digital currencies not backed by a physical 'thing'.

Recommendation 4.10

The AML/CTF Act should be amended to regulate activities relating to convertible digital currency, particularly activities undertaken by digital currency exchange providers.

4.4 Regime scope – Offshore service providers of designated services ('geographical link')

Reporting entities providing designated services under the AML/CTF Act are only regulated where the services have a geographical link with Australia. A geographical link is established when:

- the designated service is provided at or through a permanent establishment of the provider in Australia[141]
- the provider is a resident of Australia and the designated service is provided at or through a permanent establishment of the provider in a foreign country (foreign branch), or
- the provider is a subsidiary of a company that is a resident of Australia and the service is provided at or through a permanent establishment of the subsidiary in a foreign country (foreign subsidiary).[142]

The geographical link provides clarity for multi-national businesses about how the AML/CTF regime regulates them and sets practical limitations to enable more effective regulation and enforcement of the regime. However, it limits the extra-territorial reach of the AML/CTF Act, creates an uneven playing field for business and potentially creates loopholes in the regime. This is of particular concern given the rise in online services, which can be based anywhere in the world and offer services in Australia.

Consultation

Generally, both industry stakeholders and partner agencies considered that offshore service providers offering services listed under section 6 of the AML/CTF Act to customers in Australia should be captured by the AML/CTF regime. However, this regulation should not impede growth and innovation in cross-border transaction activities or duplicate comparable AML/CTF requirements across jurisdictions.

A number of industry stakeholders noted that offshore service providers could potentially gain a competitive advantage by basing themselves in jurisdictions with less stringent AML/CTF regimes and reducing their compliance costs if they are not captured under Australia's AML/CTF regime.

The findings of the MER

The MER made no specific findings on this issue.

Discussion

Since the passage of the AML/CTF Act in 2006, there has been marked growth in offshore service providers that provide designated services to customers located in Australia. These include online remittance, [143] digital currency, financial and gambling services providers.

Currently these businesses are not captured under the AML/CTF Act as they do not meet the geographical link test outlined in subsection 6(6).[144]

---

[141] Section 21 of the AML/CTF Act defines a 'permanent establishment' of a person as a place at or through which the person carries on any activities or business, and includes a place where the person is carrying on activities or business through an agent.
[142] Subsection 6(6) of the AML/CTF Act.
[143] There is one exception to the geographical link requirement. It does not apply to remittance network providers (that is, the provision of an item 32A designated service). Online remitters who are not network providers are not however captured.
[144] Subsection 6(6) of the AML/CTF Act. There is one exception to the geographical link requirement. It does not apply to remittance network providers (that is, the provision of an item 32A designated service).

The lack of coverage of these offshore service providers under Australia's AML/CTF regime creates an intelligence gap and allows online businesses to engage in regulatory arbitrage to minimise compliance costs and gain a competitive advantage.

Intelligence gap

Businesses not captured by the AML/CTF Act, such as offshore remittance providers, are generally not required to report to AUSTRAC, although AUSTRAC does have some visibility of transactions conducted by these providers. For example, a number of offshore remittance providers hold Australian bank accounts, and international funds transfer instruction reporting undertaken by the banks provides AUSTRAC with an insight into money flows into and out of Australia. However, the offshore provider often does not report information about the underlying customer of the transaction. This limits the information available for collection and analysis by AUSTRAC and, ultimately, the actionable financial intelligence available for use by AUSTRAC and its partner agencies.

AUSTRAC can also request information about transactions from counterpart FIUs in countries where the providers are based. However, these measures provide limited information and are administratively more cumbersome than traditional reporting. They do not provide a sustainable solution to bridging the intelligence gap.

An issue of particular concern is where an offshore service provider is based in a jurisdiction with weak AML/CTF obligations and/or no capability to share information with AUSTRAC. This will severely restrict visibility of these transactions and effectively provides a regulatory gap which can be exploited for ML/TF purposes.

Regulatory arbitrage

Stakeholders highlighted during the consultation process that the non-regulation of offshore businesses providing services to customers in Australia gave those businesses a competitive advantage. They can provide services at a reduced cost because they do not incur the costs associated with complying with Australian AML/CTF obligations.

Businesses seeking to maximise this competitive advantage could relocate to jurisdictions with the weakest AML/CTF regulation. This situation potentially compounds the regulatory gap and potential for criminal misuse discussed above.

Regulatory options

There are a number of challenges associated with regulating offshore service providers that provide services to customers in Australia. Models should be explored for triggering obligations under the AML/CTF Act for offshore service providers offering services directly to customers in Australia. Options include:

- **A voluntary opt-in model.** Coverage of the AML/CTF Act could be expanded to cover entities that are enrolled with AUSTRAC and provide any designated service. Offshore service providers would register with AUSTRAC on a voluntary basis and subject themselves to the AML/CTF regime to gain consumer confidence in their services. This model would be most effective if the list of entities enrolled with AUSTRAC was made public.[145] Other regulators have adopted similar models using voluntary codes of practice to regulate offshore-based businesses.[146] The obvious shortcoming of such a model is that it would be easily circumvented by those seeking to abuse offshore-based services.

[145] See *Chapter 5: Customer due diligence* for further consideration of this issue.

[146] For example, ASIC administers a voluntary ePayments code of practice to regulate consumer electronic payments, including ATMs, EFTPOS and credit card transactions, online payment, internet and mobile banking, and B-PAY. See ASIC's website for further information: www.asic.gov.au/for-consumers/codes-of-practice/epayments-code/, (accessed 15 January 2016).

- **An opt-in model linked to access to other services.** A variation of the voluntary opt-in model, this model would compel offshore service providers to enrol with AUSTRAC using domestic levers. For example, reporting entities that are financial institutions would be prohibited from holding accounts or conducting transactions with offshore-based businesses that provide designated services to customers in Australia unless the offshore business is enrolled with AUSTRAC.
- **A regulatory model based on marketing to Australian customers.** Under this model, AML/CTF obligations would apply where a designated service is offered/advertised in Australia. This model would need to overcome the practical constraints involved in identifying designated services being offered/advertised to Australian customers. While the *Interactive Gambling Act 2001* has approached this issue by prohibiting online, interactive gambling services being offered/advertised to customers in Australia, there is evidence of illegal offshore gambling operators targeting Australian customers.[147]
- **A regulatory model linked to Australian affiliates of the offshore service providers.** This model already operates under the AML/CTF regime and applies to remittance network providers (RNPs). RNPs are generally located offshore and do not provide designated services directly to customers in Australia. However, they operate a remittance network service through affiliates that have permanent establishments in Australia and provide designated services directly to customers in Australia. The geographical link test does not apply to RNPs and they must be registered with AUSTRAC before providing a remittance network service to affiliates in Australia.[148] Once registered, a RNP is responsible for applying to register all affiliates operating within its network and keeping the details of its affiliates up to date with AUSTRAC. They also have a range of other AML/CTF responsibilities on behalf of their affiliates. [149]

Other issues

Monitoring and enforcing compliance with the obligations of the AML/CTF Act for offshore service providers will present practical issues, regardless of the model chosen. The location of these businesses outside of Australia would also make supervision costly and presents challenges for traditional enforcement methods.

AUSTRAC has successfully issued infringement notices to a number of RNPs that have breached their obligations under the AML/CTF Act.[150] In the event that RNPs issued with infringement notices refuse to pay the financial penalty, AUSTRAC would consider other enforcement options, such as issuing a remedial direction, withdrawing the infringement notice and commencing civil action, or taking compliance and/or enforcement action against the affiliates of the RNPs located in Australia. However, not all offshore service providers will have affiliates with permanent establishments in Australia.

[147] On 7 September 2015, the Minister for Social Services announced a review of illegal offshore wagering and the *Interactive Gambling Act 2001* to investigate methods of strengthening enforcement and ensuring Australians are protected from illegal online wagering operators. Further information is available at the Department of Social Services' website: https://www.dss.gov.au/communities-and-vulnerable-people/programmes-services/gambling, (accessed 15 January 2016).
[148] See Item 32A of Table 1, section 6 of the AML/CTF Act.
[149] See AUSTRAC's website for further information: http://www.austrac.gov.au/chapter-5-remitter-registration-requirements#registration-requirements-rnp, (accessed 15 January 2016).
[150] See AUSTRAC's website for further information: http://www.austrac.gov.au/enforcement-action/infringement-notices-issued-austrac, (accessed 15 January 2016).

There are options for alternative enforcement action that could be applied domestically to leverage compliance by offshore service providers, including:

- requiring internet service providers to block access to specified websites
- publishing the names of 'blacklisted' businesses, and
- prohibiting Australian institutions (such as an Australian bank, authorised deposit-taking institutions, remittance business and other payments provider) from opening accounts for, or conducting transactions with offshore service providers unless the provider is registered with AUSTRAC.

The expansion of the regime under the AML/CTF Act to regulate offshore service providers could significantly increase the number of entities supervised and monitored by AUSTRAC and impact on AUSTRAC's resources. In view of this, a risk-based approach should be taken that initially targets designated services posing a high ML/TF risk. Where offshore-based businesses are located in jurisdictions that have appropriate AML/CTF regulation and similar customer identification requirements as Australia, the model should ensure there is no unnecessary duplication of AML/CTF obligations for a regulated entity.

The application of AML/CTF regulation to offshore service providers would result in the collection and handling of personal information relating to Australian customers by offshore businesses, resulting in privacy risks and impacts that would need to be addressed.

As the availability of designated services provided by offshore service providers continues to grow, AUSTRAC should monitor the ML/TF risks posed by any of these designated services that fall outside the scope of Australia's AML/CTF regime.

Recommendations

Recommendation 4.11

AUSTRAC should identify designated services that pose a high ML/TF risk when provided to an Australian customer by an offshore-based business.

Recommendation 4.12

The Attorney-General's Department, in partnership with AUSTRAC, should develop an appropriate model for applying AML/CTF obligations under the AML/CTF Act to high risk designated services provided by offshore service providers.

Recommendation 4.13

AUSTRAC should monitor the ML/TF risks posed by designated services offered by offshore service providers that fall outside the scope of Australia's AML/CTF regime.

5. Customer due diligence

Introduction

The customer due diligence (CDD) obligations under the AML/CTF regime require reporting entities to take steps to:

- identify their customers and verify their identity
- keep up-to-date information on their customers so they know if there has been a change in circumstances or business activities, and
- carry out further due diligence measures if necessary.

These obligations enable reporting entities to better understand their customers and their financial dealings. This information allows reporting entities to determine the ML/TF risk posed by each customer and efficiently manage this risk.

The CDD framework under the AML/CTF Act and Rules combines aspects of a risk-based approach with more detailed or prescriptive requirements.[151] A reporting entity must have in place an AML/CTF program, which establishes its operational framework for complying with AML/CTF obligations. Part B of an AML/CTF program covers CDD procedures, including the steps the reporting entity must take to identify customers (the applicable customer identification procedure (ACIP)).

The AML/CTF Rules set out two key components for the ACIP:

- collecting information to identify a customer, and
- verifying the collected information (in certain cases).

In some circumstances, a reporting entity is able to rely on an ACIP undertaken by another reporting entity. Reporting entities also have an obligation to conduct on-going CDD and monitoring, including scrutinising transactions.

Industry stakeholders and partner agencies raised a number of issues relating to the CDD framework, including:

- the requirements for identifying and verifying customers
- the provisions that allow one reporting entity to rely on CDD performed by another reporting entity, and
- access to, and availability of, databases, information and tools to assist reporting entities to conduct CDD.

Stakeholders also raised issues relating to amendments to the CDD obligations in the AML/CTF Rules introduced in June 2014. These amendments, which related to beneficial owners, politically exposed persons (PEPs) and general CDD requirements, aligned Australia's CDD obligations more closely to the FATF standards. The amendments took effect from 1 June 2014 and were subject to an implementation period that ended on 31 December 2015.[152]

[151] Parts 2 and 7 of the AML/CTF Act and Chapters 1, 4, 5, 6, 8, 9, 15 and 30 of the AML/CTF Rules.

[152] Ministerial Policy Principles were in place for the duration of the period in which reporting entities were required to undertake reasonable steps to comply with the new CDD requirements. Minister for Justice, *Policy (Additional Customer Due Diligence Requirements) Principles 2014*, 15 May 2014, http://www.austrac.gov.au/sites/default/files/documents/cdd_policy_principles_2014.pdf.

On 10 June 2015 AUSTRAC released for consultation additional draft changes to the AML/CTF Rules. The proposed amendments:

- update the electronic safe harbour procedure for customers
- broaden the collection of identification information to include information from sources other than the actual customer, and
- extend current customer identification exemptions to include beneficial owners and PEPs.

AUSTRAC finalised the amendments relating to extending the customer identification exemptions on 11 November 2015. The other proposed amendments are still being finalised.

Issues raised by industry stakeholders and partner agencies relating to the 2014 amendments to the AML/CTF Rules and the additional draft changes are not addressed as part of this review.[153]

There are five FATF standards relevant to CDD, encompassing general CDD (Recommendation 10), PEPs (Recommendation 12), reliance (Recommendation 17), high-risk countries (Recommendation 19) and CDD for DNFBPs (Recommendation 22). The deficiencies identified by the MER in relation to these standards are discussed below, except for issues relating to DNFBPs and high-risk countries. [154]

The framework for identifying and verifying customers

Reporting entities are required to collect information identifying the different customer types listed in Chapter 4 of the AML/CTF Rules. These are minimum requirements to collect a class of information called 'know your customer' (KYC) information. The KYC information collected differs depending upon the type of customer being identified (for example, an individual customer compared to a company or trust).

KYC information has to be verified in certain circumstances using documentation or reliable and independent electronic data.[155] The requirement to verify varies according to customer type.

The AML/CTF Rules also provide for two simplified verification procedures:

- streamlined 'safe harbour' procedures for verifying medium or low ML/TF risk customers who are individuals,[156] and
- simplified verification procedures for certain low ML/TF risk companies and trusts. [157]

These two procedures together constitute 'simplified CDD' and provide regulatory relief for some reporting entities.

Reporting entities are also required to conduct on-going CDD obligations and transaction monitoring.[158]

Consultation

Overall, there was widespread support for simplifying the framework for CDD under the AML/CTF Rules. Proposals included:

- consolidating the CDD requirements in Part B of an AML/CTF program with the Part A requirements[159]

[153] See AUSTRAC's website for further information on the June 2014 CDD amendments and consultation process: http://www.austrac.gov.au/businesses/obligations-and-compliance/customer-due-diligence, (accessed 15 January 2016).
[154] See *Chapter 4.2: Regime scope – Designated non-financial businesses and professions* and *Chapter 13: Countermeasures* for a fuller consideration of these issues.
[155] Parts 4.9 and 4.10 of the AML/CTF Rules.
[156] Paragraphs 4.2.10 to 4.2.13 of the AML/CTF Rules.
[157] Parts 4.3 and 4.4 of the AML/CTF Rules.
[158] Chapter 15 of the AML/CTF Rules.

- consolidating the general KYC requirements in Chapter 4 with the ongoing CDD requirements in Chapter 15, and
- combining the requirements to 'collect' and 'verify' into one obligation.

Industry stakeholders strongly supported the simplified CDD procedures, with one stakeholder considering that the safe harbour requirements are routinely met, online, with ease and at a low cost. Stakeholders also made numerous suggestions to expand the use of simplified CDD requirements.

Industry stakeholders considered that the AML/CTF regime should acknowledge and allow for the use of technological advances to meet KYC requirements. In particular, some stakeholders suggested a shift from reliance on 'static' databases for CDD and incorporate 'dynamic' means of verification, such as knowledge-based authentication and biometrics.

Other stakeholders encouraged incorporation of digital identifiers, such as location services, internet provider addresses, email addresses and mobile phone numbers, as part of KYC requirements.

There were a number of suggestions to enhance the verification requirements, including:

- allowing for the use of 'self-attestation', and
- allowing for the use of disclosure certificates for the verification of companies, trusts, partnerships, associations and registered cooperatives using a risk-based approach.

Some stakeholders raised concerns about the accessibility of CDD procedures for customers who may be unable to produce standard documentation to prove their identity, particularly customers who are Aboriginal or Torres Strait Islander, or newly arrived asylum seekers. Where these customers are unable to produce standard documentation, they may be prevented from accessing basic services, such as opening a bank account or accessing superannuation.

Findings of the MER

The MER rated Australia partially compliant with the FATF standard on CDD.[160] The key deficiencies identified included:

- the operation of exemptions within the AML/CTF Act and Rules, which may diminish the application of CDD in situations envisaged by the FATF standard
- inadequate verification requirements in relation to an agent of a customer, trustees and beneficiaries
- the operation of exemptions and simplified CDD measures in relation to trusts that are registered and subject to regulatory oversight, and companies that are licensed and supervised, which are not permitted by the FATF standards and do not appear to be based on proven low risk
- insufficient CDD requirements across all legal persons and legal arrangements
- the lack of a requirement to understand the control structure of non-individual customers, or understand the ownership structure
- the lack of a requirement to identify the beneficiary of a life insurance policy until pay out
- permitting reporting entities to undertake 'normal due diligence' measures as part of enhanced CDD

[159] See *Chapter 7: AML/CTF programs* for consideration of this issue.
[160] FATF Recommendation 10 (Customer due diligence).

- the lack of a requirement that reporting entities do not carry out a transaction, or terminate the business relationship, when the reporting entity is unable to comply with CDD requirements, and
- no provision allowing reporting entities to provide a designated service without completing CDD if there is a risk of tipping-off the customer by completing CDD.

The MER rated Australia as non-compliant with the FATF standard for CDD on the regulation of DNFBPs.[161]

The MER also noted that the AUD10,000 threshold for casinos to apply CDD was higher than the FATF's recommended threshold of USD/EUR3,000.[162]

Discussion

Simplifying the framework for CDD

While the CDD obligations in the AML/CTF Act and Rules were developed in close consultation with industry, they are complex and difficult to understand.

The CDD obligations under the AML/CTF Act and Rules should be restructured into a simplified framework that explicitly requires reporting entities to implement the core CDD obligations. This process should be undertaken as part of the general proposal to simplify and rationalise the AML/CTF Act and Rules discussed in *Chapter 2: Overarching issues.*

Collecting KYC information and verifying identity

KYC information requirements

The AML/CTF Rules set out the minimum KYC requirements for each customer type. These KYC requirements collect information that:

- all potential customers could reasonably be expected to possess, and
- all reporting entities could reasonably be expected to collect.

While the current KYC requirements remain appropriate, AUSTRAC should explore other reliable options that entities could utilise for KYC purposes in the future.

A number of stakeholders considered that mobile phone numbers should form part of the minimum KYC requirements for individual customers instead of the customer's residential address.[163] These stakeholders asserted that customers, particularly younger customers, frequently changed their address while retaining the one mobile phone number.

Changing the minimum KYC requirements to allow a mobile phone number to be used instead of a residential address would not be appropriate. While mobile phone providers generally ask customers for identifying information, they are not required to collect and verify the individual's identity to the standard required under the AML/CTF Act.[164] If mobile phone numbers were to be included in the minimum KYC for individuals, the CDD process could be undermined by the increased risk posed by criminals obtaining multiple phone numbers using false identities.

Some reporting entities expressed interest in using new technologies for CDD purposes, such as biometric technology. Biometrics refers to technologies that measure and analyse human body characteristics, such

[161] FATF Recommendation 22 (Designated non-financial businesses and professions: Customer due diligence). See *Chapter 4.2: Regime scope – Designated non-financial businesses and professions* for consideration of this issue.
[162] At 5 January 2016, AUD10,000 is the equivalent of USD7,150/EUR6,650.
[163] Paragraph 4.2.3 of the AML/CTF Rules requires that reporting entities collect, at a minimum, an individual customer's full name, date of birth and residential address.
[164] See the *Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2013* for the identity verification requirements for the identity checks required to activate a prepaid mobile phone service.

as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes. Reporting entities already have the flexibility to use new technology for verification purposes, where appropriate.[165] AUSTRAC should explore options to extend the use of biometrics as an alternative option to the minimum KYC requirements.

Simplified CDD requirements

The two simplified CDD procedures provide reporting entities with a cost effective and efficient way to meet their CDD obligations for lower ML/TF risk customers. These procedures should be retained, expanded to other services that have a demonstrated low ML/TF risk and merged into a single 'simplified CDD' procedure.[166]

Industry stakeholders made a number of specific proposals to expand the use of simplified CDD, including:

- applying the 'safe harbour' CDD procedures to all individual customers and to all medium or lower ML/TF risk customer types
- changing the safe harbour provisions to remove the requirement for residential address matching to be mandatory and to allow organisations to verify either the residential address or the date of birth of the customer
- allowing simplified verification for a wider range of companies and trusts (for example, foreign-registered companies)
- allowing simplified CDD procedures for select groups of 'lower risk' customers and services (for example, online accounts where there is no handling of cash, or for transactions below AUD1,000)
- where the ML/TF risk is minimal, allowing reporting entities to undertake no CDD measures, or CDD measures less stringent than the current simplified CDD procedures (for example, for low value electronic transfers where the funds are transferred domestically from one Australian bank account to another), and
- allowing simplified CDD for specific designated services and products which have a low ML/TF risk (for example, bookmakers, gift cards, managed investment schemes, certain types of financial leasing arrangements and salary packaging).

There is scope to allow reporting entities to adopt simplified CDD for a wider range of scenarios, but only where an AUSTRAC risk assessment demonstrates a low ML/TF risk. This means that simplified CDD should not be permitted for a class of customer types, transactions or designated services unless the entire class has a demonstrated low ML/TF risk. For example, all individual customers cannot be categorised as posing a low ML/TF risk, so the safe harbour provisions should not apply to all individuals as a class of customer.

A proposal for AUSTRAC to adopt a more proactive approach to providing exemptions where the applicant, the designated service, or the circumstances in which the designated service is provided pose a low ML/TF risk is discussed in *Chapter 17: Exemptions process.* The low-risk scenarios identified by stakeholders as candidates for simplified CDD should be considered as part of this more systematic approach to providing regulatory relief.

AUSTRAC is currently reviewing options to change the mandatory and optional verification requirement in the safe harbour provisions. This process will be informed by stakeholder submissions following the closure on 8 July 2015 of the separate CDD consultation process outlined above.

[165] See *Chapter 2: Overarching issues* for consideration of the issue of technology neutrality.
[166] This should occur where AUSTRAC has conducted a risk assessment and determined the ML/TF risk to be low.

Customers unable to produce standard documentation for CDD

Some customers present unique challenges for reporting entities in meeting their CDD obligations. The circumstances of these customers mean that initial identification documentation may have deficiencies. For example, a birthdate may be nominated when the actual birth was not registered or the spelling of a name may be inaccurate or represented phonetically. This creates problems when the customer is later asked to verify their identity and provide information that matches original documents. These issues are exacerbated when literacy is an issue, or where the person speaks English as a second language.

Discrepancies within information used for the identification and verification process is a particular issue in relation to superannuation. A substantial amount of time can lapse between the commencement of a superannuation account, and the ultimate withdrawal of funds. In many cases the employer provides the initial information to the superannuation fund. If this information is inaccurate, this creates difficulties for the customer accessing funds at a future date. Aboriginal and Torres Strait Islander people, in particular, experience difficulty meeting the CDD requirements of superannuation funds.

To help overcome these issues, industry stakeholders recommended amendments to the AML/CTF Rules to allow for 'self-attestation', the process in which individual customers certify that information in relation to their identity is true and correct.

The AML/CTF Act and Rules already provide reporting entities with the flexibility to verify an individual's identity in any manner they consider appropriate, including by self-attestation. Despite this flexibility, it is apparent from industry feedback that reporting entities are struggling to verify customers' identities in some circumstances. To provide clarity and certainty for reporting entities, AUSTRAC should consult with industry and relevant community representatives to develop standard industry practices and guidance to assist entities to meet their CDD obligations and deliver services to these customers who are unable to comply with more conventional methods for proving identity.[167]

The starting point for these discussions should be the minimum identity proofing requirements outlined in the National Identity Proofing Guidelines, which provide a better practice reference to organisations for proving the identity of their customers.[168]

To provide reporting entities with greater guidance as to where self-attestation may (or may not) be appropriate, the AML/CTF Rules should be amended to explicitly allow for self-attestation. As self-attestation is vulnerable to misuse by customers, it should only be available as a 'last resort' using a risk-based approach where a customer's identity cannot otherwise be verified and where there is a demonstrated low ML/TF risk.

The AML/CTF regime carries existing penalties under the AML/CTF Act (for providing false information to reporting entities) where a customer abuses the self-attestation process, although these could be difficult to enforce if the identity of the person who provided the false information is not known.[169] It is important that where self-attestation is used in lieu of standard verification processes, reporting entities apply appropriate levels of ongoing CDD and transaction monitoring to manage and mitigate the higher ML/TF risk associated with customer identities established using self-attestation.

[167] For example, the Australian Institute of Superannuation Trustees has created a working group to help effectively establish and meet the superannuation needs of Aboriginal and Torres Strait Islander people: http://www.aist.asn.au/about/aist-in-the-community/indigenous-super.aspx, (accessed 15 January 2016).
[168] Attorney-General's Department, *National Identity Proofing Guidelines*, 2014, https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/NationalIdentityProofingGuidelines.pdf.
[169] For example, see sections 136 and 137 of the AML/CTF Act.

Disclosure certificates

Self-attestation using disclosure certificates is explicitly provided for under the AML/CTF Rules for companies, trusts, partnerships, associations and registered cooperatives.[170] This allows an appropriate officer to certify certain information to verify the customer's identity.

One industry stakeholder considered that self-attestation should be expanded to allow reporting entities to accept disclosure certificates using a risk-based approach rather than as prescribed by the requirements in Chapter 30 of the AML/CTF Rules. For example, Chapter 30 requires the trustee to certify the information in relation to a trust, when the auditor of the trust may in fact be best placed to certify matters about the beneficiaries and the beneficial owner.

The AML/CTF Rules should be amended to allow reporting entities to adopt a risk-based approach to accepting disclosure certificates that have been certified by an appropriate officer. This amendment will significantly increase the utility and efficiency of these provisions for reporting entities.

Addressing general CDD deficiencies identified in the MER

With the introduction of the June 2014 amendments to the AML/CTF Rules, Australia has implemented the FATF's core requirements for CDD. The deficiencies identified in the MER are generally of a minor, technical nature and often relate to the lack of an explicit obligation in the AML/CTF Rules. While these obligations often do exist, the complexity of the AML/CTF Act and Rules makes it difficult to understand the scope of obligations and how the regime operates to impose these obligations.

The proposal to simplify the AML/CTF Act and Rules should generally address these deficiencies. These amendments should also explicitly prohibit reporting entities from providing a designated service if CDD cannot be completed and require them to consider making an SMR in these circumstances.[171]

Proposals for a new AUSTRAC exemption process should also address the concerns in the MER about the operation of future exemptions in relation to CDD.[172]

The MER recommended that the AUD10,000 CDD threshold for casinos should be lowered to be consistent with the FATF's recommended threshold of USD/EUR3,000.[173] Industry stakeholders recommended that the threshold should be raised, with AUD20,000 suggested as an appropriate threshold.

As this threshold was first introduced under the FTR Act and continued under the AML/CTF Act, a ML/TF risk assessment should be conducted to reassess whether the value of the threshold continues to be appropriate. This assessment should also consider whether any threshold change should apply only to casinos (as required by the FATF) or other gambling service providers regulated under the AML/CTF Act as well.

Politically exposed persons

'Politically exposed persons' (PEPs) are individuals, whether Australian or foreign nationals, who occupy a prominent public position or functions in a government body or international organisation. Under the AML/CTF Rules, the definition of PEPs also extends to their immediate family members and close associates.[174]

---

[170] Chapter 30 of the AML/CTF Rules.
[171] This requirement is currently implicit as reporting entities are prevented from providing a designated service to a customer if the ACIP cannot be carried out (section 32 of the AML/CTF Act).
[172] See *Chapter 17: Exemptions process*.
[173] At 5 January 2016, AUD10,000 is the equivalent of USD7,150/EUR6,650.
[174] See paragraph 1.2.1 of the AML/CTF Rules.

With the 2014 amendments to the AML/CTF Rules, reporting entities must now determine whether a customer or beneficial owner is a PEP before the provision of a designated service, or as soon as practicable after the designated service has been provided to the customer.[175]

Consultation

Industry stakeholders asked for more clarity surrounding the CDD obligations that apply to PEPs and for a central register of domestic PEPs to be established to assist reporting entities in fulfilling their PEP obligations.

Other stakeholders asked for the requirements for PEPs to be strengthened by:

- removing the time limit on PEPs so that they remain PEPs even after they have left public office
- requiring PEPs to provide their financial institution with an asset and income declaration form, as well as subsequent updates, and
- allowing Australian authorities to automatically share information with authorities of other governments when a foreign PEP purchases property in Australia, transfers funds or undertakes gambling activity, unless the Government has reason to prosecute the person in question.[176]

Findings of the MER

The MER rated Australia as largely compliant with the FATF's standards for conducting CDD on PEPs, although it considered that the notion of 'close associates' within the AML/CTF Rules is too restrictive and important officials of political parties are not explicitly covered in the Rules.[177]

The MER also noted that CDD requirements only apply to beneficiaries of a life insurance policy that are PEPs at the time of pay out. There are no further obligations that apply to reporting entities where this type of pay out to a PEP occurs in a high-risk situation, as required by the FATF standards.

Discussion

While stakeholders indicated in submissions that aspects of the new PEP obligations were unclear, AUSTRAC has since released and finalised guidance on PEPs, in consultation with industry stakeholders. This clarifies key terms used in the PEPs definition, including the notions of 'close associate' and 'officials of political parties'.[178] This guidance should provide greater clarity for stakeholders and address the concerns raised in the MER.

Stakeholders commonly asked for the Government to establish a register of PEPs to assist reporting entities to meet their obligations. Third-party service providers have already created registers to assist reporting entities to meet their PEP obligations, noting that there may be limitations on the extent of the data.[179] These commercial PEP registers provide a quick and cost-efficient way for reporting entities to meet their CDD obligations and should not be replicated by government.

The AML/CTF Rules should be amended to address the MER deficiency relating to application of enhanced CDD requirements to beneficiaries of a life insurance policy that are PEPs at the time of pay out.

---

[175] See paragraph 4.13.1 of the AML/CTF Rules.
[176] Issues in relation to information-sharing are discussed in *Chapter 14: Secrecy and access.*
[177] FATF Recommendation 12 (Politically exposed persons).
[178] AUSTRAC, *AUSTRAC compliance guide: 'Politically exposed persons'*, http://www.austrac.gov.au/part-b-amlctf-program-customer-due-diligence-procedures#peps, (accessed 15 January 2016).
[179] For example, World-Check. See Thompson-Reuters' website for further information: https://risk.thomsonreuters.com/products/world-check, (accessed 15 January 2015).

Reliance

The AML/CTF Act and Rules allow a reporting entity to rely on an ACIP carried out by another reporting entity in limited circumstances.[180] These circumstances are:

- where a licensed financial adviser arranges for a customer to receive a designated service from a second reporting entity (for example, where a financial adviser refers a customer to a bank, the bank can rely on the ACIP carried out by the adviser), and
- where a customer of one member of a designated business group becomes a customer of another member of the designated business group, and is required to undergo the ACIP.

A reporting entity is unable to rely on customer identification conducted outside Australia unless the AUSTRAC CEO provides the reporting entity with an exemption. In 2009, the AUSTRAC CEO issued a declaration allowing a reporting entity to rely on customer identification conducted in a foreign country in certain circumstances. The declaration was primarily intended to allow Australian reporting entities to rely on customer identification conducted in New Zealand.[181]

Consultation

Industry stakeholders indicated that the reliance provisions under the AML/CTF regime are too restrictive. They strongly supported expanding the use and application of reliance (consistent with the FATF standards) and highlighted the approaches taken to reliance in the United Kingdom, New Zealand and European Union.

Findings of the MER

The MER rated Australia as partially compliant with the FATF standards on reliance.[182] The deficiencies identified in the MER were:

- it is not explicitly stated that the reporting entity relying on a third party remains ultimately responsible for CDD measures
- there is no obligation for reporting entities to satisfy themselves that, where they are relying on a third party located abroad, the third party is regulated, supervised and monitored, and has measures in place for compliance with the FATF standards for CDD and record-keeping, and
- the geographic risk has not been taken into account when determining those countries in which third parties being relied on can be based.

Discussion

The model for reliance under the AML/CTF Act and Rules should be made accessible to reporting entities. As reliance is an important measure that can deliver greater efficiencies and significant regulatory relief for reporting entities. This new model should be based on the United Kingdom's model for reliance and be consistent with the FATF standards.[183] It should generally permit reporting entities to rely on identification procedures conducted by a third party, provided that:

- the third party consents to being relied on

[180] Section 38 of the AML/CTF Act and Chapter 7 of the AML/CTF Rules.
[181] AUSTRAC CEO, *Declaration*, 16 March 2009, http://www.austrac.gov.au/sites/default/files/documents/declaration_s38.pdf.
[182] FATF Recommendation 17 (Reliance).
[183] For example, refer to section 5.6 of Part I of the Joint Money Laundering Steering Group, *Prevention of money laundering/combating terrorist financing guidance (Revised Version-2014)*, 2014, http://www.jmlsg.org.uk/, (accessed 15 January 2016).

- notwithstanding the third party's consent, the relying business remains ultimately responsible for CDD, and
- the third party is a prescribed entity located in Australia or another country where it is subject to appropriate regulation and similar customer identification requirements as are applicable in Australia.

Any reporting entity consenting to be relied upon under this proposed model should be required to retain the CDD records that are relied upon for a specified period from the date on which reliance commences. The reporting entity should be required to make these records available to the entity relying on them as soon as is reasonably practicable, if requested. The relying entity should also be required to take steps to ensure the entity being relied upon will provide the required information prior to reliance commencing.

Where reliance is used, reporting entities should still be required to fulfil their ongoing CDD obligations under the AML/CTF Act and Rules. Additionally, AUSTRAC (and other agencies with AML/CTF Act information-gathering powers) should have the power to access the CDD records obtained by a reporting entity from the third party under a reliance arrangement.

To assist reporting entities to identify comparable overseas jurisdictions for the purposes of reliance, AUSTRAC should publish non-binding guidance that lists jurisdictions with AML/CTF regimes comparable to Australia.[184]

A prescribed entity under the new model should include credit and financial institutions, but options for relying on CDD conducted by other professionals regulated under the AML/CTF regime should be explored, particularly if the scope of the regime is expanded to regulate all DNFBPs.[185] Third-party reliance is allowed under the European Union Anti-Money Laundering Directive and used across professions.[186] For example, subject to a number of conditions similar to those outlined above, the United Kingdom allows legal practitioners to rely on CDD performed on the following professionals:

- auditor
- insolvency practitioner
- external accountant
- tax adviser, and
- independent legal professional.

Other issues relevant to CDD

Registers to assist in CDD on legal persons and arrangements

A wide range of legal persons and arrangements can be created in Australia. These include:

- **legal persons**, including companies (proprietary, public non-listed, public listed), partnerships (incorporated or limited partnerships), associations (incorporated or unincorporated) and registered and unregistered cooperatives, and
- **legal arrangements**, such as trusts.

[184] This is consistent with overarching Recommendation 2.4 which proposes that AUSTRAC provide additional guidance for industry.
[185] See *Chapter 4.2: Regime scope – Designated non-financial businesses and professions* for further information.
[186] European Union, *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing*, 5 February 2013, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52013PC0045.

In Australia, proprietary companies, public non-listed and public listed companies, incorporated limited partnerships and incorporated associations are regulated at the federal level by ASIC. Partnerships, associations and cooperatives are regulated at the state and territory level.

Trust law is derived from the common law, although states and territories also have legislation which imposes additional obligations on trustees and a trust's constituent elements. Where a trustee is a corporate entity, they will be regulated by ASIC. If the trust receives income, it will be regulated by Commonwealth tax laws and must lodge an annual tax return.

Australia already has a number of registers in relation to companies and other incorporated entities, partnerships, associations and cooperatives.

While there is currently no national register of trusts, a large number of trusts that receive income (and are required to have an Australian Business Number (ABN)) are registered by the ATO on the Australian Business Register or registered with ASIC (if the trustee is incorporated).

These registers assist reporting entities to undertake CDD in a quick and cost efficient manner. However, there are gaps in the types of entities registered and the types of information available, particularly in relation to beneficial ownership. These gaps present challenges for reporting entities conducting CDD.

Consultation

Numerous industry stakeholders discussed the challenges associated with verifying information on the ownership of legal persons and legal arrangements. These stakeholders considered that a centralised register of beneficial ownership information would ensure that reporting entities are able to comply with CDD obligations efficiently and effectively.

One stakeholder recommended that beneficial ownership information could be better collected under existing arrangements by placing additional obligations on regulators:

- For **companies**: ASIC should be required to collect beneficial ownership information in each company's annual return, and make that information available to reporting entities.
- For **registered managed investment schemes**: ASIC should be required to collect beneficial ownership information (as part of the scheme's annual reporting) and make it available to reporting entities.
- For **trusts with an ABN:** the ATO should be required to collect beneficial ownership information as part of the trust's annual reporting and make it available to reporting entities.

Stakeholders also raised concerns about the lack of a central database for unincorporated partnerships, unincorporated associations and cooperatives, while others raised the possibility of the creation of a central KYC database. They also considered that reporting entities needed greater access to existing federal, state and territory databases, including through the Australian Government's Document Verification Service (DVS).

Findings of the MER

The MER identified a number of significant shortcomings concerning the transparency of beneficial ownership of legal persons and legal arrangements in Australia.[187] These include the following:

- there is no requirement for companies or company registers to obtain and hold up-to-date information to determine the ultimate natural person who is the beneficial owner beyond the immediate shareholder

[187] See FATF Recommendations 24 (Transparency and beneficial ownership of legal persons) and 25 (Transparency and beneficial ownership of legal arrangements).

- there is no obligation for trustees to hold and maintain information on trusts
- there is no obligation for trustees to keep this information up-to-date and accurate
- there is no obligation for trustees to disclose their status to financial institutions and DNFBPs, and
- there are no proportionate and dissuasive sanctions available to enforce the requirement to exchange information with competent authorities in a timely manner.

Discussion

Reporting entities indicated that they are experiencing difficulties in accessing reliable and independent information about beneficial ownership.

A number of countries have taken major steps towards the development of national registers of beneficial ownership to assist regulated businesses to comply with their CDD obligations under AML/CTF laws. This is particularly apparent in European countries in response to the European Union's fourth AML Directive.[188] For example, in March 2015, the United Kingdom legislated to create a national register of beneficial ownership.[189]

As part of its report on insolvency in the Australian construction industry, the Senate Economics References Committee recommended in December 2015 that the Government, through the work of the Legislative and Governance Forum for Corporations, establish a register of beneficial ownership.[190]

The establishment of a national register of beneficial ownership within Australia, or the addition of new obligations on existing registers, involves a wide range of legislative instruments, regulators and industry participants at the federal, state and territory level. The implementation of either one of these proposals would be consistent with the recent work of the Group of 20 (G20) nations concerning the importance of transparency in corporate structures and beneficial ownership, not only in the context of AML/CTF obligations, but also in the administration of global taxation laws.[191]

Any proposals to improve the availability of, and access to, information on legal persons and arrangements in Australia will have implications for a wide range of government agencies at the federal, state and territory level and should be explored with the relevant government agencies outside of this review process.

Access to databases and the Document Verification Service (DVS)

Consultation

Stakeholders considered that reporting entities should have greater access to registers maintained by federal, state and territory regulators and agencies to help them meet their CDD obligations in a cost-effective manner. A number of stakeholders also expressed strong support for the DVS initiative as a positive step, particularly those entities that conduct their operations almost exclusively online, such as sports betting businesses.

---

[188] European Union, *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing*, 5 February 2013, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52013PC0045.

[189] On 26 March 2015, the United Kingdom passed the *Small Business, Enterprise and Employment Act 2015* which establishes a central public registry on beneficial ownership information (see Part 7). The Act is to be fully implemented by April 2016. See the United Kingdom Department for Business, Innovation & Skills' website for further detail: https://www.gov.uk/government/consultations/company-ownership-and-control-register-implementation, (accessed 15 January 2016).

[190] Recommendation 35, *Insolvency in the Australian construction industry,* December 2015, Economics References Committee, http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Insolvency_construction/Report.

[191] In 2014, the G20 released its *High-Level Principles on Beneficial Ownership Transparency*: https://g20.org/wp-content/uploads/2014/12/g20_high-level_principles_beneficial_ownership_transparency.pdf.

A 2008 report by the Australian Law Reform Commission (ALRC) into Australia's framework for the protection of privacy also recommended that this review consider whether the use of the electoral roll by reporting entities for the purpose of identification verification is appropriate.[192]

Discussion

The DVS is a federal, state and territory initiative, managed by the Attorney-General's Department (AGD), which allows authorised organisations, such as reporting entities, to electronically match identifying information on certain government-issued identity documents directly with the issuing government bodies (whether Commonwealth, state or territory).[193] This allows reporting entities to check that the information contained on an identity document presented by an individual is current or valid.

Some stakeholders considered that the usefulness of the DVS was limited due to the high cost of using the service and the omission of a number of key databases from the DVS Commercial Service, including births, deaths and marriages registries.[194]

AGD is working to improve the integrity and performance of DVS matching services and expanding the range and quality of documents available to the private sector. For example, DVS users can now verify date of birth information on Medicare records. In November 2015, the Australian and New Zealand Governments announced new reciprocal arrangements for the verification of identity documents, to enable New Zealand organisations to use the DVS and Australian organisations to use the corresponding Confirmation Service.

AGD is continuing to work with the states and territories to expand the DVS commercial service to include births, deaths and marriages databases, which is expected to occur by late-2016. AGD has significantly decreased the waiting period for approvals to use the DVS and is likely to abolish the $250 DVS application fee.

Items 5-7 of subsection 90B(4) of the *Commonwealth Electoral Act 1918* permit the Australian Electoral Commission (AEC) to give a copy of the Commonwealth electoral roll to prescribed persons or organisations to assist reporting entities in conducting CDD. Six organisations are prescribed for the purposes of items 5-7.[195] As access to the electoral roll is provided for under the *Commonwealth Electoral Act 1918*, and not the AML/CTF Act, this issue is outside of the terms of reference of this review. The AEC, AUSTRAC and AGD are, however, actively considering issues relating to reporting entity access to the electoral roll for CDD.

Verifying that entities are regulated by AUSTRAC

Industry stakeholders suggested that regulatory efficiencies could be achieved if AUSTRAC permitted reporting entities to search the Reporting Entities Roll to verify whether an entity that they intend to do business with is regulated by AUSTRAC. The ability to conduct this type of search is relevant where a reporting entity requests a designated service from another entity and where a reporting entity may wish to rely on the ACIP conducted by another entity.

Reporting entities and the public already have access to the Remittance Sector Register via AUSTRAC's website. This allows reporting entities and the public to check if a remitter is registered with AUSTRAC, and

[192] Recommendation 16-4(d). Australian Law Reform Commission, 12 August 2008, *For Your Information: Australian Privacy Law and Practice,* ALRC Report 108, http://www.alrc.gov.au/publications/report-108.
[193] Documents available to be verified through the DVS Commercial Service include driver licences, passports, visas, Immicards, citizenship certificates and Medicare cards. See the DVS's website at http://www.dvs.gov.au, (accessed 15 January 2016).
[194] AGD is working with the states and territories to expand the DVS Commercial Service to include those databases in the future.
[195] Regulation 7 of the *Electoral and Referendum Regulation 1940.*

if it has any conditions placed on its registration.[196] Similar access should be given to the Reporting Entities Roll, subject to appropriate privacy controls.

Trusted digital identities

Industry stakeholders highlighted the difficulties in conducting online verification and supported the development of trusted digital identities to allow reporting entities to more efficiently and effectively verify the identities of customers and meet their CDD obligations.

The development of a trusted digital identity has implications that extend beyond the application of AML/CTF measures and the terms of reference of this review.

In 2014 the Financial Systems Inquiry recommended the development of a national strategy for a federated-style model of trusted digital identities.[197] The Government agreed with this recommendation and tasked the Digital Transformation Office with developing a Trusted Digital Identity Framework.[198] The framework will establish a set of principles and standards for the use of accredited government and third-party digital identities to enable individuals and businesses to access services more easily.[199]

Recommendations

Recommendation 5.1

The AML/CTF Act should be simplified to explicitly require reporting entities to implement the core customer due diligence obligations.

Recommendation 5.2

The AML/CTF Rules for customer due diligence should be rationalised and simplified as a priority, using plain language to facilitate ease of use and supplemented by enhanced guidance.

Recommendation 5.3

AUSTRAC should consider and explore other reliable options, including those utilising new technologies, as alternatives to the existing minimum know your customer requirements for individual customers.

Recommendation 5.4

The safe harbour and simplified verification procedures under the AML/CTF Rules should be rationalised into a single simplified customer due diligence procedure.

Recommendation 5.5

AUSTRAC should consider expanding the availability of simplified customer due diligence to designated services and customers that have a minimal or low ML/TF risk.

Recommendation 5.6

The AML/CTF Rules should explicitly allow for use of self-attestation to identify individual customers using a risk-based approach only as a measure of last resort where a customer's identity cannot otherwise be reasonably obtained or verified.

---

[196] AUSTRAC, *Remittance Sector Register,* https://online.austrac.gov.au/ao/public/rsregister.seam, (accessed 15 January 2016).
[197] Recommendation 15, Financial Systems Inquiry, *Final Report*, 7 December 2014, http://fsi.gov.au/publications/final-report/.
[198] Australian Government, *Improving Australia's financial system: Government response to the Financial System Inquiry*, 20 October 2015, http://www.treasury.gov.au/PublicationsAndMedia/Publications/2015/Govt%20response%20to%20the%20FSI.
[199] See the Digital Transformation Office's website for further information: https://www.dto.gov.au/budget/trusted-digital-identity-framework, (accessed 15 January 2016).

Recommendation 5.7

The AML/CTF Rules should allow reporting entities to accept disclosure certificates certified by an acceptable officer using a risk-based approach.

Recommendation 5.8

AUSTRAC and industry representatives should develop guidance to assist reporting entities to conduct customer due diligence on customers that may experience difficulty accessing services provided by reporting entities because they are unable to comply with the more conventional methods for proving identity.

Recommendation 5.9

The AML/CTF Act should be amended to explicitly prohibit reporting entities from providing a regulated service if the applicable customer identification procedure cannot be carried out and require reporting entities to consider making a suspicious matter report in such situations.

Recommendation 5.10

AUSTRAC should conduct an ML/TF risk assessment on whether the customer due diligence threshold for casinos and other gaming providers should change.

Recommendation 5.11

The AML/CTF Rules should be amended to require reporting entities to conduct specific enhanced customer due diligence measures (in line with the FATF standards) at the time of pay out where the beneficiary or beneficial owner of a life insurance policy is a politically exposed person and a higher ML/TF risk is identified.

Recommendation 5.12

The AML/CTF Act should be amended to expand the ability of reporting entities to rely on customer identification procedures performed by a third party, subject to the following conditions:

(a) where the third party agrees to being relied on, the relying business remains ultimately responsible for the customer due diligence measures, and

(b) where the third party is outside of Australia, the third party is subject to appropriate regulation and similar customer identification requirements as are applicable in Australia.

Recommendation 5.13

AUSTRAC should permit access to the Reporting Entities Roll, subject to appropriate privacy restrictions, in a similar manner to the Remittance Sector Register.

6. Reporting obligations

Introduction

One of the key obligations imposed on reporting entities under the AML/CTF Act and FTR Act is the requirement to report certain financial transactions and suspicious matters to AUSTRAC.

Reporting to AUSTRAC first commenced in 1988 under the CTR Act and continued under the FTR Act. While these reporting requirements were largely subsumed by the AML/CTF Act in 2008, some residual reporting requirements remain under the FTR Act.[200]

Reporting obligations under the AML/CTF Act are set out in Parts 3 and 4 and include requirements to report:

- international funds transfer instructions (IFTIs)
- threshold transactions (TTRs)
- suspicious matters (SMRs), and
- cross-border movements of physical currency (CBM-PCs) and bearer negotiable instruments (CBM-BNIs).

Part 5 of the AML/CTF Act sets out information requirements in relation to electronic funds transfer instructions (EFTIs).

Under the FTR Act, cash dealers must submit:

- significant cash transaction reports (SCTRs) (section 7), and
- suspect transaction reports (SUSTRs) (section 16).

Solicitors must also report SCTRs under section 15A of the FTR Act.

The information provided through these reports is used by AUSTRAC to generate financial intelligence to assist government agencies to detect and disrupt serious and organised crime, minimise threats to Australia's national security and protect revenue.

Industry stakeholders supported changes to reporting obligations under the AML/CTF Act. In particular, they asked for reporting to be simplified and reporting thresholds to be reviewed. More broadly, stakeholders strongly supported removing duplication across different reporting obligations and more closely aligning information collected and reported to AUSTRAC with the information needs of law enforcement.

Partner agencies asked for existing thresholds to be retained at their current value and for reporting requirements to be expanded in certain circumstances.

These issues are discussed below separately in relation to each of the reporting obligations. Issues in relation to CBM-PCs and CBM-BNIs are discussed in *Chapter 12: Cross-border movements of physical currency and bearer negotiable instruments.*

The ALRC also recommended in its report on Australia's framework for the protection of privacy that this review consider whether the number and range of transactions for which identification is required should

[200] See *Chapter 18: The Financial Transaction Reports Act 1988* for consideration of this issue.

be more limited than currently provided for under the legislation.[201] The ALRC particularly highlighted the AUD10,000 threshold for TTRs. This recommendation is discussed below.

International and electronic funds transfer instructions

A person who sends or receives an IFTI transmitted into or out of Australia must report certain information about the transaction to AUSTRAC, irrespective of the value of the transfer. There are two types of IFTIs:

- IFTI-E – reportable by an authorised deposit-taking institutions, bank, building society or credit union or a person specified in the AML/CTF Rules, and
- IFTI-DRA – reportable by a provider of a designated remittance arrangement.

The IFTI reporting requirements are set out in section 45 of the AML/CTF Act. Chapters 16 and 17 of the AML/CTF Rules set out the reportable details.

Part 5 of the AML/CTF Act sets out the information which reporting entities are required to include about the origin of money in a domestic or international EFTI. Chapter 12 of the AML/CTF Rules provides further details on the requirements.

Consultation

The volume and take-up of online transactions is steadily increasing, particularly low value transactions. In view of this, some industry stakeholders supported the introduction of a minimum value threshold for IFTI reporting to provide reporting entities with regulatory relief.

Industry stakeholders also proposed measures to streamline and strengthen the IFTI reporting framework, including:

- requiring reporting of actual payments instead of payment instructions for IFTIs
- aligning the information to be collected and reported for IFTIs with the information required by AUSTRAC and its partner agencies, rather than relying on the information-gathering power under section 49 of the AML/CTF Act to request any omitted information
- ensuring the definitions of EFTIs reflect actual operation of EFTIs
- expanding the definition of an IFTI to capture other transactions that involve international funds transfers, such as credit and debit card transactions
- reviewing the reporting requirements to:
    - only require the beneficiary bank (that is, the bank that holds the beneficiary customer's account and processes the payment) to report the IFTI, and
    - allow any reporting entity who is a party to the funds transfer to submit the IFTI report, with the parties involved in the transfer agreeing among themselves the arrangements for reporting and how each party will contribute the information required to populate the report, and
- creating IFTI reporting obligations for authorised deposit-taking institutions that use the Western Union Account-Based Money Transfer system.

One partner agency suggested that IFTI reports should be submitted for ATM cash withdrawals from overseas bank accounts.

[201] Recommendation 16-4(b). Australian Law Reform Commission, 12 August 2008, *For Your Information: Australian Privacy Law and Practice,* ALRC Report 108, http://www.alrc.gov.au/publications/report-108.

The findings of the MER

The MER rated Australia partially compliant with the FATF standards for collecting and passing on information in domestic and cross-border wire transfers.[202] The main deficiencies identified were that the AML/CTF Act does not:

- meet the FATF standards in relation to the collection and verification of information about the originators and beneficiaries wire transfers
- place explicit obligations on financial institutions to ensure that wire transfers comply with the FATF's information requirements and that the risks associated with non-complaint wire transfers are mitigated
- apply Australia's wire transfer requirements to designated remittance arrangements, and
- require freezing action be undertaken in wire transfers in relation to Australia's targeted financial sanctions regime.

Discussion

Thresholds

Australia is one of only a few countries to require the reporting of IFTIs and the only country that does not apply a minimum value threshold to this type of reporting.

During 2014-15, reporting entities reported over 91 million IFTIs to AUSTRAC with a combined value of AUD4.6 trillion. This represents around 95 per cent of all transaction reports submitted to AUSTRAC.[203] A significant number of these IFTIs collected involved low-value transactions. For example, in 2014-15, 63.1 per cent of all IFTIs reported by reporting entities (57.5 million IFTIs) were for low-value transactions involving AUD100 or less (see Table 3). This trend is expected to become more pronounced as customers' retail and shopping habits move increasingly online.

The majority of the regulatory burden associated with reporting IFTIs for low value transactions was borne by one reporting entity (56.0 million IFTIs), as Table 3 demonstrates.

Table 3: Value of IFTIs reported in 2014-15

Value of transaction	IFTIs reported by all reporting entities		IFTIs reported by one major reporting entity	
	Number	% of all IFTIs reported	Number	% of all IFTIs reported
All IFTIs reported	91.1 million	100%	65.7 million	72.1%
AUD0 – 100	57.5 million	63.1%	56.0 million	61.5%

There are compelling reasons to retain the obligation to report all IFTIs, regardless of the value of the transaction. Low value transactions do not always pose a low risk of criminal activity. This is particularly true of the risks associated with terrorism financing, child exploitation, people smuggling and human trafficking, where low value payments are often a distinguishing characteristic of the criminal activity.

For terrorism financing in particular, only very small amounts are needed to fund terrorist acts and support terrorists and terrorist organisations. This risk is reflected in the Government's Foreign Fighters Initiative, which in part is intended to enhance the information captured through IFTI reporting.

Information on low-value payments can assist authorities to build an overall picture of a suspected criminal's financial activity or identify assets or sources of income that might otherwise remain hidden, as

[202] FATF Recommendation 16 (Wire transfers).
[203] See *Appendix 2* for data on the volume and value of IFTIs from 2007-08 to 2014-15.

case studies 8, 9 and 10 illustrate. In these cases, the significance of an IFTI is not just in the materiality of the payment reported in one transaction, but in the materiality of all payments made to a recipient within a period of time.

CASE STUDY 8: AUSTRAC INFORMATION REVEALED EXTENT OF PEOPLE SMUGGLING OPERATION[204]

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

Authorities alleged that suspects A and B were key players in a people smuggling syndicate, responsible for planning and facilitating unlawful arrivals into Australia. AUSTRAC analysis of financial transaction reports showed that over a five-year period suspect B sent 28 IFTIs out of Australia totalling more than AUD42,000. The IFTIs were primarily sent to Indonesia. The IFTIs undertaken by suspect B were conducted via remitters for low-value transfers of between AUD100 and 5,000. A small number of the IFTIs were sent with payment details describing them as 'gift' or 'personal'.

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

- the Indonesia-based 'ordering' customer for three IFTIs sent to Australia from Indonesia over a 10-day period, totalling more than AUD7,000
- the Indonesia-based beneficiary of six IFTIs totalling more than AUD20,000 sent from Australia to Indonesia over a two-month period.

The information provided by the IFTIs assisted in the arrest and conviction of suspects A and B for people smuggling offences under the *Migration Act 1958*. Both were sentenced to imprisonment.

CASE STUDY 9: CHILD EXPLOITATION ACTIVITY DETECTED USING IFTI[205]

AUSTRAC information alerted a law enforcement agency to the activities of a suspect who was apparently sending large sums of money overseas in multiple small transactions.

The Australian based offender was identified sending thousands of dollars in sub-AUD100 amounts to purchase live child sex shows in the Philippines. One report from this operation indicates the offender sent AUD6,205 across 107 transactions, with only one transaction greater than AUD99.

The offender was convicted of using a carriage service to cause child exploitation material to be transmitted and one count of procuring a child outside Australia to engage in sexual activity, and is currently serving a 7 year sentence in Victoria.

CASE STUDY 10: CHILD EXPLOITATION ACTIVITY DETECTED USING IFTI – PAY PER VIEW[206]

AUSTRAC information alerted a law enforcement agency to the activities of a suspect who was apparently sending large sums of money overseas in multiple small transactions.

The Australia-based offender was procuring child exploitation via pay-per-view websites in the Philippines. AUSTRAC reporting identified multiple international payments for this service in the AUD20 – AUD30 range, with only a few payments exceeding AUD99.

The offender was convicted of various offences relating to accessing child exploitation material and is currently serving an 11 year sentence in Victoria.

The identity data attached to low-value IFTI reports is also valuable for law enforcement purposes. Low-value transactions are more likely to be personal purchases where purchasers use their correct residential or mailing addresses, as well as other identifiers. This information can be cross-referenced with other

[204] Source: AUSTRAC.
[205] Source: Australian Federal Police.
[206] Source: Australian Federal Police.

information to develop profiles of a person who may be under investigation. This identity data is of particular value where a complex financial investigation is required to be undertaken without contacting the taxpayer as part of addressing organised crime risks.

A series of IFTI payments considered collectively can also help detect online businesses and evaluate the risk of undeclared sales for both income tax and GST purposes.

The obligation to report all IFTIs, regardless of value, provides Australian law enforcement agencies with an important advantage for detecting and analysing suspected criminal transfers and terrorism financing. This advantage should be preserved, particularly in the current climate where low-value transactions are proving useful to combat terrorism financing.

However, an assessment should be conducted as to whether specific classes of transactions below a threshold could be exempted from the IFTI reporting requirements where they pose a demonstrated low ML/TF risk and provide little intelligence value. These types of exemptions could be provided through existing mechanisms under the AML/CTF Act and Rules and could provide significant regulatory relief for some reporting entities.[207]

Scope of reporting requirements

Partner agencies considered that the lack of an IFTI reporting obligation applicable to the international movement of funds using credit cards and debit cards represents a significant gap in the AML/CTF reporting framework. A number of industry stakeholders also supported expanding the scope of IFTI reporting to capture these movements of funds.

Credit cards and debit cards payments are the most common type of non-cash payment made in Australia, accounting for over 60 per cent of the volume of non-cash payments.

The take-up and volume of these cards is likely to continue to increase into the future as business becomes increasingly digitised.

Under the AML/CTF Act, IFTI reporting obligations only apply to some international transactions involving credit and debit cards. For example, if an international transaction is conducted to buy a piece of clothing from a foreign website, and the payment is made using a credit card and processed by a third-party intermediary (which is a reporting entity), an IFTI report is required. If the same international transaction is conducted and the payment for the purchase is made using a credit card and processed directly by the foreign website, an IFTI report is not required.

While partner agencies can use other legislation to access credit card and debit card information, this access occurs on an ad-hoc basis and there is no mandatory reporting requirement for businesses for AML/CTF purposes.

Expanding the scope of the IFTI reporting obligations under the AML/CTF Act to capture the international movement of funds using credit cards and debit cards would significantly increase the regulatory burden on some reporting entities. It would also significantly increase the volume of IFTI reports submitted to AUSTRAC.

In view of this, an assessment of the viability and impacts of expanding IFTI reporting requirements to include the reporting of transactions undertaken using credit/debit cards should be undertaken.

The ML/TF risks associated with international transactions that involve the withdrawal of cash from ATMs located in Australia using foreign-issued cards should also be assessed. There is evidence that ATMs located in Australia are being used to withdraw cash from overseas accounts held with financial institutions located

[207] Mechanisms for providing exemptions to reporting entities from AML/CTF obligations are discussed at *Chapter 17: Exemption process.*

in a foreign country. These cash withdrawals enable individuals in Australia to access funds that have been diverted offshore to evade tax. Information about these transactions is not currently reported to AUSTRAC as this type of transaction does not fall within the EFTI and IFTI requirements in the AML/CTF Act. The absence of reporting obligations for these transactions makes ATM withdrawals from foreign accounts an attractive methodology for transferring illicit funds into Australia. Options to impose reporting obligations, whether as a type of IFTI or as a new report type, should be explored.

Information collected in IFTIs

Currently, a number of reporting entities that provide a large volume of reports to AUSTRAC are also reporting additional payment information pursuant to a notice issued by AUSTRAC or a partner agency under section 49 of the AML/CTF Act. This payment information includes details about the payee (for example, BSB number, account number, full account name, family name, birthdate, address, sequence number and, if relevant, business name, Australian Company Number, Australian Business Number and Australian Registered Body Number).

AUSTRAC and partner agencies ask for this additional information to better understand who the payment is going to and the details underlying the payment. This type of information is particularly important for combating terrorism financing and the threat posed by Australians involved in foreign conflicts.

During the course of the review, AUSTRAC received additional government funding to combat the threat posed by foreign fighters by enhancing its data capture and integrity process for transaction reports. This project, which is anticipated to be completed by late 2017, seeks to optimise how transaction data is obtained and transformed by AUSTRAC systems. It is also intended that this project will lead to changes in the types of information required to be reported in IFTIs. These changes may see additional types of information reported in IFTIs, such as mobile phone numbers, email addresses and IP addresses, that will better equip law enforcement agencies to detect and disrupt terrorism and foreign fighters.

These changes will help align the IFTI reporting requirements with the types of additional payment information agencies are currently requiring reporting entities to provide under section 49 of the AML/CTF Act. This harmonisation will reduce the need to use section 49 in this manner and address the concerns of some stakeholders that the section 49 power was being used to address gaps in IFTI reporting requirements.[208]

Partner agencies recommended that consideration be given to including other types of information in the IFTI requirements (for example, tax file number and the payment method for ordering the IFTI) to enhance Australia's ability to combat money laundering and terrorism financing. Additional changes to the information required to be reported in IFTIs should be explored in conjunction with the foreign fighters initiative.

Reporting of IFTI-DRAs

The definition of a designated remittance arrangement under Section 10 of the AML/CTF Act is very broad and inadvertently imposes IFTI-DRA reporting obligations on reporting entities that are not operating remittance businesses. This issue is addressed in *Chapter 11: Remittance sector* as part of a wider discussion about the implications of the current definition of a designated remittance arrangement.

Addressing deficiencies identified in the MER

Australia implements the FATF's wire transfer requirements through the EFTI requirements under Part 5 of the AML/CTF Act. These EFTI requirements largely reflect the 2003 FATF standards.

[208] See *Chapter 15: Audit, information-gathering and enforcement* for consideration of this issue.

The changes to the FATF standards in 2012 significantly altered the requirements for wire transfers and the MER considered that Australia did not meet the newer FATF standards. To address these deficiencies, the AML/CTF Act should be amended to better align with the FATF standards for wire transfers as outlined below.

The EFTI requirements should be reformed to better meet the FATF's requirements to include and pass on information about originators and beneficiaries in wire transfers. In some cases, reporting entities are already collecting this information. For example, Australian financial institutions already collect information about overseas beneficiaries in order to make IFTI reports to AUSTRAC, meaning this information should already be available to include in wire transfers as per the requirements set out in Chapters 16 and 17 of the AML/CTF Rules. Similarly, while Part 5 does not require that information about originators be verified, reporting entities should already be verifying information about their customers as part of their CDD obligations.

The MER noted a lack of several requirements for ordering, beneficiary and intermediary financial institutions to ensure that wire transfers comply with the FATF's information requirements and that the risks associated with non-complaint wire transfers are mitigated. These requirements currently form part of reporting entities' overarching requirements to manage and mitigate their ML/TF risks, including transaction monitoring.

The MER concluded that obligations for remitters do not comply with the newer standards. Including designated remittance arrangements in the funds transfer chain will ensure that information on the customers of remitters is included in wire transfers and supports the proposed reforms to reduce duplication of IFTI reporting by remitters and financial institutions discussed below.

The MER also considered that there is a lack of freezing action undertaken in wire transfers in relation to Australian sanction law. This is an inaccurate assessment. Financial institutions are already subject to Australia's general sanction law that criminalises the use of, or dealing with, assets owned or controlled by individuals or entities designated for targeted financial sanctions. It is also a serious criminal offence to make assets available, directly or indirectly, to designated persons or entities.[209] This includes where the financial institution is conducting a wire transfer.

Other FATF members have already implemented these changes, or are considering these changes.[210] If Australian reporting entities are not required to obtain the relevant wire transfer information, it could potentially delay international payments in and out of Australia. In the long term, this may impact on Australia's reputation as a country with an efficient and modern financial system.

The New Payments Platform

The New Payments Platform (NPP) is a major industry initiative driven by the Reserve Bank of Australia, Australian Payments Clearing Association and NPP Australia Limited (which comprises representation from 13 financial institutions).[211]

The NPP is currently under construction and is expected to be operational in late 2017. It will provide a centralised infrastructure for conducting payments in real-time and is expected to offer substantial efficiency gains to businesses and customers.

---

[209] See *Chapter 15: Audit, information-gathering and enforcement* for further information of Australian sanction law.
[210] For example, the FATF found Malaysia has fully implemented the FATF's revised wire transfer requirements (FATF Recommendation 16) as part of its mutual evaluation. Financial Action Task Force, *Malaysia: Mutual Evaluation Report*, September 2015, paragraph a5.89, http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-malaysia-2015.html.
[211] See the Australian Payments Clearing Association's website for further information on the NPP: http://www.apca.com.au/about-payments/future-of-payments/new-payments-platform-phases-1-2, (accessed 15 January 2016).

The NPP provides substantial challenges and opportunities for the AML/CTF regime, particularly for transaction reporting in regard to data integrity, timeliness and accuracy and the range of information that could be reported. It also presents opportunities to significantly reduce the compliance and regulatory burden on reporting entities.

In view of this, AUSTRAC and AGD should closely monitor the progress of the NPP and continue to engage with its primary participants.

Threshold transaction reports

If a reporting entity provides a designated service to a customer that involves the transfer of physical currency (or e-currency) of AUD10,000 or more (or the foreign currency equivalent), the reporting entity must submit a TTR to AUSTRAC.

The requirements for TTR reporting are set out in section 43 of the AML/CTF Act. Chapter 19 of the AML/CTF Rules set out the reportable details. Similar requirements to submit SCTRs apply to entities which remain regulated under the FTR Act.

Consultation

Industry stakeholders asked for a review of the range of information collected in TTRs and for aspects of the legal framework for TTRs to be clarified. In particular, stakeholders sought clarification of the TTR reporting requirements in circumstances where a customer conducts multiple cash transactions with a total value of AUD10,000 or more during a single visit. While some stakeholders sought clarity through greater prescription in the AML/CTF Act and Rules, others asked for enhanced guidance.

Most stakeholders supported an increase in the threshold to a minimum of AUD15,000 to reflect the impact of inflation, but partner agencies generally supported retaining the current threshold of AUD10,000.

The ALRC has previously expressed concerns about 'the pervasive nature of the monitoring that is to occur due to the mandatory reporting threshold of $10,000'. In 2008 the ALRC recommended that "the threshold should be reviewed to reflect price inflation and minimise the unnecessary collection of personal information".[212]

The findings of the MER

While the FATF standards do not require the reporting of currency transactions above a fixed amount, they do anticipate countries requiring the reporting of large cash transactions.[213]

Discussion

Clarifying TTR obligations

Prescribing TTR obligations in more detail in the AML/CTF Rules is impractical, as it is difficult to anticipate the different ways that customers conduct transactions. In view of this, AUSTRAC should clarify TTR obligations by providing reporting entities with more guidance, which should be developed in consultation with industry.

Thresholds

While the mandatory reporting of cash transactions above a specified threshold is not a FATF requirement, Australia and a number of countries impose TTR reporting obligations because of the ML/TF risks posed by

[212] Australian Law Reform Commission, 12 August 2008, *For Your Information: Australian Privacy Law and Practice,* ALRC Report 108, paragraph 6.81, http://www.alrc.gov.au/publications/report-108.
[213] FATF Recommendation 29 (Financial intelligence units).

transactions that involve large amounts of cash. The obligation to report such transactions disrupts attempts by criminals to place large amounts of cash into the financial system and provides law enforcement with valuable intelligence.

In 2014-15 almost 4.7 million TTRs and SCTRs were reported to AUSTRAC with a combined value of AUD169 billion.[214]

Case study 11 below demonstrates how TTR reporting can disrupt criminal activity

CASE STUDY 11: INFORMATION FROM INDUSTRY HELPED EXPOSE SUSPECT FUNDS TRANSFERS TO CHINA[215]

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

The person came to the attention of AUSTRAC after reporting entities submitted a series of SMRs detailing the suspect's activities. Further investigations revealed that the suspect had been making regular cash deposits into a personal bank account. The source of these cash deposits could also not be established and there was no evidence of the suspect receiving salary payments into the bank account from any employer.

On occasion, the suspect would present cash in amounts of about AUD9,900 to pay for international funds transfers to individuals who were assessed to be the suspect's relatives in China. The amounts involved strongly suggested to reporting entity staff that the suspect was deliberately structuring the cash payments to fall just below the AUD10,000 TTR threshold. The suspect conducted 28 international funds transfers totalling approximately AUD295,000, most of which were for the amount of AUD9,900. The suspect was charged and prosecuted under section 142 of the AML/CTF Act for conducting transactions to avoid reporting requirements and sentenced to four months imprisonment.

The implementation of mandatory reporting thresholds for cash transactions is likely to increase globally over the coming years, particularly in light of recent terrorist incidents. The French Government has already announced in March 2015 a series of new measures to counter terrorism and terrorism financing following the release of a report on terrorism financing.[216] A key concern raised in this report is the "ability of certain terrorist networks to secure underground funding, often in the form of small sums", as demonstrated by the terrorist attacks in Paris in January 2015 (and later in November 2015 attacks). New measures being adopted by the French Government include the systematic reporting of any cash deposits and withdrawals with a combined value of more than EUR10,000 (over a single month) to France's financial intelligence unit from 1 January 2016.

Similarly, New Zealand has recently introduced a cash transaction reporting requirement, with the threshold set at NZD10,000.[217]

Of the countries that already require TTR reporting, the nominated threshold that triggers the reporting obligation varies, as demonstrated by Table 4.

TABLE 4: COMPARISON OF CASH TRANSACTION REPORTING THRESHOLDS ACROSS SEVEN JURISDICTIONS

	Australia	United States	United Kingdom	New Zealand	Canada	Singapore	Hong Kong

[214] See *Appendix 3* for data on the volume and value of TTRs from 2007-08 to 2014-15.
[215] Source: AUSTRAC.
[216] DP Lutte contre le financement de terrorisme anglais, *Countering Terrorist Financing,* March 2015.
[217] In November 2015, the New Zealand Parliament passed the *Anti-Money Laundering and Countering Financing of Terrorism Amendment Act 2015*. This Act introduces a requirement that a reporting requirement for domestic physical cash transactions, as well as an international wire transfer reporting requirement (above a NZD1,000 threshold). The reporting requirements are not yet in force, but commence on 1 January 2017. See the New Zealand government's website for further information: http://www.beehive.govt.nz/sites/all/files/FAQs_-_Organised_Crime_and_Anti-corruption_Bill.pdf, (accessed 15 January 2016).

	Australia	United States	United Kingdom	New Zealand	Canada	Singapore	Hong Kong
Threshold (local currency)	AUD 10,000	USD 10,000	No reporting requirement	NZD 10,000	CAD 10,000	SGD 10,000[218] / 20,000[219]	No reporting requirement
Threshold (AUD)[220]	AUD 10,000	AUD 13,829	No reporting requirement	AUD 9,352	AUD 9,958	AUD 9,719 / 19,437	No reporting requirement

The threshold of AUD10,000 was originally set in 1988 for SCTR reporting under the FTR Act.[221] Since that time, several factors have impacted on the number of TTRs reported:

- Australia's population has increased from 16.5 million in 1988 to 24 million in 2016.
- There has been a significant increase in the value of AUD10,000 due to inflation, with the AUD10,000 threshold set in 1988 now equivalent to AUD21,311.[222]
- The purchasing power of the Australian dollar has also increased significantly since 1988. Notwithstanding inflationary effects, AUD10,000 has more than double the purchasing power in 2015 than it would have had in 1988, particularly as a range of commodities, including luxury commodities, are more affordable for a wider range of people.[223]
- There has been a significant uptake and usage of credit and debit cards in Australia, particularly with the emerging uptake of 'near field communications' such as PayWave, resulting in a decrease in the use of cash. Cash however remains the method of choice for the purchase of illicit products, such as illicit drugs or stolen goods.

Overall, the number of TTRs has plateaued in recent years due primarily to the overall decline in the use of cash in Australia.[224]

While the impact of inflation on the relative value of the threshold over time provides a strong argument for the threshold to be increased, any increase in the threshold will lead to a loss of financial intelligence for AUSTRAC and its partner agencies. A substantial number of TTRs received by AUSTRAC involved transactions valued between AUD10,000 and AUD14,999. For example, during the period May 2014 to May 2015, 39 per cent of TTRs received by AUSTRAC involved transactions valued between AUD10,000 and AUD14,999.

If a TTR threshold of AUD15,000 had been applied during this period, more than 1.8 million reports would not have been submitted to AUSTRAC.

Some TTRs involving amounts between AUD10,000 and AUD14,999 have provided valuable intelligence to authorities. On occasion, reporting entities that have submitted multiple, related TTRs have also been prompted to submit corresponding SMRs to AUSTRAC. However, any series of apparently suspicious transactions involving the same customer and large amounts of cash should be identified by reporting

[218] Cash transaction reporting requirement for casinos.
[219] Cash transaction reporting requirement for dealers in precious metals and stones.
[220] At 4 January 2016.
[221] Section 3 of the FTR Act.
[222] Reserve Bank of Australia, *Inflation Calculator*, http://www.rba.gov.au/calculator/annualDecimal.html, (accessed on 15 January 2016).
[223] The equivalent buying power of AUD10,000 in 2015 would have been AUD4,481 in 1988. See Australian Bureau of Statistics, *Consumer Price Index Inflation Calculator*, http://www.abs.gov.au/websitedbs/d3310114.nsf/home/Consumer+Price+Index+Inflation+Calculator, (accessed on 15 January 2016).
[224] See *Appendix 2*.

entities as part of their general obligation to scrutinise transactions (regardless of whether the relevant transactions also trigger a TTR reporting requirement).

Partner agencies strongly objected to raising the threshold to AUD15,000 on the grounds that it would allow more cash to be laundered more quickly. Criminals would be able to increase the value of each transaction by 50 per cent while continuing to remain under the new threshold. An increase would also reduce the frequency of contact between the launderer and the business, providing less information to indicate structuring of transactions and fewer opportunities for detection and intelligence collection. In addition, while bona fide transactions are increasingly conducted online, the purchase of illicit goods remains largely cash-based, enhancing the value of the TTR reporting requirement.

In view of this, the TTR threshold should remain at AUD10,000. However, AUSTRAC should take a more proactive approach to providing exemptions from TTR reporting where a service, or the circumstances within which a service is provided, poses a low ML/TF risk. To date, only a limited number of exemptions from the TTR obligations have been provided.[225]

Suspicious matter reports

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. The conditions under which a reporting entity must submit an SMR to AUSTRAC are set out in section 41 of the AML/CTF Act. Chapter 18 of the AML/CTF Rules sets out the reportable details for SMRs.

Similar requirements to submit SUSTRs apply to entities which remain regulated under the FTR Act.

Consultation

Industry stakeholders considered the reporting of suspicious matters to be appropriate to achieve the outcomes of the AML/CTF regime. Some stakeholders called for greater prescription or more objective criteria to assist reporting entities to determine whether a suspicion has arisen.

The findings of the MER

The MER found Australia to be compliant with the FATF standards for reporting suspicious matters.[226] However, the MER also noted that the SMR requirements do not apply to most DNFBPs, as Australia's AML/CTF regime only regulates casinos and bullion dealers within the DNFBP sector.[227]

Discussion

The SMR provisions under the AML/CTF Act appear to be working well. In 2014-15, reporting entities submitted a total of 81,074 reports of suspicious matters, a 21 per cent increase compared to 2013-14.[228] This total comprises SMRs submitted under the AML/CTF Act and a small number of SUSTRs submitted under the FTR Act. The SMR reports provided by reporting entities are of a relatively high quality, providing constructive descriptions of the suspicion that triggered the SMR.

SMR reports are used by AUSTRAC to generate financial intelligence or are provided directly to partner agencies. AUSTRAC automatically forwards some SMRs that involve a potential high risk to certain partner agencies within one hour of receipt. Other SMRs that are flagged according to indicators are made

[225] Chapter 31 of the AML/CTF Rules exempts certain transactions from the TTR requirement.
[226] FATF Recommendation 20 (Reporting of suspicious transactions).
[227] The coverage of DNFBPs under the AML/CTF Act is discussed in *Chapter 4.2: Regime scope – Designated non-financial businesses and professions.*
[228] See *Appendix 2* for data on the volume of SMRs from 2007-08 to 2014-15.

available within 24 hours. AUSTRAC refers these SMRs to partner agencies based on the nature of the alleged offence, risk or other material fact.

While stakeholders are seeking more prescriptive criteria for SMR reporting, the preferred approach is to better educate reporting entities on their SMR obligations through enhanced engagement and guidance.[229] SMRs are inherently subjective reports, as they rely on each individual's assessment of whether a suspicion has arisen. What constitutes suspicious behaviour will depend upon the particular circumstances of a particular transaction and cannot be legislated. In view of this, prescriptive requirements would not be appropriate.

Simplification of reporting

Consultation

Industry stakeholders strongly supported simplifying the legal framework for the reporting of IFTIs and TTRs by removing some of the duplication that occurs and streamlining transaction obligations.

Discussion

There are two types of IFTI reports – IFTI-Es and IFTI-DRAs. These reports recognise the different ways money or property is transmitted into or out of Australia and the range of entities who send or receive IFTIs into or out of Australia.

Since the commencement of the AML/CTF Act, an increasing number of remitters are using the formal financial system to transfer money on behalf of their customers. In these circumstances, two IFTI reports are required to be submitted – one from the provider of a designated remittance arrangement and one from the financial institution. Each report shows different customer information. This is largely a result of the funds transfer chain definition in the AML/CTF Act not extending to IFTI-DRAs.[230]

Streamlining information across different types of transaction reports would provide regulatory efficiencies to reporting entities. For example, currently when a customer transacts AUD10,000 or more of physical currency, and transfers those funds outside of Australia electronically through a financial institution, separate TTR and IFTI reports need to be submitted for the one transaction, rather than one consolidated report.

The reporting framework under the AML/CTF Act should be rationalised and streamlined to generate regulatory efficiencies. The AML/CTF Rules should be reviewed and amended to ensure that entities are only required to submit one report for a particular transaction in circumstances such as the example above.

[229] AUSTRAC already provides feedback to reporting entities on SMRs in a number of ways. This includes through regular publishing of AUSTRAC case studies and typology reports, and at industry meetings and forums. Specific feedback on SMRs is also provided to some reporting entities as part of their compliance assessments and ongoing regulatory engagement.

[230] See subsection 64(2) of the AML/CTF Act.

Recommendations

Recommendation 6.1

AUSTRAC to conduct an assessment on the viability and impacts of changes to the international funds transfer instruction reporting regime to:

(a) provide exemptions for international funds transfer instructions below a certain threshold, relating to specific low ML/TF risk designated services

(b) include the reporting of transactions undertaken using credit/debit cards, and

(c) expand the scope of information reported to AUSTRAC.

Recommendation 6.2

AUSTRAC should assess the ML/TF risks associated with international transactions that involve the withdrawal of cash from ATMs located in Australia using foreign-issued cards.

Recommendation 6.3

The AML/CTF Act should be amended to better align the electronic funds transfer instructions requirements with the FATF standards for wire transfers.

Recommendation 6.4

The AML/CTF Act and Rules should be amended to simplify and streamline transaction reporting obligations and produce regulatory efficiencies. This process should include:

(a) consideration of extending the funds transfer chain definition to providers of designated remittance arrangements

(b) reviewing the value of requiring transaction reports to be submitted by two entities involved in the one transaction, and

(c) allowing threshold transaction reports and international funds transfer instructions to be submitted as one report when they relate to the same transaction.

Recommendation 6.5

Changes to reporting requirements should occur concurrently with the proposed changes arising from AUSTRAC's Foreign Fighters Initiative.

Recommendation 6.6

AUSTRAC and the Attorney-General's Department should closely monitor the progress of the New Payments Platform and continue to engage with its primary participants.

7. AML/CTF programs

The AML/CTF Act requires reporting entities to develop and maintain a written AML/CTF program for their business. The program establishes the operational framework for reporting entities to meet their AML/CTF Act compliance obligations and sets out how reporting entities manage the risk of their products or services being misused for ML/TF.

AML/CTF programs comprise two parts:

- Part A covers how a reporting entity identifies, manages and reduces the ML/TF risks it faces, and
- Part B covers the reporting entity's CDD procedures.[231]

The AML/CTF Rules specify the primary components to be included within an AML/CTF program.

Reporting entities can have different types of AML/CTF programs depending on whether they are an individual entity or a member of a designated business group (DBG). Additionally, a 'special' AML/CTF program – which only includes the Part B component – applies to certain entities.[232]

Consultation

Overall, industry stakeholders indicated that the complexity of the AML/CTF program requirements generates uncertainty and ambiguity for reporting entities, particularly small and medium-sized businesses. They made suggestions to improve reporting entities' understanding of their obligations and promote better compliance. These include:

- simplifying AML/CTF program requirements
- developing AUSTRAC-approved templates to assist reporting entities to conduct ML/TF risk assessments and develop AML/CTF programs
- describing the role and function of AML/CTF compliance officers and maintaining competency standards and qualifications for this role
- clarifying how domestic AML/CTF program requirements should apply to permanent establishments offshore
- prescribing a minimum time frame for independent reviews, and
- expanding the DBG definition to allow a larger range of economic entities to take advantage of the DBG framework.

One partner agency suggested the introduction of an obligation for reporting entities to 'continuously disclose' to AUSTRAC serious breaches of the AML/CTF Act.

[231] See *Chapter 5: Customer due diligence* for further information on Part B of the AML/CTF program.
[232] For example, financial planners that hold an Australian Financial Services (AFS) license and arrange the provision of designated services for others.

The findings of the MER

The MER rated Australia partially compliant with the FATF standards covering the internal AML/CTF controls an entity must have in place to reduce its ML/TF risks. The MER identified two main deficiencies with AML/CTF program requirements:

- apart from the obligation to nominate a compliance officer at management level, reporting entities are not required to have any other compliance management arrangements, and
- the requirement for reporting entities to maintain an audit function to test their AML/CTF program is limited to Part A of the AML/CTF program and contains insufficient information on the frequency of the audit and the guarantee of its independence.[233]

The MER found that these 'internal control' deficiencies applied at the DBG level, as well as for individual reporting entities.

Other deficiencies identified in the MER include the lack of specific obligations requiring:

- reporting entities to take enhanced CDD measures to manage and mitigate higher ML/TF risks identified by the country and incorporate this information into their risk assessments[234]
- Australian reporting entities with branches or subsidiaries that operate overseas to require those branches or subsidiaries to comply with Australian AML/CTF standards in relation to Part A of an AML/CTF program, including the AML/CTF risk awareness training and employee due diligence programs, and[235]
- reporting entities to manage and mitigate the ML/TF risks posed by new technologies.[236]

Discussion

Simplifying AML/CTF program requirements

The AML/CTF program requirements are too complex and should be simplified to promote regulatory efficiencies and compliance with obligations.

The starting point for this process should be to merge the Part A and Part B program obligations into a single program obligation while maintaining existing program exemptions (for example, some businesses are currently only required to have a 'special' AML/CTF program that complies with the existing Part B requirements). The connection between obligations under the AML/CTF Act and the Rules also should be explicit, rather than implied, to ensure greater clarity.

Options should also be explored to permit reporting entities to adopt simplified AML/CTF programs where it can be demonstrated that the service provided represents a low ML/TF risk.[237]

Reporting entities should already be taking into account the guidance on higher ML/TF risk services and customers provided by AUSTRAC. To address the MER's concern and assist reporting entities to manage and mitigate their ML/TF risks, the AML/CTF program requirements should make it explicit that reporting entities are required to incorporate information provided by AUSTRAC or other relevant authorities on high ML/TF risks into their risk assessments.

---

[233] FATF Recommendation 18 (Internal controls and foreign branches and subsidiaries).
[234] FATF Recommendation 1 (Assessing risk and applying a risk-based approach).
[235] FATF Recommendation 18 (Internal controls and foreign branches and subsidiaries).
[236] FATF Recommendation 15 (New technologies).
[237] See *Chapter 17: Exemptions process* for further information on exemptions for low ML/TF risk.

Template AML/CTF programs and risk assessments

While some industry stakeholders were comfortable with the AML/CTF program requirements, others asked for greater prescription of the obligations and the development of AUSTRAC-approved 'templates' for risk assessments and AML/CTF programs.

The risk-based approach underpinning the AML/CTF regime focuses on building a culture of compliance among reporting entities. Under this approach, reporting entities must take responsibility for understanding the ML/TF risks associated with their business, and develop and implement an AML/CTF program to manage and mitigate those risks. They must also continuously monitor their ML/TF risks and adjust their AML/CTF measures accordingly.

The development of AUSTRAC-approved templates for risk assessments and AML/CTF programs is likely to undermine the objective of the risk-based approach, as some reporting entities, particularly those with limited resources, may simply adopt these templates without assessing and understanding their specific ML/TF risks and how these risks change over time.

The preferred approach is for AUSTRAC to develop tools and guidance that build the capacity of reporting entities to assess and understand risks and develop AML/CTF programs that respond to those risks. These tools should build on AUSTRAC's existing sector-specific guidance on understanding risk and developing AML/CTF programs.[238]

AML/CTF compliance officer requirements

While the AML/CTF Rules refer to tasks that AML/CTF compliance officers are authorised to perform, there is no description of the role and function of the AML/CTF compliance officer or compliance arrangements. [239] The AML/CTF Rules should be amended to address this issue and be accompanied by guidance to assist reporting entities to understand and implement this obligation.

Stakeholders supported the development of competency standards and qualifications for AML/CTF compliance officers to help build the capacity of reporting entities to comply with their obligations. In some regulatory settings, industry sets relevant standards for competency levels and training obligations for compliance officers under an industry code. Industry sectors regulated under the AML/CTF Act are well placed to understand the ML/TF risks faced by their members and in the best position to develop their own sector-specific standards for competency levels for AML/CTF officers.

Reporting serious breaches

There is no requirement under the AML/CTF Act for reporting entities to report serious breaches of AML/CTF obligations to AUSTRAC in a timely manner. This means that serious breaches may only be discovered by AUSTRAC when a reporting entity lodges an annual compliance report, as part of an audit or independent review, or as part of AUSTRAC's supervisory activities.[240] These measures do not sufficiently enable AUSTRAC to ensure that reporting entities are responding swiftly to serious breaches and implementing appropriate processes and procedures to prevent any further non-compliance.

To address this issue, reporting entities should be required to continuously disclose to AUSTRAC serious breaches of the AML/CTF Act. The open and transparent reporting of such breaches would enable AUSTRAC to quickly assess the nature and seriousness of the breach, ensure the breach is remedied, and

---

[238] See, for example, AUSTRAC's *AML/CTF compliance guide for hotels and clubs, AML/CTF compliance guide for independent remittance dealers* and *the AML/CTF compliance guide for bookmakers*, available on AUSTRAC's website: http://www.austrac.gov.au/businesses/obligations-and-compliance/industry-specific-guides, (accessed 15 January 2016).

[239] The requirement for reporting entities to designate a person as the AML/CTF compliance officer is set out in Part 8.5 and Part 9.5 of the AML/CTF Rules.

[240] See *Chapter 9: AML/CTF compliance reports* for further information.

determine if follow-up compliance or enforcement action is necessary. A continuous disclosure obligation would also contribute to a reporting entity's ML/TF risk mitigation.

The new obligation to notify AUSTRAC of a serious breach could be achieved through an online notification system. Obligations to remedy the serious breach would flow from existing provisions of the AML/CTF Act and Rules.

AUSTRAC should develop guidance to explain what would constitute a serious, 'reportable' breach to ensure reporting entities clearly understand this new obligation.[241]

To encourage compliance with the new obligation, reporting entities who self-report serious breaches should be eligible for a reduction in any pecuniary penalty that may apply to the breach. This approach is adopted under a number of other regulatory frameworks to encourage reporting of serious breaches and promote a culture of compliance.[242]

Independent review of AML/CTF programs

Part 8.6 of the AML/CTF Rules require entities to have Part A of their AML/CTF programs independently reviewed or 'audited'.

AUSTRAC guidance indicates that a reporting entity must determine how often it will arrange for the reviews to occur, depending on the 'nature, size and complexity of the business, and the type and level of ML/TF risk it might face'.[243] Some stakeholders found this requirement challenging and asked for a legislated minimum time frame to provide more certainty.

The requirement for reporting entities to determine the frequency of these reviews is consistent with the risk-based approach under the AML/CTF regime. It forms part of the broader expectation that reporting entities should understand and monitor their ML/TF risks, and make adjustments to their AML/CTF measures in response to those ML/TF risks. If a minimum time frame is prescribed, the risk is that reporting entities may elect to adopt the legislated minimum time frame for conducting independent reviews rather than monitor their ML/TF risks and consider whether more frequent reviews may be appropriate.

To assist reporting entities to comply with the requirements for independent reviews, AUSTRAC should amend its guidance to identify the factors that should be taken into account when determining the frequency of independent reviews and provide examples of circumstances that may trigger more frequent reviews. The development of this guidance would also address the FATF's concerns about insufficient information regarding the frequency of reviews.

The AML/CTF Rules should be amended to address the FATF's concern that there is no guarantee of the independence of the reviewer. While the AML/CTF Rules already provide that Part A of an AML/CTF program (either standard or joint) must be subject to a regular independent review by an internal or external party, an explicit requirement should be introduced to ensure that the reviewer (whether internal or external) has independence.

The review recommendation to merge Parts A and B into a single AML/CTF program requirement would also address the FATF's concern that the independent review requirement is limited to Part A of an AML/CTF program.

---

[241] See *Chapter 2: Overarching issues* for further information on issues relating to AUSTRAC guidance.

[242] For example, ASIC requires notification of serious breaches by AFS license holders and the Australian Prudential Regulation Authority (APRA) requires notification of serious breaches by APRA-regulated entities. Similarly, if general practitioners become aware of an incorrect Medicare payment and notify the Department of Human Services voluntarily, they may avoid an administrative penalty.

[243] AUSTRAC, *AUSTRAC compliance guide*, 'Regular independent review of Part A', www.austrac.gov.au/part-amlctf-program#independent-review, (accessed 15 January 2016).

Assessing the risk of new technologies

The FATF standards require regulated entities to assess, and take appropriate measures to manage and mitigate, the ML/TF risks posed by new products and new technologies prior to launching or using them.[244]

While the MER for Australia noted that the AML/CTF Rules require reporting entities to assess the ML/TF risks posed by new technologies prior to their adoption, the MER concluded that there is no explicit requirement for reporting entities to mitigate and manage these ML/TF risks.[245] To address the FATF's concerns, the AML/CTF Rules should be amended to specifically require the reporting entity to mitigate and manage the ML/TF risks posed by new technologies.

The proposed amendment is not likely to have a regulatory impact as reporting entities already have an indirect obligation to mitigate and manage the ML/TF risks posed by new technologies as part of their broader obligation to develop and implement an AML/CTF program that mitigates and manages the ML/TF risk the reporting entity may reasonably face.[246]

Designated business groups and joint AML/CTF programs

A DBG is a group of two or more associated businesses or persons who are reporting entities and join together to share certain obligations under the AML/CTF Act.[247]

Reporting entities that are able to form a DBG can have a joint AML/CTF program. This capability allows related entities to use common processes to address their AML/CTF obligations and minimise regulatory burden across the group. Importantly, reporting entities can share information about SMRs with fellow members of their DBG to manage their ML/TF risks without breaching the tipping-off provisions in the AML/CTF Act.[248]

By January 2016, 278 DBGs had formed under the AML/CTF Act, covering 1,745 reporting entities.

The DBG framework does not align with how businesses currently structure themselves into 'corporate groups', particularly businesses that are part of multi-national corporate groups. For example, one large financial institution in Australia has two DBGs within its corporate group. This restricts the ability of the institution to achieve regulatory efficiencies, share SMR-related information across the corporate group, and manage and mitigate its ML/TF risk at the corporate group level. The splitting of a corporate group across two DBGs also makes it difficult for AUSTRAC to effectively regulate and supervise reporting entities at the group level and monitor all aspects of the business conducted by a group worldwide. This is contrary to the Basel Committee on Banking Supervision's *Core Principles for Effective Supervision*, which the FATF standards require member countries to apply.[249]

The AML/CTF Act and Rules that provide for joint AML/CTF programs should be amended and replaced by a new DBG framework that allows an AML/CTF program to incorporate all reporting entities within a corporate group. The new framework should be flexible enough to allow the corporate group to adopt different risk structures and controls for different entities within the group, as appropriate. It should also

[244] FATF Recommendation 15 (New technologies).
[245] Subparagraphs 8.1.5(5) and 9.2.5(5) of the AML/CTF Rules.
[246] Part 7 of the AML/CTF Act.
[247] See section 5 of the AML/CTF Act and part 2.1 of the AML/CTF Rules for the DBG requirements.
[248] See *Chapter 14: Secrecy and access* for consideration of the limitations imposed by the tipping-off offence in sharing information between related entities.
[249] The Basel Committee is a global standard-setter for the prudential regulation of banks. FATF Recommendation 26 (Regulation and supervision of financial institutions) requires countries to follow the Basel Committee's core principle relating to consolidated group supervision for AML/CTF purposes. See Principle 12 – Consolidated supervision, Basel Committee on Banking Supervision, *Core Principles for Effective Supervision,* September 2012, http://www.bis.org/publ/bcbs230.htm, (accessed 15 January 2016).

allow financial institutions to include their foreign branches and subsidiaries in the AML/CTF program for the corporate group.

These amendments would deliver long-term regulatory efficiencies for reporting entities that belong to a corporate group and enhance the ability of AUSTRAC to supervise and monitor these reporting entities as necessary within the corporate group.

Extending AML/CTF program obligations to foreign branches and subsidiaries

Subsection 6(6) of the AML/CTF Act extends the application of the AML/CTF Act to foreign branches and subsidiaries of Australian financial institutions. Paragraphs 8.8 and 9.8 of the AML/CTF Rules set out the obligations that apply to foreign branches and subsidiaries.

The obligations that apply to foreign branches and subsidiaries do not comply with the FATF standards.[250] For example, there is no obligation for financial institutions to apply the higher standard where the AML/CTF requirements in the other country are less strict than Australia's and no obligation to inform AUSTRAC when the other country does not permit the proper implementation of AML/CTF measures consistent with Australia's AML/CTF regime. There is also no obligation on financial institutions to apply the AML/CTF risk awareness training and employee due diligence components of their AML/CTF programs to their foreign branches and subsidiaries.

The AML/CTF Act and Rules should be amended to strengthen the controls that apply to any branches or subsidiaries that a reporting entity operates in a foreign jurisdiction and align these controls with the FATF standards.

The supervision of offshore branches and subsidiaries of Australian reporting entities presents some practical difficulties for AUSTRAC. To overcome these difficulties, the AML/CTF Act should be amended to give AUSTRAC the power to require reporting entities that operate offshore branches and subsidiaries to have the AML/CTF programs for these branches and subsidiaries reviewed by a locally-based independent auditor. This audit report should be made available to AUSTRAC to verify the appropriateness of the branches and subsidiaries' AML/CTF programs.

The regulatory impact of these proposals to introduce controls for foreign branches or subsidiaries will depend upon the strength of the AML/CTF measures in the country hosting the branch or subsidiary. The weaker the AML/CTF measures are in the host country, the greater the regulatory burden to manage the more significant ML/TF risks poses by conducting business in that country.

Recommendations

Recommendation 7.1

The AML/CTF Act and Rules should be amended to merge and streamline the Part A and Part B requirements for AML/CTF programs into a single requirement for reporting entities to develop, implement and maintain an AML/CTF program that is effective in identifying, mitigating and managing their ML/TF risks.

[250] FATF Recommendation 18 (Internal controls and foreign branches and subsidiaries).

Recommendation 7.2

The AML/CTF Act should be amended to impose an obligation on reporting entities to report serious breaches of AML/CTF obligations to AUSTRAC in a timely manner. These amendments should also allow for any pecuniary penalty that may apply to a self-reported breach to be reduced or waived, where appropriate, and be accompanied by AUSTRAC guidance.

Recommendation 7.3

The AML/CTF Rules should be amended to:

(a) require reporting entities to incorporate information provided by AUSTRAC or other relevant authorities on high ML/TF risks into their risk assessments

(b) describe the roles and functions of an AML/CTF compliance officer and associated AML/CTF compliance arrangements

(c) guarantee the independence of the reviewer of AML/CTF programs, and

(d) require reporting entities to identify, mitigate and manage the ML/TF risks posed by new technologies.

Recommendation 7.4

AUSTRAC should develop guidance to assist reporting entities to:

(a) assess their ML/TF risks and develop AML/CTF programs, and

(b) determine how often independent reviews of their AML/CTF programs should be conducted.

Recommendation 7.5

The AML/CTF Act and Rules should be amended to replace the designated business group and joint AML/CTF program construct with a framework that allows an AML/CTF program to incorporate all reporting entities within a corporate group.

Recommendation 7.6

The AML/CTF Act and Rules should be amended to require reporting entities to:

(a) apply AML/CTF measures to its foreign branches and subsidiaries that are consistent with requirements under the AML/CTF Act where the AML/CTF measures in the other country are less strict than Australia's, and

(b) inform AUSTRAC where the foreign host country of foreign branches and subsidiaries does not permit the proper implementation of these AML/CTF measures.

Recommendation 7.7

The AML/CTF Rules should be amended to require reporting entities that operate branches or subsidiaries located in foreign countries to have the AML/CTF programs for these branches or subsidiaries reviewed by an independent auditor when required by AUSTRAC. The reporting entity should also be required to provide the audit report to AUSTRAC.

8. Record-keeping

Part 10 of the AML/CTF Act requires reporting entities to make and retain certain records for seven years. These requirements apply to:

- records relating to the provision of a designated service to a customer
- records of the ACIPs the entities undertake for customers to whom they provided, or proposed to provide, a designated service
- records of EFTIs
- AML/CTF programs, and
- due diligence assessments of correspondent banking relationships.

The AML/CTF Act and Rules do not prescribe a specific format in which the required records must be stored.

The AML/CTF Rules contain exemptions to these record-keeping obligations.[251]

Consultation

Industry stakeholders supported lowering the record-keeping retention period from seven years to five years to align with the FATF standards. There was also support for greater prescription as to what records should be kept by reporting entities.

One stakeholder considered that the AML/CTF Act should explicitly provide that reporting entities can retain records electronically, rather than in hard copy paper format.

The findings of the MER

The MER rated Australia as largely compliant with the FATF's record-keeping standard.[252] Three minor deficiencies were identified:

- there is no explicit obligation that transaction records be retained that are sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity
- reporting entities are not required to keep all account files and business correspondence because of the exemptions provided under the AML/CTF Act for certain documents, particularly customer-specific documents, and
- there are insufficient requirements to require reporting entities to make CDD information and transaction records swiftly available to competent authorities.

Discussion

Lowering the record-keeping retention period

Stakeholders recommended reducing the period for retaining records under the AML/CTF Act from seven to five years to harmonise AML/CTF Act requirements with those of the *Income Tax Assessment Act 1936* and the FATF standards, and provide some regulatory relief to reporting entities. A reduction would also

[251] Chapters 20 and 29 of the AML/CTF Rules.
[252] FATF Recommendation 11 (Record-keeping).

respond to concerns raised by the ALRC as part of a review of Australian privacy law and practice conducted in 2008. At that time, the ALRC recommended that the statutory review of the AML/CTF Act consider whether a retention period of seven years remained appropriate following concerns expressed through a public consultation process that it exceeded FATF requirements and represented unnecessary monitoring of the financial affairs of ordinary citizens.[253]

However, record-keeping obligations imposed on reporting entities under other legislation would significantly limit the deregulatory benefits of a reduction in the record-retention period under the AML/CTF Act. Around 80% of reporting entities are incorporated and required to retain business records for seven years under the *Corporations Act 2001.* Other unincorporated reporting entities are required by other legislation to retain records for seven years (for example, certain gaming service providers,[254] certain partnerships[255] and non-bank lenders[256]). The remaining reporting entities that could benefit are small businesses and any regulatory savings are likely to be negligible.

Partner agencies also argued that the requirement under the AML/CTF Act to keep records for seven years is useful for assisting complex investigations that can take many years to unfold.

In view of the limited deregulatory benefits associated with a lower retention period and the intelligence value of the records to law enforcement, the retention period should remain at seven years.

Addressing the minor deficiencies identified in the MER

Exemptions on retaining certain customer-specific records

The MER noted that the record-keeping exemptions provided in Chapter 29 of the AML/CTF Rules include exemptions from retaining routine correspondence and documents created for the purpose of submitting reports to AUSTRAC, particularly account statements. However, these exempt documents are not the types of records envisaged to be kept under the FATF standards, as they are not documents obtained through CDD. In view of this, these documents should continue to be exempt from the record-keeping requirements.

Reconstructing individual financial transactions

The MER noted that Australia does not have an explicit requirement that the transaction records retained by reporting entities must allow for the reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity. The MER recognised that this deficiency is mitigated to some extent by a broader complementary reporting framework consisting of other legislation and guidelines, which requires some reporting entities to retain sufficient data to reconstruct individual transactions.[257] In particular, Australia's unique TTR and IFTI reporting requirements means a large number of transactions are already required to be recorded in a manner that would enable the reconstruction of individual transactions.[258]

However, some reporting entities and transactions do not fall within this broader reporting framework. It is likely that businesses already keep sufficient records to reconstruct these transactions as part of normal business practices (e.g. retaining a receipt of the transaction). However, to ensure that there is no gap, the AML/CTF Act should be amended to explicitly require reporting entities to make and retain sufficient records to allow for the reconstruction of individual transactions.

---

[253] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC Report 108, 12 August 2008, http://www.alrc.gov.au/publications/report-108.
[254] See, for example, regulation 3.7.5 of the *Gaming Regulation Act 2003* (Victoria); section 141 of the *Gaming Control Act 1993* (Tasmania).
[255] See, for example, section 79E of the *Partnership Act 1958* (Victoria).
[256] See, for example, section 95 of the *National Consumer Credit Protection Act 2009.*
[257] For example, the *Australian Securities and Investment Commission Act 2001*, *Corporations Act 2001* and *Evidence Act 1995*.
[258] See *Chapter 6: Reporting obligations* for further information.

Making records swiftly available to authorities

The MER concluded that there are no specific requirements in the AML/CTF Act that require reporting entities to make records available to AUSTRAC and its partner agencies 'swiftly' in accordance with the FATF standards.

While reporting entities may have obligations to make records available to competent authorities under other legislation, law enforcement agencies have reported that lengthy delays sometimes occur in gaining access to reporting entities' records.

The AML/CTF Act should be amended to address this issue by requiring reporting entities to keep their AML/CTF records in a format that enables them to be provided to AUSTRAC and other relevant partner agencies swiftly.

Records required to be kept

Some stakeholders asked for greater prescription of what records should be kept by reporting entities. AUSTRAC should develop guidance to clarify this issue.

Recommendations

Recommendation 8.1

The AML/CTF Act should be amended to establish an explicit requirement that sufficient transaction records must be made and kept by reporting entities to enable reconstruction of individual transactions.

Recommendation 8.2

The AML/CTF Rules should be amended to establish an obligation that reporting entities maintain their AML/CTF records in a format that allows the records to be provided to AUSTRAC and partner agencies swiftly.

Recommendation 8.3

AUSTRAC should develop guidance to assist reporting entities to understand what records they should keep.

9. AML/CTF compliance reports

Section 47 of the AML/CTF Act requires reporting entities to lodge an annual compliance report (ACR) to AUSTRAC that outlines the reporting entity's compliance with the AML/CTF Act, Rules and Regulations. These provisions also allow a member of a DBG to lodge an ACR on behalf of all members of the DBG.

Consultation

Some industry stakeholders considered that the ACR requirements are too onerous and could be streamlined. They proposed two alternative models for compliance reporting:

- a declaration model under which reporting entities testify to their compliance (or non-compliance) with their AML/CTF obligations on an annual basis, and
- a senior management compliance reporting model under which the AML/CTF compliance officer submits an annual report to senior management on the business's AML/CTF compliance, with reports to be made available to AUSTRAC upon request and admissible in court.[259]

The findings of the MER

The MER contained no specific recommendations about AML/CTF compliance reporting, but considered that ACRs could be improved to provide better visibility of the effectiveness of reporting entities' AML/CTF programs.[260]

Discussion

There are approximately 6,500 reporting entities that are required to lodge an ACR. The information collected informs AUSTRAC's risk-based approach to supervision. Some reporting entities are exempted from lodging ACRs.[261]

The format for the ACR currently comprises an online questionnaire with fixed-choice responses across 22 question areas. This format is unduly onerous and the content of the questionnaire has become outdated.

In view of this, AUSTRAC should develop a new compliance reporting process in consultation with industry that reduces the regulatory burden on reporting entities while enhancing the value of the process to reporting entities and AUSTRAC.[262]

Recommendation

Recommendation 9.1

AUSTRAC should develop, in consultation with industry, a new compliance reporting process that is relevant to the information needs of AUSTRAC and reduces unnecessary regulatory burden.

[259] This reflects the model used in the United Kingdom.
[260] Paragraph 6.19 of the MER.
[261] Exempt entities include remittance network providers and their affiliates, certain financial planners and small gaming venues.
[262] AUSTRAC commenced a review of its compliance reporting framework during 2014-2015. This included public consultation conducted during October and November 2014 on a draft *Regulation Impact Statement – Proposed changes to the annual compliance report* (RIS). See AUSTRAC's website for further information: www.austrac.gov.au/consultation-paper-austrac-proposed-changes-annual-compliance-report, (accessed 15 January 2016).

10. Correspondent banking

Correspondent banking is the provision of banking services by one financial institution (the 'correspondent') to another financial institution (the 'respondent').

These banking relationships are vulnerable to misuse for ML/TF purposes because they involve a financial institution carrying out transactions on behalf of another financial institution's customers where information on those customers is very limited. The ML/TF risks associated with these banking relationships are particularly high where the respondent bank is located in a country where there are weak regulatory AML/CTF controls and/or poor supervision of these controls.

The obligations relating to correspondent banking relationships are set out in Part 8 of the AML/CTF Act and Chapter 3 of the AML/CTF Rules. The obligations apply to correspondent financial institutions based or operating in Australia and require them to:

- undertake a preliminary ML/TF risk assessment before entering into a correspondent banking relationship[263]
- perform a due diligence assessment if warranted by the ML/TF risk identified in the preliminary assessment[264]
- conduct regular ML/TF risk assessments after entering into correspondent banking relationships, and
- conduct regular due diligence assessments if warranted by the risk identified in the ML/TF risk assessment.[265]

A number of other obligations relating to correspondent banking relationships are specified under section 99 of the AML/CTF Act, including requirements for approval from senior officers and requirements for documentation.

The AML/CTF Act also prohibits financial institutions from:

- entering into a correspondent banking relationship with a shell bank or another financial institution that has a correspondent banking relationship with a shell bank,[266] and
- continuing to do business with a correspondent bank that becomes a shell bank.[267]

Consultation

Industry stakeholders indicated that the correspondent banking obligations are too complex, cumbersome and difficult to understand. They also considered that the definition of correspondent banking under the AML/CTF regime is too prescriptive and fails to recognise the different approaches taken to correspondent banking relationships globally.

Some stakeholders sought greater clarity surrounding the due diligence requirements for *nostro* and *vostro* accounts and the requirement to assess the risk of the ownership and control structure of the other financial institution.[268]

---

[263] Subsection 97(1) of the AML/CTF Act.
[264] Subsection 97(2) of the AML/CTF Act.
[265] Section 98 of the AML/CTF Act.
[266] Section 95 of the AML/CTF Act. The FATF defines a 'shell bank' to be a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision.
[267] Section 96 of the AML/CTF Act.

The findings of the MER

The MER noted major shortcomings in Australia's compliance with the FATF standards for correspondent banking, rating Australia as non-compliant.[269] The key deficiencies identified include:

- there is no mandatory requirement to conduct due diligence assessments for correspondent banking relationships
- financial institutions are not required to consider the quality of ML/TF supervision conducted in the country of the respondent institution in the due diligence assessment
- there are no requirements with respect to 'payable-through accounts', and
- the extent of the prohibition on entering into a correspondent banking relationship with a shell bank is unclear.

Discussion

Simplify and streamline obligations

The correspondent banking obligations under the AML/CTF Act and Rules are unduly complex and do not comply with the FATF standards. These obligations should be amended to establish a one-step process that enhances compliance with the FATF standards by requiring financial institutions to conduct a due diligence assessment before entering into any correspondent banking relationship.

The new one-step process will streamline obligations, but will remove financial institutions' discretion to conduct due diligence assessments. While this new approach will increase the regulatory impost on reporting entities, it is consistent with the FATF standards and recognises the inherent ML/TF risks posed by correspondent banking relationships.

The due diligence assessment under the new process should continue to include the matters listed in paragraph 3.1.2 of the AML/CTF Rules, as well as a new requirement that financial institutions consider the quality of ML/TF supervision in the country of the respondent institution. This will also strengthen compliance with the FATF standards.

The AML/CTF Act and Rules should also be amended to simplify requirements, and guidance developed to assist financial institutions to comply with key obligations. This should clarify for institutions:

- how to conduct a due diligence assessment
- the factors to be considered in determining the risks posed by the management structure of a respondent bank, and
- the due diligence requirements regarding *nostro* and *vostro* accounts.

AUSTRAC should also develop guidance to indicate the types of AML/CTF responsibilities that should be documented for a correspondent banking relationship.[270]

Broadening the correspondent banking definition

A correspondent banking relationship is defined under the AML/CTF Act as a relationship where one financial institution provides banking services to another financial institution.[271] A financial institution is

[268] A *nostro* account means a bank account held in a foreign country by a domestic bank, denominated in the currency of that country. A *vostro* account means the account that a correspondent bank holds on behalf of a foreign bank. See paragraph 3.1.2(7) of the AML/CTF Rules for obligations in relation to assessing the risks associated with ownership and control structures.
[269] FATF Recommendation 13 (Correspondent banking).
[270] See *Chapter 2: Overarching issues* for further information on issues relating to AUSTRAC guidance.

defined under the AML/CTF Act as a bank, a building society, a credit union, an authorised deposit-taking institution or a person specified in the AML/CTF Rules.[272]

The definition of a correspondent banking relationship is unduly narrow, failing to recognise other correspondent banking arrangements that financial institutions can enter into with foreign entities that are not considered to be financial institutions for the purposes of the AML/CTF Act.[273] This has regulatory implications. Financial institutions that enter into correspondent banking relationships with such foreign entities must comply with the more stringent CDD obligations under Chapter 4 of the AML/CTF Rules for services provided under the relationship, rather than only conducting a due diligence assessment of the foreign entity itself.

Stakeholders strongly supported adopting a broader definition of correspondent banking relationships that aligns with the *Wolfsberg Anti-Money Laundering Principles for Correspondent Banking.*[274] Under the Wolfsberg principles, correspondent banking is 'the provision of banking services by an authorized institution to another institution to enable the latter to provide services and products to its own customers'.[275] The breadth of the definition recognises the different approaches taken to correspondent banking relationships globally.[276]

The AML/CTF Act should be amended so that the definition of correspondent banking relationship aligns with modern global approaches to correspondent banking arrangements.

Addressing other deficiencies identified in the MER

Payable-through accounts

The FATF defines payable-through accounts as correspondent accounts that are used directly by third parties to transact business on their own behalf, rather than by a correspondent bank conducting transactions on behalf of its customers.[277] These accounts are recognised globally as posing high ML/TF risks for a financial institution, particularly if the financial institution does not have access to information about the third parties accessing the account.

The AML/CTF Act should be amended to include specific due diligence measures for payable-through accounts that are consistent with the FATF standards to address the significant ML/TF risks they pose.

Shell banks

Financial institutions are prohibited from entering into correspondent banking relationships with another financial institution that has a correspondent banking relationship with a shell bank.[278] Financial institutions are also required to terminate a correspondent banking relationship if they become aware that a respondent bank has a correspondent banking relationships with a shell bank.[279] However, financial institutions are not required to satisfy themselves that a respondent financial institution that they are

---

[271] Section 5 of the AML/CTF Act.
[272] *Ibid.*
[273] Different jurisdictions have different definitions for financial institutions and banks.
[274] The Wolfsberg Group of International Financial Institutions has agreed upon principles to constitute global guidance on the establishment and maintenance of Foreign Correspondent Banking relationships. These principles are published online at http://www.wolfsberg-principles.com.
[275] Wolfsberg Group of International Financial Institutions, *Wolfsberg Anti-Money Laundering Principles for Correspondent Banking*, 2014, http://www.wolfsberg-principles.com, (accessed 15 January 2016).
[276] For example, under the *Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance* correspondent banking is defined for AML/CTF purposes in Hong Kong as "the provision of banking services by an authorized institution to another institution to enable the latter to provide services and products to its own customers".
[277] Financial action Task Force, *The FATF Recommendations*, p. 69, February 2013, http://www.fatf-gafi.org/topics/fatfrecommendations/documents/fatf-recommendations.html.
[278] Section 95 of the AML/CTF Act.
[279] Subsection 96(2) of the AML/CTF Act.

entering into a correspondent banking relationship with does not permit its accounts to be used by shell banks. This is inconsistent with the FATF standards.

The AML/CTF Act should be amended to explicitly require that financial institutions are satisfied that their respondent banks' accounts cannot be used by shell banks to comply with the FATF standards. This amendment is likely to have a minor regulatory impact as it is industry best practice for financial institutions to conduct due diligence on their respondent banks to ensure they do not enter into a correspondent banking relationship that may later expose their business to significant ML/TF risks.

Recommendations

Recommendation 10.1

The AML/CTF Act and Rules should be amended to simplify and streamline the correspondent banking obligations to establish a one-step process for conducting due diligence assessments on respondent financial institutions that is consistent with the FATF standards.

Recommendation 10.2

The AML/CTF Rules should be amended to require financial institutions to consider the quality of ML/TF supervision conducted in the country of the respondent institution as part of the due diligence assessment.

Recommendation 10.3

The AML/CTF Act should be amended to:

(a) broaden the definition of correspondent banking in line with international approaches that are consistent with the FATF standards

(b) require financial institutions to undertake specific due diligence in relation to payable-through accounts consistent with the FATF standards, and

(c) prohibit financial institutions from entering into a corresponding banking relationship with an institution that is able to enter into a correspondent banking relationship with a shell bank.

11. Remittance sector

Remittance or money transfer businesses (remitters) are non-bank financial entities that transfer money on behalf of others. Remitters provide a relatively quick, low cost service, giving customers access to foreign regions and countries with limited or no financial infrastructure. Migrant communities and workers commonly use remitters to send money home to many developing countries around the world.

The remittance sector globally is diverse, ranging from large organisations that oversee international remittance networks to smaller, informal money transfer systems that often operate outside the regulated financial system.[280] The services provided by remitters are considered to pose a higher ML/TF risk than most other sectors because they operate outside of conventional banking system and involve sending money to places that do not have established, modern banking networks.[281]

Any person providing a remittance service in Australia is a reporting entity for the purposes of the AML/CTF Act and subject to AML/CTF compliance and reporting obligations. In 2011, these obligations were significantly enhanced and registration requirements introduced.[282] Remitters must now register with AUSTRAC and reapply for registration every three years. Any person seeking registration must provide AUSTRAC with information relevant to their suitability for registration and allow AUSTRAC to obtain information from other persons to determine their suitability. The AUSTRAC CEO has the power to refuse, suspend, cancel or impose conditions on registration and sanction unregistered remitters with infringement notices.

Remitters make up a large number of the reporting entities covered by the AML/CTF Act, with over 5,700 separate reporting entities appearing on the Remittance Sector Register (RSR).[283] The sector's diversity ranges from international corporate-sized remitters with many affiliates (or sub-agents), through to micro-businesses with five or fewer staff and single person operators. For regulatory purposes, Part 6 of the AML/CTF Act defines three categories of remitters:

- Remitter Network Providers (RNPs) (81 separate entities)
- affiliates of RNPs (about 5,100), and
- independents (about 510).[284]

The top 20 remitters, mainly RNPs and some large independents, are responsible for 76 per cent of the total volume of IFTI reports and 83 per cent of the total value of IFTI reports submitted by the sector each year. Independents, which include large and small remitters, account for about 30 per cent of the sector's total IFTI report value. Although numerically large, remitters account for only about one per cent, and 11 per cent of the total volume, (AUD52 billion over 9.8 million IFTI reports) of all IFTIs into and out of Australia processed in 2015.

---

[280] Well known examples include the Middle East and North Africa's 'hawala' system, China's 'flying money' system, India's 'hundi' system and the Philippine's 'padala' system. See Australian Institute of Criminology, *Money Laundering and terrorism financing risks posed by alternative remittance in Australia,* 2010, AIC Reports: Research and Public Policy Series 106.

[281] AUSTRAC, *Money Laundering in Australia 2011*, 2011, http://www.austrac.gov.au/publications/corporate-publications-and-reports/money-laundering-australia-2011; AUSTRAC, *Terrorism Financing in Australia 2014*, 2014, http://www.austrac.gov.au/publications/corporate-publications-and-reports/terrorism-financing-australia-2014.

[282] *Combating the Financing of People Smuggling and Other Measures Act 2011*.

[283] At January 2016. Registrations exceed the number of remittance entities. Since an entity can be registered in more than one capacity (that is, as an independent and affiliate) and can also be an affiliate of more than one remitter network, the total number of registrations is over 6,000.

[284] Approximate numbers for each of the three categories have been used as numbers fluctuate weekly, reflecting the fluid entry and exit of businesses into and from the sector.

Consultation

Partner agencies and a number of industry stakeholders representing remitters supported stronger regulation of the remittance sector through a stringent licensing regime to more effectively mitigate the ML/TF risks. This included proposals for monitoring powers and tougher penalties for unregistered remitters.

Industry stakeholders considered that a licensing regime for remitters may improve the reputation of the sector within Australia. Over the past few years, Australian banks have been closing accounts held by some remitters. This is partly in response to concerns about the perceived reputational risks associated with servicing the remittance industry, including ML/TF risk and the risk of breaching sanctions laws. In some cases, this 'de-banking' was also a response to requirements imposed by international correspondent banks.[285]

De-banking of remitters has also occurred in other countries, including the United Kingdom and the United States of America.

Numerous stakeholders expressed concerns that de-banking could cause financial hardship for migrant communities and workers if it meant they were unable to access remittance services to send money overseas to their families and stressed the need for 'financial inclusion' in the provision of banking services.[286] Concerns were also raised that closing off access to bank accounts might lead remitters and their customers to shift towards unregulated, 'underground' financial systems.

A number of stakeholders commented that the definition of a designated remittance arrangement (DRA) under section 10 of the AML/CTF Act is too broad, generating uncertainty and unintended effects. For example, businesses that conduct transactions through a bank may be required to register with AUSTRAC as remitters even though their remittance activity is incidental to their core services (for example, superannuation funds and stockbrokers). As well as confining the registration requirement to remitters, stakeholders also recommended relieving entities not strictly operating as remitters from the obligation to report IFTI-DRAs.[287]

The findings of the MER

The MER found Australia's framework for remitters largely complies with the FATF standards, identifying only a few minor deficiencies.[288]

While remitters are registered and supervised by AUSTRAC, the MER considered that the implicit requirement for RNPs to monitor their affiliates' compliance with obligations was not sufficient to ensure monitoring was done in line with FATF standards. The MER recommended that this obligation be made explicit.

In its consideration of Australia's requirements for wire transfers,[289] the MER reported that the AML/CTF Act does not apply the same requirements to remitters as it does to intermediary and

[285] Financial Action Task Force, *Drivers for "de-risking" go beyond anti-money laundering / terrorist financing,* June 2015, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/derisking-goes-beyond-amlcft.html.
[286] The Global Partnership for Financial Inclusion on behalf of the G20 defines 'financial inclusion' to be a state in which all working age adults have effective access to credit, savings, payments, and insurance from formal service providers. Global Partnership for Financial Inclusion, *Global Standard-Setting Bodies and Financial Inclusion for the Poor: Toward Proportionate Standards and Guidance*, p. 7, http://www.gpfi.org/sites/default/files/documents/CGAP.pdf.
[287] IFTI-DRAs are IFTIs carried out through a designated remittance arrangement. See *Chapter 6: Reporting obligations* for further information.
[288] FATF Recommendation 14 (Money or value transfer services (MVTS)).
[289] FATF Recommendation 16 (Wire transfers).

beneficiary institutions, which includes collecting, passing on and verifying the accuracy and identification of information. This issue is considered in *Chapter 6: Reporting obligations*.

The MER also noted that representatives from the remittance sector reported to the FATF assessment team that the implementation of AML/CTF obligations, and the capacity to assess risk, varied greatly across the sector. Smaller remitters were generally seen as lacking the capacity to implement and comply with complex regulatory requirements.[290]

Discussion

There is a longstanding view held by Australian law enforcement, and expressed in national risk assessments, that the remittance sector poses a high ML/TF risk. The informal nature of remittance businesses and their ability to send money to foreign regions and countries with limited or no financial infrastructure, and potentially weak AML/CTF controls, makes them vulnerable to misuse by terrorists, terrorist groups and other criminals.

The recent closure of some remitter's accounts by banks reflects the banking sector's concerns about the varying levels of professionalism within the sector and the limited capacity of the sector to mitigate its vulnerability to ML/TF abuse. A significant number of remitters consulted during the review recognised that changes are required to improve the sector's professionalism and compliance with AML/CTF obligations if they are to operate in, and benefit from, a well-regulated financial system.

Close regulation of remitters is relatively recent. The enhanced registration system introduced in 2011 under the AML/CTF Act has improved oversight of the sector to some extent and removed many operators assessed as 'high risk'. RNPs are now responsible for undertaking due diligence of their affiliates and monitoring their compliance and transaction reporting.

This enhanced framework, along with the stronger registration process, has improved AUSTRAC's ability to monitor the sector, as the MER acknowledged.

AUSTRAC enforcement action has also increased. Since 2011, eleven remitters have had their registration cancelled, seven remitters have been refused registration, one remitter has had their registration renewal request refused, five remitters have been suspended from the RSR, and 18 remitters have had conditions imposed on their registration. Despite tighter regulation, unregistered and high-risk entities still operate in the sector. Three infringement notices have been issued to major RNPs for compliance breaches, including providing services through unregistered affiliates.

Enhanced registration has not prevented entry into the market of entities that lack the capacity to understand and comply with AML/CTF requirements, or the registering of remittance businesses associated with criminals. It is also suspected that criminals are re-entering the remittance sector (or 'phoenixing')[291] via remittance businesses registered by third parties (for example, family or associates), allowing them to continue operating or exerting a controlling influence over money laundering remittance businesses.

Major investigations, particularly under the Eligo National Task Force, have detected large-scale money laundering occurring in the sector, as case study 12 illustrates.

[290] Pages 86-87 and 160-161 of the MER.

[291] 'Phoenixing' generally refers to businesses or companies that close down (for instance, through liquidation, de-registration or lapsed registration or licensing) but resume business under a different name or legal form.

CASE STUDY 12: ELIGO NATIONAL TASK FORCE AND REMITTERS[292]

In 2011 AUSTRAC produced a classified National Threat Assessment (NTA) on Money Laundering[293] which assessed the overall money laundering threat from the alternative remittance sector as high. The NTA found that parts of the sector are easily exploited, making remitters an attractive money laundering channel with its strong links to high-risk countries and the involvement of domestic and global money laundering syndicates.

In December 2012 the ACC Board established the Eligo National Task Force to combat high-risk remitters and operators of other informal value transfer systems impacting Australia.

Eligo is focused on long-term prevention strategies, using criminal intelligence to disrupt money laundering, drive greater sector professionalism and make it harder for organised crime to exploit the remittance sector. By 31 December 2015, Eligo's operational outcomes included:

- cash seizures totalling more than AUD79 million
- drug seizures with an estimated street value of more than AUD1.4 billion (including methylamphetamine estimated at over AUD1.2 billion)
- seizure of 61 firearms
- restraint of more than AUD56 million worth of assets
- arrest of 417 people on 991 charges
- disruption of 61 serious and organised criminal groups/networks, and
- identification of more than 416 targets previously unknown to law enforcement.

Issues have also been identified in relation to AUSTRAC's regulatory oversight of unregistered remittance businesses. On 8 September 2015, the Parliamentary Joint Committee on Law Enforcement tabled its report on financial related crime. In its report, the Committee recognised that AUSTRAC had been criticised for not taking strong enough compliance action against operators who were not meeting their obligations under the AML/CTF regime, or complying with AUSTRAC's instructions. The Committee recommended that AUSTRAC consider and then implement mechanisms to increase its regulatory oversight of the activities of unregistered remitters.[294]

In response to the Committee's recommendation, AUSTRAC is reviewing its existing strategies for discovering and responding to unregistered remittance businesses. It is likely that this issue will be mitigated by a range of enhancements and measures outlined in this chapter and the broader report.

Alternative options for regulating remitters should be explored to:

- strengthen controls on entry to the sector to reduce the risk of criminal infiltration directly or through exploitation of low-compliance remitters, and
- introduce technical capacity requirements to operate a remittance business in order to promote professionalism, compliance and capacity to assess and mitigate risk.

[292] Source: Australian Crime Commission. See their website for further information: https://www.crimecommission.gov.au/organised-crime/joint-task-forces-and-initiatives/eligo-national-task-force, (accessed 15 January 2016).

[293] The sanitised version of the NTA is available on AUSTRAC's website. AUSTRAC, *Money Laundering in Australia 2011*, 2011, http://www.austrac.gov.au/publications/corporate-publications-and-reports/money-laundering-australia-2011.

[294] Recommendation 10, Parliamentary Joint Committee on Law Enforcement, *Report: Inquiry into financial related crime*, September 2015, http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/Financial_related_crime/Report.

Enhanced regulation

Law enforcement and sections of the remittance sector strongly supported enhancing regulation for remitters by shifting from the current registration scheme to a more stringent licensing system in line with approaches adopted overseas.[295] In particular, they supported the introduction of:

- tiered licensing, with categories of licenses based on the nature and scale of a remitter's business activities and the introduction of caps in the amounts that can be transferred under each category of license
- 'fit and proper person' tests to examine the probity and suitability of all key personnel, such as directors, managers, beneficial owners and any other persons who direct or control the business, and
- a technical capacity or competency requirement, where an applicant must demonstrate they understand and can meet the regulatory and compliance obligations to operate a remittance business (similar requirements and obligations are a feature of licensing regimes in the energy and gaming sectors and for holders for AFS licenses).

Representatives from the remittance sector supported the introduction of these regulatory measures on the basis that it may improve the reputation of the sector, while law enforcement considered that stronger regulation may assist with mitigating the ML/TF risks posed by remittance services.

The above options for licensing remitters, separately or in combination, would increase entry requirements for remitters, compliance costs for the sector and regulatory expense for government without necessarily delivering the desired outcomes. While stronger entry and compliance requirements may improve the capacity of the sector to understand and comply with AML/CTF obligations, the sector would continue to pose a high ML/TF risk because of the ability of remitters to send money to foreign regions and countries with limited or no financial infrastructure and weak AML/CTF controls.

Limiting the total value of funds a remitter can remit within a certain time period (for example, a month) is unlikely to mitigate these risks, as small operators that have reached their monthly limit could simply outsource transfers to other remitters that have not reached their limit. Imposing a transaction threshold (that is, only allowing a remitter to process a transaction up to a prescribed maximum value), in addition to a volume limit, would help mitigate some of these risks. However, transfers to high-risk countries for terrorism financing tend to involve small amounts of funds below any prescribed threshold. In any case, either option would require close AUSTRAC supervision to ensure remitters are complying with such transaction threshold requirements.

A tiered system with licensing tests would probably advantage larger and medium sized businesses, with repercussions for competitive neutrality. However, smaller non-affiliated remitters account for only a small share of the total value of transaction activity. Any movement of customers away from smaller, non-affiliated remitters is unlikely to be significant, and is likely to be outweighed by benefits in mitigating risk.

Enhancing or 'front-loading' registration requirements would expand AUSTRAC's current process for checking registration applications. At the time of registration, remitters would be required to answer questions that are currently included within the annual AML/CTF compliance report.[296] This approach would improve screening of remitters at the point of registration. 'Fit and proper person' and technical capacity tests would also lift the bar for entry and promote professionalism in the sector but may exclude

[295] Countries such as the United Kingdom, Ireland, Canada, Malaysia and European Union members have adopted licensing systems to strengthen remitter regulation.
[296] See *Chapter 9: AML/CTF compliance reports* for further information.

smaller businesses that tend to cater to some migrant communities and have an impact on the ability of these communities to remit money overseas.

Options for enhanced regulation should consider the risk of displacement (for example, high-risk customers, remitters and suspicious financial activities moving underground, out of AUSTRAC's regulatory oversight, by using alternative banking platforms) and broader economic factors, such as competitive neutrality, deregulation and financial inclusion.

Stronger regulation of one financial channel often has a displacement effect, with criminals shifting to less regulated channels to avoid detection. Partner agencies held concerns in 2011 that money launderers and criminals may go 'underground' to unregistered remitters once the new registration enhancements were introduced. However, AUSTRAC and its partner agencies have not found evidence to suggest this has happened. Instead, the remittance sector has grown steadily since 2011 with international funds flows from this sector increasing in volume and value.

More recently, AUSTRAC data has not shown any significant decline in IFTI funds flows reported to AUSTRAC since the issue of de-banking arose. Initial data from AUSTRAC suggests de-banked remitters have not gone underground but instead mainly moved to become affiliates of RNPs.[297]

The preferred approach to addressing the ML/TF risks posed by remitters is to enhance regulation under the existing registration process and give the AUSTRAC CEO stronger powers to control the registration of remitters. The AUSTRAC CEO currently has the power to cancel a remitter's registration where the registration involves, or may involve, a significant ML/TF or people smuggling risk, or when the person has breached one or more conditions of registration. However, the AUSTRAC CEO also has no power to remove or cancel a registered entity that is inactive (that is, one that is not providing remittance services) or to ban individuals, such as key personnel (including directors and beneficial owners), from being involved in the industry.

A power to ban persons found to be unsuitable or to have breached a Commonwealth, state or territory law from being involved as a key employee or associate of a remitter would help to limit criminal infiltration and manipulation of the sector. To maintain its registration a remitter would need to demonstrate it no longer had a relationship with a banned person. Similar powers operate in the gaming industry where the associates of an applicant (that is, directors, primary shareholders and key decision-makers) are subject to a probity assessment as part of the licensing processes.[298]

A power to suspend or cancel a remitter's registration once the registered remitter ceases to carry on a remittance business would ensure that the registration certificate is not passed to a third party who may wish to avoid scrutiny by AUSTRAC.[299] For instance, a registered remitter subject to AUSTRAC interest may seek to be removed from the RSR but later 'activate' a dormant business registered under another company name. AUSTRAC has already detected this sort of activity. The exercise of these proposed additional powers by the AUSTRAC CEO could have a significant impact on a person's business or livelihood. In view of this, decisions made using these powers should be reviewable, similar to the powers under sections 75Q, 75R and 75S of the AML/CTF Act.

Providing more flexibility for the AUSTRAC CEO to publish the detailed circumstances of a remitter cancellation would also help deter non-compliance and criminal links with the sector. It would also alert other financial businesses, such as banks, that an entity is no longer registered and publicise that it is illegal for the entity to continue to operate as a remitter.

---

[297] AUSTRAC, *Bank de-risking of remittance businesses,* 2015, http://www.austrac.gov.au/bank-de-risking-remittance-businesses.
[298] For example, Chapter 10, Part 4A of the *Monitoring Relationships with Associates) of the Gambling Regulation Act 2003* (Victoria).
[299] This would be similar to ASIC's power to suspend or cancel an AFS license. See section 915B of the *Corporations Act 2001*.

Other options for strengthening the registration process should be explored with industry and partner agencies.

Definitional clarity

The definition of a 'designated remittance arrangement' in section 10 of the AML/CTF Act is overly broad and should be narrowed so that non-remittance businesses are not captured unintentionally. The definition should be amended to cover a person or a business operating as a remitter (such as a money or value transfer system or alternative remittance dealer or provider) and exclude entities that only provide remittance-type transactions that are incidental to their core services. This would ensure section 10 operated as intended and help remove unnecessary compliance burden on entities unintentionally caught under the current definition. Such clarification will also resolve stakeholders' concern about the requirement that non-remitters report IFTI-DRAs.

Other measures

The obligation on RNPs to monitor their affiliates' compliance should be made explicit to strengthen oversight of the sector and bring Australia into line with FATF standards. This measure would also support RNP efforts to ensure their affiliates are registered and reduce their exposure to enforcement action for operating unregistered affiliates.

Stronger penalties for unregistered operators would augment the current regulatory framework but these are reactive measures which, alone, would not address concerns about the standards required for market entry and remitter professionalism. The current penalties also already exceed those detailed in the Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers.[300] This may hinder the case for further increases. On the other hand, if entry requirements to operate in the sector are raised, increased penalties may become more important to counter any growth in unregistered remitter activity. A decision on whether to seek higher penalties could be deferred until the broader regulatory framework is settled.

Recommendations

Recommendation 11.1

A government-industry working group should be established to develop options for strengthening regulatory oversight of remitters, including consideration of the existing enforcement power and penalty regimes, under the AML/CTF Act.

Recommendation 11.2

The definition of a designated remittance arrangement in the AML/CTF Act should be amended to ensure that non-remittance businesses are not unintentionally regulated as remitters under the AML/CTF Act.

Recommendation 11.3

The AML/CTF Act and Rules should be amended to explicitly require remittance network providers to monitor their affiliates' compliance and report to AUSTRAC on breaches and remedial action as required.

[300] Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, September 2011, https://www.ag.gov.au/Publications/Pages/GuidetoFramingCommonwealthOffencesInfringementNoticesandEnforcementPowers.aspx.

Recommendation 11.4

The AUSTRAC CEO should be allowed to:

(a) deregister remitters that are not conducting remittance activities (as evidenced by a lack of reporting or other relevant activity)

(b) ban individuals from involvement in the management or business of a remitter based on a demonstrated lack of suitability, fitness or propriety, and

(c) publish refusals and notices detailing the circumstance of a cancellation of the registration of a remitter.

12. Cross-border movement of physical currency and bearer negotiable instruments

Clandestine movement of cash and other valuable items across borders is a common money laundering method around the world.[301] Criminals move cash and valuables across border to:

- launder funds by placing them in another jurisdiction, typically with weaker AML/CTF controls
- pay for illicit goods
- use illicit funds to purchase assets and goods, and
- hide proceeds from authorities and complicate asset recovery.

Cross-border movements of cash and other valuable items can also be used to facilitate terrorism financing.

The FATF requires countries to put in place a cross-border reporting system for physical currency and bearer negotiable instruments (BNIs) to give law enforcement visibility over cross-border movements of currency. Australia implements this requirement in Part 4 of the AML/CTF Act by creating reporting obligations in relation to the cross-border movements of physical currency and BNIs.[302]

Cross-border movements of physical currency of AUD10,000 or more (or the foreign currency equivalent) must be reported to AUSTRAC (a 'CBM-PC' report). This requirement captures the carrying, mailing or shipping of physical currency. In 2014-15, a total of 48,272 CBM-PCs reports were submitted, with a value of AUD8.4 billion.[303]

There is no threshold value attached to the requirement to report cross-border movements of BNIs. The requirement to report depends on a request being made by an authorised (police or customs) officer. If a person produces one or more BNIs to a police or customs officer or is found to have one or more BNIs by a police or customs officer, they must make a report to AUSTRAC if requested (a 'CBM-BNI' report). In 2014-15, a total of 692 CBM-BNIs were submitted, with a value of AUD321 million.[304]

To support the enforcement of these reporting obligations, Division 8 of Part 15 of the AML/CTF Act establishes questioning, search, arrest and seizure powers for customs and police officers, as well as criminal and civil penalties for the failure to comply with reporting requirements and questioning and search powers.

Consultation

Partner agencies primarily focused on three aspects of the cross-border reporting requirements:

- the threshold applicable for CBM-PC reports
- the lack of a threshold for CBM-BNI reports, and

[301] See for example; AUSTRAC, *Money laundering in Australia 2011*, 2011, p. 33, http://www.austrac.gov.au/publications/corporate-publications-and-reports/money-laundering-australia-2011; Australian Crime Commission, *Organised Crime in Australia 2013*, 2013, p. 14, https://www.crimecommission.gov.au/sites/default/files/ACC%20OCA%202013-1.pdf.

[302] Section 17 of the AML/CTF Act defines a BNI to be a bill of exchange, cheque, promissory note, bearer bond, traveller's cheque, money order, postal order or similar order, or a negotiable instrument not covered by the preceding types.

[303] See *Appendix 2* for further data on the volume and value of CBM-PCs reported.

[304] See *Appendix 2* for further data on the volume and value of CBM-BNIs reported.

- the scope of items to which reporting requirements apply.

Partner agencies raised concerns that the lack of reporting obligations that apply to other high-value items and the inability to seize unreported goods represented a key vulnerability. They proposed expanding the cross-border reporting requirements to include:

- high-value portable instruments such as stored value cards, gaming chips, token plaques or letters of credit, and
- high-value portable goods such as bullion and precious stones and jewellery.

Partner agencies also considered that Australia's AML/CTF regime could be strengthened by aligning the disclosure system for BNIs with the system for physical currency, and expanding the search and seizure powers available to customs and police officers under sections 199 and 200 of the AML/CTF Act.

The findings of the MER

The MER identified one shortcoming in Australia's compliance with the FATF standards for cross-border movements of physical currency and BNIs.[305] The MER considered that the sanctions available for breaching cross-border reporting obligations are not consistently proportionate and dissuasive, with the civil penalties available too low to be dissuasive and the criminal penalties too high to be proportionate.

Discussion

CBM-PC threshold

The threshold for reporting cross-border cash movements was set in 1997 at AUD10,000 and remains at that level today. This threshold is below the FATF's recommended threshold of USD/EUR15,000.

Australia is not the only country to set a lower threshold than required by the FATF for CBM-PC reporting, as indicated in Table 5.

TABLE 5: COMPARISON OF CROSS-BORDER REPORTING THRESHOLDS IN KEY FOREIGN COUNTERPARTS

Country / organisation	Threshold (local currency)	Threshold (AUD)[306]	Mandatory BNI reporting?
FATF (recommended)	USD15,000 / EUR15,000	AUD20,878 / AUD22,621	Countries' discretion
Australia	AUD10,000	AUD10,000	No
United States	USD10,000	AUD13,925	Yes
United Kingdom	EUR10,000	AUD15,081	Yes
New Zealand	NZD10,000	AUD9,388	Yes
Canada	CAD10,000	AUD9,992	Yes
Singapore	SGD20,000	AUD19,537	Yes
Hong Kong	No threshold	No threshold	No

The effect of inflation since 1997 means that the AUD10,000 threshold ostensibly applies to lower value CBM-PC transactions in 2016 than in 1997. If the CBM-PC threshold had kept pace with inflation, today's threshold would be set at AUD15,867.[307]

[305] FATF Recommendation 32 (Cash couriers).
[306] At 5 January 2016.
[307] Reserve Bank of Australia, Inflation Calculator, http://www.rba.gov.au/calculator/annualDecimal.html, (accessed 15 January 2016). The purchasing power of the Australian dollar has also increased significantly since 1997 - the equivalent purchasing power of AUD10,000 in 2015 would have been AUD6,213 in 1997. See Australian Bureau of Statistics, Consumer Price Index Inflation

However, the ML/TF risks associated with cross border movements of cash, BNIs and other instruments remain significant. High-value portable goods and instruments continue to be an important methodology for concealing the movement of illicit funds offshore. This includes funds to support terrorist groups and terrorist activity, particularly for Australians who travelling overseas to become foreign terrorist fighters and supporters in places such as Syria.[308]

In light of these ongoing risks, the CBM-PC threshold should be maintained at AUD10,000.

CBM-BNI threshold

Under Part 4 of the AML/CTF Act, BNIs are only required to be declared and reported at the Australian border if a person is requested to do so by a customs or police officer. This means there is no mandatory requirement to report the cross border movement of BNIs, regardless of their value.

The request and disclosure approach to cross border movements of BNIs was originally adopted to enable more targeted use of customs and police resources.[309] However, this approach has led to difficulties in enforcing BNI reporting obligations at the Australian border, as the series of procedural steps required for an offence to be committed generates a gap within the regime that can lead to individuals avoiding reporting requirements.[310]

The gap arises because the relevant offence provisions relating to the failure to make a CBM-BNI report depend on the person carrying the BNI *being requested to make a report* about the BNI by a police or customs officer. Failing to declare a BNI is not an offence under the AML/CTF Act, even if the person has been asked to declare by a customs or police officer.[311]

To close this gap, the AML/CTF Act should be amended to require mandatory reporting of BNIs above a prescribed threshold.

Consolidation of reporting requirements

If the reporting requirements for cross border movements of BNI and physical currency are to be aligned, the reporting framework under Part 4 could be consolidated into a single reporting requirement. Under this new framework there would be mandatory reporting of cross border movements of 'cash' equal to or over AUD10,000, where 'cash' is defined broadly to include physical currency, BNIs and other high-value goods and instruments (see below for a discussion of high-value goods and instruments).[312]

To ensure the new reporting framework under Part 4 has the flexibility to accommodate emerging threats, the revised definition of 'cash' should also include any instrument prescribed in the AML/CTF Rules as 'cash' for the purposes of Part 4.

This proposal will simplify the reporting framework under Part 4 and align Australia with a number of key foreign counterparts which require mandatory BNI reporting above a threshold (see Table 5 above).

Calculator, http://www.abs.gov.au/websitedbs/d3310114.nsf/home/Consumer+Price+Index+Inflation+Calculator, (accessed 15 January 2016).

[308] AUSTRAC, *Terrorism Financing in Australia 2014*, 2014, http://www.austrac.gov.au/publications/corporate-publications-and-reports/terrorism-financing-australia-2014.

[309] Item 9, *Anti-Terrorism Bill (No. 2) 2005 Explanatory Memorandum*, https://www.comlaw.gov.au/Details/C2005B00185/Explanatory%20Memorandum/Text.

[310] From July 2011 to June 2014 there were no convictions for failing to report movement of BNIs into and out of Australia when requested.

[311] A person does not commit an offence under section 59 of the AML/CTF Act unless:

- a BNI is discovered by, or disclosed to, an officer,
- the officer requests that the person carrying the BNI makes a report about the BNI, and
- the person then refuses to make such a report.

[312] Singapore takes such an approach in its cross-border reporting regime. See the Singapore Police Force's website for further information: http://www.cad.gov.sg/aml-cft/suspicious-transaction-reporting-office/reporting-of-cross-border-movements-of-physical-currency-and-bearer-negotiable-instruments, (accessed 15 January 2016).

Scope of reporting requirements

High-value instruments

Some high-value instruments such as gaming chips, tokens, plaques or letters of credit and stored value cards (SVC) are currently not required to be reported at the Australian border.

These types of instruments can be an attractive vehicle for those seeking to conceal and move illicit funds, as they allow criminals to consolidate the illicit funds into small, but high-value instruments that can be readily transported across Australia's borders and redeemed for value at a later date. In particular, there is increasing evidence that financial products that provide low-value, high-volume accessibility and anonymity for individuals, such as pre-paid SVCs, are being used to finance terrorism. There is also a significant risk that Australians linked to foreign terrorist groups may use the SVCs to access funds overseas.[313]

Case study 13 demonstrates the vulnerabilities posed by the cross-border movements of SVCs.

CASE STUDY 13: STORED VALUE CARDS USED TO FACILITATE MONEY LAUNDERING[314]

An investigation identified a person of interest (POI) as being in possession of numerous false identity documents, including driver licences and foreign passports.

The POI was detained at an airport attempting to fly to India. He was found to be carrying approximately AUD140,000 cash and 46 SVCs. A search warrant at a storage unit rented in his name located further SVCs and gift cards. It was alleged that the POI intended to take the money and the SVCs to India in order to launder proceeds of crime.

It appears that the POI purchased these cards from post offices and service stations. While the POI had cross-border reporting obligations in relation to the cash, he had no obligation to report the SVCs.

While it is not illegal to transport high-value instruments into and out of Australia, Australian authorities should be aware of such movements and have the ability to act where they appear suspicious. To this end, the proposed expanded definition of 'cash' should also include other high-value instruments that pose high ML/TF risks, such as SVCs. This would capture the cross-border movement of these instruments under the proposed consolidated reporting requirement where the value of the instruments is AUD10,000 or more.

There are technological challenges in determining the value of different SVCs at the Australia border. In view of these challenges, the feasibility of acquiring technology that will allow customs officers to accurately assess the value of SVCs should be explored.

High-value goods

High-value goods such as bullion, precious stones and jewellery also facilitate the physical transportation of value across borders, as case study 14 demonstrates.

[313] AUSTRAC, *Terrorism Financing in Australia 2014*, 2014, http://www.austrac.gov.au/publications/corporate-publications-and-reports/terrorism-financing-australia-2014.
[314] Source: AUSTRAC.

CASE STUDY 14: POTENTIAL BULLION SMUGGLING[315]

On 28 May 2014, a target identified by law enforcement was departing Australia for India. A covert x-ray of the target's checked baggage revealed anomalies which resulted in the physical search of a bag. Located inside the bag were seven blocks of Swiss fine gold, with a total value of approximately AUD350,000.

Had this situation involved a similar quantity of physical currency, the customs officers could have detained the individual for not declaring the cash prior to departure. However, customs officers do not currently have the power to detain a person for the movement of large quantities of bullion. As the person had not committed an offence under the AML/CTF Act, he was permitted to board his flight and depart the country with the bullion in his possession.

To address the ML/TF risks posed by these cross border movements, a reporting requirement should be imposed where bullion worth AUD10,000 or more is carried across the border. This could be achieved by including bullion within the proposed new definition of 'cash' under Part 4.

While a similar vulnerability exists in relation to precious stones and jewellery, the mandatory reporting of cross-border movements of precious stones and jewellery worth AUD10,000 or more is likely to cause significant disruption to passenger flows because of the large volume of passengers who are likely to be carry personal jewellery. Assessing the value of precious stones and jewellery at the border could also present significant practical difficulties for police and customs officers due to the specialised skills required to determine the value of such goods. In view of these challenges, precious stones and jewellery should not be included within the recommended broader definition of 'cash' at this point in time.

Search and seizure powers

Some of the ML/TF vulnerabilities associated with the cross border movement of high-value goods and instruments could be addressed by removing the link between the search and seizure powers under the AML/CTF Act and the reporting requirements under Part 4.

Currently, police and customs officers can question travellers at the border as to whether they are carrying any physical currency and whether they have made a CBM-PC.[316] They may also question travellers whether they have any BNIs and require a person that is carrying BNIs to make a CBM-BNI report.[317] In these circumstances, the police and customs officers' powers of examination, search and seizure are linked to the reporting and declarations requirements under Part 4 and limited as follows:

- **Physical currency** – the powers are only available to ascertain whether the person has currency in respect of which a CBM-PC is required (that is, over AUD10,000).[318]
- **BNIs** – the powers are only available when an officer has reasonable grounds to suspect the person has made a false or misleading declaration or refuses or fails to make a declaration following a request to do so.[319]

While police and customs officers have powers to search and seize under other legislation, under the AML/CTF Act they do not have general search and seizure powers in relation to cross-border movements of physical currency below the AUD10,000 threshold or BNIs where a person has not been asked to declare whether they are carrying any BNIs. De-linking the search and seizure powers from the reporting and declaration requirements will ensure that there will be no gaps in officers' ability to search and seize 'cash' where there is:

[315] Source: Australian Crime Commission.
[316] Subsections 199(1)-(2) of the AML/CTF Act.
[317] Subsections 59(1) and 200(1)-(2) of the AML/CTF Act.
[318] Subsections 199(3)-(11) of the AML/CTF Act.
[319] Subsections 200(3)-(13) of the AML/CTF Act.

- a suspicion of money laundering, terrorism financing or other serious criminal offences, or
- where there has been a breach of the cross-border reporting requirements under the AML/CTF Act. [320]

This approach would also bring Australia's cross-border movement reporting regime more in line with the FATF standards.[321]

Offence provisions

The MER considered that the sanctions that apply to breaches of cross-border movements of cash and BNIs obligations were not consistently proportionate and dissuasive, with the civil penalties available being too low to be dissuasive and the criminal penalties being too high to be proportionate.

The civil penalty available for failing to comply with the CBM-PC or CBM-BNI requirements is five penalty units (AUD900) if the amount involved is AUD20,000 or more, or two penalty units (AUD360) for amounts of less than AUD20,000.[322] The MER found that this sanction, while proportionate, is not dissuasive.

The civil penalties available under Australia's AML/CTF regime are significantly lower than those in other countries assessed by the FATF and should be increased to align with international counterparts.[323] The tiered approach to determining the penalties – where the penalty depends on the amount of funds involved – should be retained to enable proportionate and dissuasive sanctions.

The maximum criminal penalty available for these offences is two years imprisonment or 500 penalty units (AUD90,000) or both. This is similar to the maximum penalties that are available for these offences in other countries assessed by the FATF.[324] The Australian criminal penalties are proportionate, as they represent the maximum penalty available, not a prescribed penalty. Courts therefore have the flexibility to consider all the circumstances of the case and apply an appropriate sanction up to the maximum penalty.

Sections 199 and 200 create offences for failing to comply with questioning and search powers in relation to physical currency and BNIs. Only criminal penalties are available for these offences. The availability of a civil penalty for a failure to comply with sections 199 and 200 would provide a wider range of options for law enforcement to respond to such breaches and assist in ensuring these penalties remain proportionate.

'Eligible place' definition

Under sections 199 and 200, police and customs officers are able to go onto or enter any 'eligible place'. Eligible place is defined in section 5 of the AML/CTF Act to mean places as defined in the *Customs Act 1901*, including areas appointed by the Comptroller-General of Customs and 'licensed warehouses'.

Reliance on the *Customs Act 1901* definition of 'eligible place' limits the reach of the search powers relating to cross-border movements, preventing police and customs officers from searching areas surrounding appointed airports, ports or wharves.

The AML/CTF Act should be amended to allow the definition of 'eligible place' to be expanded by way of a Regulation. This would establish a more flexible approach to allowing additional areas to be designated as

[320] Using the recommended broader definition of 'cash', this would include physical currency, BNIs and bullion.
[321] See criterion 32.8 of the FATF Methodology.
[322] Section 186 of the AML/CTF Act.
[323] **Norway**: Civil penalty is equivalent to 20% of the total amount of currency or BNI not declared. **Spain**: Civil penalty is from a minimum of EUR€600 up to twice the total amount of currency or BNI not declared. **Belgium:** Civil penalty is EUR€125 to EUR€1,250. **Malaysia:** No civil penalty. All four countries were assessed as compliant with Recommendation 32.
[324] **Norway**: No criminal penalty. **Spain**: No criminal penalty. **Belgium:** Criminal penalty is imprisonment of eight days to five years or a fine of EUR€25 to EUR€25,000. **Malaysia:** Criminal penalty is imprisonment of up to five years or a fine not exceeding RM3 million (failing to declare) and imprisonment of up to three years or a fine not exceeding RM500,000 (incorrect declaration).

'eligible places' for the purposes of the AML/CTF Act while ensuring adequate transparency of search powers.

Recommendations

Recommendation 12.1

The current cross-border reporting regime for physical currency and BNIs in the AML/CTF Act should be replaced with a consolidated requirement to report 'cash' of AUD10,000 or more. For the purposes of Part 4 of the AML/CTF Act, cash should be defined as:

- physical currency
- bearer negotiable instruments (using the extended definition in Recommendation 12.2)
- bullion, and
- an object or instrument specified in the AML/CTF Rules.

Recommendation 12.2

The current definition of a bearer negotiable instrument under the AML/CTF Act should be amended to include:

- gaming chips or tokens
- plaques or letters of credit, and
- an object or instrument specified in the AML/CTF Rules.

Recommendation 12.3

The Attorney-General's Department, AUSTRAC and the Department of Immigration and Border Protection should investigate the feasibility of establishing cross-border reporting obligations in relation to stored value cards.

Recommendation 12.4

The powers under sections 199 and 200 of the AML/CTF Act should be broadened to allow police and customs officers to search and seize 'cash' where there is:

- a suspicion of money laundering, terrorism financing or other serious criminal offences, or
- where there has been a breach of the cross-border reporting requirements under the AML/CTF Act.

Recommendation 12.5

The AML/CTF Act should be amended to increase the civil penalty available for failing to comply with the cross-border 'cash' reporting requirement in line with international standards.

Recommendation 12.6

Sections 199 and 200 of the AML/CTF Act should be amended to provide for a civil penalty for breach of these provisions.

Recommendation 12.7

The AML/CTF Act should be amended to allow the definition of 'eligible place' to be expanded to include other designated areas (for the purposes of the AML/CTF Act) by way of regulation.

13. Countermeasures

The AML/CTF regime establishes a framework to allow Australia to apply countermeasures against high-risk countries and non-cooperative jurisdictions that have strategic AML/CTF deficiencies.[325] This includes a regulation-making power that allows the Government to designate a country as a 'prescribed foreign country'. Once a country is designated as a prescribed foreign country, reporting entities must apply their enhanced due diligence program to all dealings with that country, including enhanced CDD on customers and enhanced vigilance on all transactions involving that country.[326] The regulation-making power also allows transactions with residents of prescribed foreign countries to be prohibit or regulated.

Up until February 2016, AML/CTF countermeasures had only been applied to Iran, with Iran designated as a prescribed foreign country for the purposes of the AML/CTF Act and transactions of AUD20,000 or more between Australia and Iran were prohibited without prior authorisation from the Department of Foreign Affairs and Trade (DFAT).[327]

Consultation

Stakeholders did not provide comment on the countermeasures requirements.

The findings of the MER

The MER identified moderate shortcomings in Australia's compliance with the FATF standard on higher risk countries and countermeasures.[328] These deficiencies are:

- reporting entities under the AML/CTF Act are not required to apply enhanced CDD to their relationships and transactions with the Democratic People's Republic of Korea (DPRK / North Korea), despite the FATF first calling for member countries to introduce these requirements in 2011,[329] and
- some of the enhanced CDD measures required under Chapter 15 of the AML/CTF Rules address normal CDD, rather than enhanced CDD.

Discussion

A new regulation was made in February 2016 to designate the DPRK as a prescribed foreign country for the purposes of the AML/CTF Act and require reporting entities to conduct enhanced CDD on all relationships and transactions with the DPRK. The new regulation ensures Australia complies with the FATF's call to member countries to apply enhanced CDD to their relationships and transactions with DPRK to mitigate the ML/TF risks posed by this higher risk jurisdiction. The new regulation also removes the prohibition on the processing of transactions involving persons in Iran with a value of at least AUD20,000. This measure aligns Australia with international action to implement changes to sanctions on Iran in return for commitments from Iran in relation to its nuclear program. However, consistent with the FATF's continued call for

[325] Part 9 of the AML/CTF Act.
[326] Chapter 15 of the AML/CTF Rules.
[327] The *Anti-Money Laundering and Counter-Terrorism Financing (Prescribed Foreign Countries) Regulation 2016* commenced on 26 February 2016, replacing the *Anti-Money Laundering and Counter-Terrorism Financing (Iran Countermeasures) Regulation 2014.*
[328] FATF Recommendation 19 (Higher risk countries).
[329] At January 2016, the FATF lists two countries as 'high-risk and non-cooperative jurisdictions' (Iran and DPRK). Further information is on the FATF's website: http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/, (accessed 15 January 2016).

counter-measures against Iran, it remains a prescribed foreign country for the purposes of the AML/CTF Act.

Some of the enhanced CDD measures for higher risk countries do address normal CDD. However, 'normal' measures undertaken as part of an enhanced CDD program can satisfy enhanced CDD requirements provided the measures are consistent with the risks identified. For example, normal measures such as clarifying or updating KYC information, or information about a customer's activity or business, may be consistent with enhanced CDD where there is doubt about the veracity or adequacy of previously obtained KYC information. This is also consistent with the FATF standards.[330] In view of this, this review makes no recommendations to changes these requirements.

[330] The interpretive note to FATF Recommendation 10 (Customer due diligence) in the FATF standards, lists 'Obtaining additional information on the customer and updating more regularly the identification data of customer and beneficial owner' as an example of an enhanced CDD measures that could be applied to a high-risk business relationship.

14. Secrecy and access

AUSTRAC collects a range of information to support its complementary roles as Australia's AML/CTF regulator and specialist financial intelligence unit (FIU). This information is collected under the AML/CTF Act and other Commonwealth, state and territory legislation.

Reporting entities provide information to AUSTRAC under the AML/CTF Act primarily through the reporting of TTRs, IFTIs and SMRs. AUSTRAC analyses and disseminates this information as actionable financial intelligence to partner agencies, including domestic law enforcement, national security, human services and revenue protection agencies. AUSTRAC information is also shared with international counterparts for law enforcement, regulatory and counter-terrorism purposes.

The secrecy and access provisions under Part 11 of the AML/CTF Act regulate access to, and the use and disclosure of, AUSTRAC information. These provisions are intended to ensure that the sensitive information under AUSTRAC's control is secure and protected from unauthorised access, use and disclosure.

Consultation

Partner agencies identified the complexity of the secrecy and access provisions as a major concern, with some provisions hampering timely access to financial intelligence to combat ML/TF and other serious crimes.

Specifically, concerns were raised about:

- the inadequacy of the AML/CTF Act definitions for 'AUSTRAC information' and 'eligible collected information'
- the scope of AUSTRAC's powers to retain, use and disclose AUSTRAC information
- a lack of clarity surrounding the ability of partner agencies and foreign governments to acquire, access and disclose AUSTRAC information, particularly for those Commonwealth, state and territory agencies that are not formally designated under the AML/CTF Act
- the impact on partner agency operations of restrictions on the use of AUSTRAC information
- inconsistencies in the scope of safeguards to protect AUSTRAC information from inappropriate access and use
- the inability of AUSTRAC to share information with the private sector to enable collaborative approaches to combating serious crime
- the inability to disclose aggregated AUSTRAC data to support the development of domestic and international policy and research, and
- gaps within, and the complexity of, the offence regime under Part 11.

There was significant support for simplifying Part 11 to establish a more flexible and effective framework for sharing AUSTRAC information that keeps pace with new approaches to investigating serious crime, both in Australia and overseas.

Some industry stakeholders expressed concern about the scope of the tipping-off provisions under section 123 of the AML/CTF Act. These provisions were seen as inhibiting the ability of financial institutions, in particular multi-national institutions, to share SMR-related information within corporate groups and properly manage their ML/TF risks. Other stakeholders did not wish to see any changes in the current tipping-off provisions due to concerns about the potential misuse of the information.

One stakeholder asked for the ability to disclose information related to SMRs to auditors to assist reporting entities to demonstrate compliance with CDD obligations.

The ALRC also recommended that the review should consider whether reporting entities, AUSTRAC and designated agencies are appropriately handling information collected under the AML/CTF regime.[331]

The findings of the MER

The MER concludes that Australia fully complies with the FATF standards that require countries to:

- protect the security and confidentiality of information collected by FIUs, and[332]
- prohibit under law disclosures about the fact that a suspicious transaction report or related information is being filed, or has been filed, with the FIU.[333]

Discussion

Since the passage of the AML/CTF Act in 2006, the national security and organised crime environment in Australia has changed significantly. Law enforcement agencies are placing an increased emphasis on protecting the Australian community through better prevention, enhanced detection and greater disruption of threats. To achieve this goal, these agencies are increasingly working collaboratively at the national and international level.

Effective and efficient information-sharing arrangements between domestic and international partners are crucial to support these collaborative efforts.

Collaboration and information-sharing with the private sector is also critical to effectively combat serious and organised crime, assisting the private and public sectors to reach a shared (and up-to-date) understanding of the risks within a jurisdiction and support efforts to prevent and disrupt criminal activities.[334]

Partner agencies commonly agreed that the secrecy and access provisions under Part 11 do not support effective, timely and collaborative information-sharing arrangements. They consider the existing provisions unduly complex and restrictive, generating significant uncertainty and impeding the use of AUSTRAC's intelligence for operational purposes.

The specific concerns about Part 11 can be grouped under the following themes:

- the scope of AUSTRAC information
- the ability to use and share AUSTRAC information
- gaps and conflicting provisions
- the confidentiality and security of AUSTRAC information
- unauthorised disclosures by third parties, and
- the scope of the tipping-off offence.

---

[331] Recommendations 16-4(a) and 16-4(e), Australian Law Reform Commission, 12 August 2008, *For Your Information: Australian Privacy Law and Practice,* ALRC Report 108, http://www.alrc.gov.au/publications/report-108.
[332] FATF Recommendation 29 (Financial intelligence unit).
[333] FATF Recommendation 21 (Tipping-off and confidentiality).
[334] The FATF standards generally support the sharing of targeted financial intelligence information with the private sector. See FATF Recommendations 9, 10, 16, 17, 18, 24, 25, 26, and 27.

The scope of AUSTRAC information

'AUSTRAC information' is defined under section 5 of the AML/CTF Act as eligible collected information, a compilation by the AUSTRAC CEO of eligible collected information, or an analysis by the AUSTRAC CEO of eligible collected information. Section 5 also defines 'eligible collected information' as information 'obtained' by the AUSTRAC CEO under Australian laws, or from a government body, or an authorised officer pursuant to specific provisions.[335]

The definition of AUSTRAC information (and eligible collected information) is narrow in practice and does not anticipate all the ways in which information is collected or obtained by the AUSTRAC CEO. For example, the definition does not capture information that the AUSTRAC CEO can receive from:

- a person who is not a reporting entity about a transaction that appears suspicious
- a person who wishes to 'dob-in' an alleged breach of regulatory obligations, and
- international, multi-jurisdictional bodies with a law enforcement function (such as Europol and Interpol).

This additional information collected by AUSTRAC is relevant to the functions of the AUSTRAC CEO and highly sensitive. While the information should be treated as confidential, it is not considered to be AUSTRAC information for the purposes of the AML/CTF Act so the protections and controls under Part 11 do not apply.

In view of this, the AML/CTF Act definition of AUSTRAC information should be amended to reflect the full range of information in AUSTRAC's possession.

The ability to use and share AUSTRAC information

Part 11 establishes a complex framework that governs access to, and the dissemination of, AUSTRAC information by the AUSTRAC CEO and AUSTRAC's partner agencies. This framework is highly technical and prescriptive, with different requirements applying to different agencies.[336] Factors determining access and usage include the function of the agency, the status of the agency, whether the agency is a Commonwealth, state or territory agency, and the purpose for which the information will be used. These factors can overlap, causing confusion and delaying a partner agency's ability to access information in a timely way and follow the trail of illicit funds before it disappears.

Part 11 also provides that AUSTRAC information may be communicated to a foreign country provided a number of safeguards are met.[337] In addition, any person may apply for access to AUSTRAC information under the *Privacy Act 1988* or the *Freedom of Information Act 1982* (FOI Act). However, FOI Act exemptions apply to specific types of information held by AUSTRAC.

This prescriptive approach to authorising access to AUSTRAC information hampers the effective and efficient sharing of AUSTRAC information with a range of agencies and entities for legitimate purposes. For example, this approach does not readily facilitate the timely sharing of AUSTRAC information with:

- multi-agency task forces and 'fusion bodies' for law enforcement, intelligence-gathering and national security purposes
- some foreign agencies and multi-jurisdictional bodies for law enforcement, intelligence-gathering and national security purposes

[335] See *Chapter 15: Audit, information-gathering and enforcement* for further information on information-gathering powers.
[336] See the definition of a 'designated agency' under section 5 of the AML/CTF Act.
[337] Sections 132-133C of the AML/CTF Act.

- trusted private sector partners (including reporting entities) to assist them in understanding and managing ML/TF risks
- non-designated state and territory agencies for investigating a possible or probable breach of the law of the Commonwealth
- auditors who are assessing a reporting entity's compliance with its CDD obligations, and
- private and public bodies engaged in policy development and research.

A key concern is the inability of AUSTRAC and partner agencies to readily share AUSTRAC information across government agencies to support collaborative approaches to tackling serious and organised crime. Instances have arisen where members of task forces have been excluded from discussions involving AUSTRAC information because their agency has not been designated under the AML/CTF Act as an agency that can access AUSTRAC information. In other situations, a task force member may be authorised to receive AUSTRAC information (for example, by temporary appointment to a designated agency such as the AFP for the duration of the taskforce), but is prohibited from sharing this information with their original agency because that agency is not designated under the AML/CTF Act.

AUSTRAC and Australian law enforcement agencies were also unable to disclose AUSTRAC information to multi-national law enforcement or criminal intelligence entities, such as Interpol or Europol, because the relevant provisions of the AML/CTF Act only allowed disclosure to a foreign country or part of a foreign country. On 29 February 2016, the *Crimes Legislation Amendment (Proceeds of Crime and Other Measures) Act 2015* received royal assent. The Act amended the definition of 'foreign law enforcement agency' in section 5 of the AML/CTF Act to allow the AFP and ACC to share AUSTRAC information with Interpol, Europol and other international bodies prescribed by regulation.

Part 11 does not facilitate the sharing of sensitive AUSTRAC information with the private sector. This limits AUSTRAC's ability to provide information that alerts and educates reporting entities about new and emerging risks or assist them with their managing risks. It also prevents AUSTRAC from developing 'trusted partnerships' with key reporting entities to enhance and facilitate the discovery, analysis and dissemination of financial intelligence necessary to combat and disrupt ML/TF and other serious and organised crime.

The forging of trusted partnerships between public and private partners has been a major development in various jurisdictions. In December 2015, the FATF held a Special Plenary meeting to consider strategies to combat the financing of ISIL, their affiliates, and other terrorist groups. Arising from this Special Plenary meeting the FATF agreed, among other things, to take immediate actions to improve information exchange between government agencies, between countries, and with the private sector.[338]

In February 2015, the United Kingdom Home Office, the National Crime Agency and the British Bankers' Association established on a trial basis the Joint Money Laundering Intelligence Taskforce (JMLIT).[339] The JMLIT aims to provide an information-sharing environment for the public and private sectors actors involved in the combating of terrorism financing and money laundering.

The constraints of Part 11 will also limit the sharing of information in support of future public-private partnership initiatives. This includes the establishment of a dedicated financial intelligence centre of

[338] Financial Action Task Force, *The Financial Action Task Force leads renewed global effort to counter terrorist financing*, 14 December 2015, http://www.fatf-gafi.org/publications/fatfgeneral/documents/fatf-leads-renewed-global-effort-to-counter-terrorist-financing.html.
[339] British Bankers' Association, *Uniting to tackle financial crime*, 27 February 2015, https://www.bba.org.uk/news/bba-voice/uniting-to-tackle-financial-crime/#.Vq1VPzbZVjo.

excellence, with similar features to the United Kingdom JMLIT, comprising AUSTRAC, domestic and international partners and trusted industry partners.

Significant reforms are required to Part 11 to provide clear authorisations for accessing, using and disseminating AUSTRAC information to better support contemporary and innovative approaches to combating ML/TF and other serious crime. These authorisations should be expanded for the other purposes detailed above, subject to appropriate protections and controls.

Gaps and conflicting provisions

There are a number of gaps in the scope of Part 11.

The AUSTRAC CEO is able to authorise an official of a non-designated Commonwealth agency to access AUSTRAC information for the purpose of an investigation of a possible breach of a law of the Commonwealth or a proposed investigation of a possible breach of a law of the Commonwealth.[340] This provision is useful as it recognises that Commonwealth agencies with regulatory functions may periodically require access to AUSTRAC information for the purpose of an investigation.

However, there are no similar provisions permitting the AUSTRAC CEO to authorise an official of a non-designated state or territory agency, such as a state or territory casino or gaming regulator, to access AUSTRAC information for the same purpose. This can hamper the ability of state or territory agencies with regulatory functions to investigate matters and take enforcement action, as well as inhibit the sharing of AUSTRAC information across agencies involved in national (joint Commonwealth, state and territory) operations and task forces.

Part 11 also does not allow the use of the AUSTRAC information to support legitimate regulatory actions by AUSTRAC's partner agencies. Many of AUSTRAC's partner agencies are responsible for making 'administrative decisions' and as part of this process are required to put 'adverse material' to the person who will be affected by the decision. However, AUSTRAC's main partner agencies (other than the ATO) are not expressly authorised under Part 11 to disclose AUSTRAC information for the purpose of making an administrative decision. This restriction can inhibit the use of relevant AUSTRAC information in making administrative decisions and cause procedural fairness problems as the AUSTRAC information cannot be put before the affected person.

The use of AUSTRAC information to support regulatory actions by authorities, including the making of administrative decisions, is consistent with the policy objectives of the AML/CTF Act. In view of this, changes to allow the use of AUSTRAC information for this purpose should be supported.

Some partner agencies are established under enabling legislation that also provides for access to, and the use of, collected information. This means that, where an official from a partner agency accesses AUSTRAC information, the official may have to comply with two secrecy and access frameworks which may be incompatible or conflicting. For example, the AML/CTF Act permits 'further disclosure' by partner agencies for the performance of their duties where the disclosure is authorised under Division 4 of Part 11. However, it may not be clear which obligation prevails where such a disclosure is not permitted under Division 4 of Part 11 of the AML/CTF Act but is permitted under a partner agency's enabling legislation.

Similar questions arise in relation to the interaction of authorisations provided by the AUSTRAC CEO under section 126 with sections 127 and 128, as well as other 'access' provisions in Division 4 of Part 11.

[340] See section 129 of the AML/CTF Act.

The provisions of Part 11 of the AML/CTF Act and other agencies' secrecy and access provisions should be harmonised to ensure that officials from partner agencies have a clear understanding of their obligations when dealing with AUSTRAC information.

The confidentiality and security of AUSTRAC information

Part 11 of the AML/CTF Act establishes a range of protections and controls over the use of AUSTRAC information, including prohibitions on some disclosures, statutory inadmissibility of some types of information, limitations on the use of particular types of information by particular classes of officials and a statutory bar on compelling production or disclosure of AUSTRAC information in court or tribunal proceedings.

These protections and controls do not adequately safeguard all information that is collected under the AML/CTF Act, particularly when it is collected by other agencies.

For example, under section 49 AUSTRAC and a number of other agencies are able to give reporting entities or another person a written notice asking for further information relating to SMRs, TTRs or IFTIs. Where the notice is issued by AUSTRAC and the information is provided to AUSTRAC, AUSTRAC is exempt from the operation of the FOI Act in relation to this information. This exemption does not extend to other agencies that have the same power under section 49 to collect the same information. In addition, where another agency collects such information under section 49 and passes on that information to AUSTRAC, AUSTRAC's FOI Act exemption does not apply to that information.

Similarly, where a reporting entity provides another agency with further information in accordance with a notice under section 49, the information is not subject to the protections against disclosure found in Part 11 that would apply if AUSTRAC had issued the written notice.

While sensitive and confidential information received by AUSTRAC (or another Commonwealth agency or authority) from a foreign counterpart FIU or foreign government is exempt from disclosure under the FOI Act, this information does not have the protections given to sensitive and confidential AUSTRAC information (SMRs and information gathered under section 49 that relates to SMRs). As this information is therefore admissible in court and tribunal proceedings conducted in Australia, foreign agencies and foreign governments may be reluctant to share sensitive and confidential information with AUSTRAC.

Sensitive and confidential information provided to AUSTRAC by a foreign agency or foreign country should have the same protections as sensitive and confidential AUSTRAC information. This means, as a general rule, the evidence should be inadmissible into evidence in court and tribunal proceedings. However, an exemption should be available where the AUSTRAC CEO issues a certificate that the source of sensitive and confidential information has explicitly consented to the information being admitted into evidence in the proceedings. This approach would give the foreign country or agency providing the information control over the extent to which such information can be produced in court or tribunal proceedings in Australia.

The protections under Part 11 also do not apply to all of the information collected under the FTR Act. For example, section 122 of the AML/CTF Act restricts what may be done with information collected under section 49. However, these restrictions do not apply to information collected under the comparable section 16 of the FTR Act. Information collected under subsection 16(4) of the FTR Act by persons other than the AUSTRAC CEO (for example, AFP or ACC officials) also does not fall within the definition of AUSTRAC information and is not subject to the protections that normally apply to AUSTRAC information.

Greater consistency is required in the application of the controls, protections, powers and authorisations that apply to information collected under the AML/CTF Act and held by AUSTRAC and its partner agencies. These controls, protections, powers and authorisations should reflect the sensitive nature of the

information collected by AUSTRAC and should not vary according to which agency collected, or is holding, the information.

One option to protect all of AUSTRAC's sensitive information from being publicly disclosed is for AUSTRAC to be classified as a 'law enforcement agency' for the purposes of the FOI Act. As this issue does not relate to the provisions of the AML/CTF Act, it should be considered externally to this review.

Unauthorised disclosures by third parties

The AML/CTF Act has a number of protections against the unauthorised disclosures of AUSTRAC information that could be strengthened by prohibiting unauthorised disclosure by third parties.

Disclosure of sensitive information obtained by employees of government departments or agencies in the course of employment is generally subject to legislative sanctions under other legislation.[341] For example, secrecy provisions covering the national security and intelligence community expressly cover employees and, in some cases, third parties engaged by the agency.[342]

Part 11 of the AML/CTF Act establishes offence provisions that essentially relate to one act – the unauthorised disclosure of AUSTRAC information by AUSTRAC personnel, partner agency personnel, and other persons (for example, consultants engaged by AUSTRAC). However, there are limited offences relating to the subsequent unauthorised disclosure of AUSTRAC information by third parties.[343]

Disclosures of AUSTRAC information by third parties should be prohibited under the AML/CTF Act. The offence that applies to such disclosures should require that:

- the person knew, or was reckless as to whether, the information was initially disclosed in contravention of a secrecy offence, and
- the person knew, intended or was reckless as to whether, the subsequent disclosure of the information would cause, or was reasonably likely to cause, harm to an essential public interest.[344]

These requirements would ensure that the new offence is sufficiently targeted at those engaging in improper conduct, and would not apply to a third person who received AUSTRAC information and innocently or unknowingly passed on that information.

Scope of the 'tipping-off' offence

The 'tipping-off' provisions under section 123 of AML/CTF Act prohibit a reporting entity from disclosing to any person (other than AUSTRAC) that it has formed a suspicion about a customer or that it has submitted an SMR to AUSTRAC subject to some exemptions.

[341] For example, subsection 70(1) of the *Crimes Act 1914* and subsection 142.2(1)(ii) of the *Criminal Code Act 1995*.
[342] Subsections 60A(1) and 40ZA of the *Australian Federal Police Act*, subsection 51(1) of the *Australian Crime Commission Act 2002*, subsection 207(1) of the *Law Enforcement Integrity Commissioner Act 2006* and subsection 29(1)(b) of the *Intelligence Services Act 2001*.
[343] For example, see subsections 128(5) and (10) of the AML/CTF Act.
[344] The proposed requirements for offences that apply to forward disclosures of unlawfully obtained information by third parties are consistent with recommendations made by the Australian Law Reform Commission arising from its inquiry into secrecy laws and open government. See Australian Law Reform Commission, *Secrecy Law and Open Government in Australia,* Report 112, March 2010, http://www.alrc.gov.au/publications/report-112.

Stakeholders generally supported the policy objective underpinning this offence, but they indicated that the provisions prevent:

- multinational financial institutions from taking a global risk management approach to customers who hold accounts in multiple jurisdictions, and sharing information about SMRs with foreign parent entities, and
- reporting entities from providing information to AML/CTF auditors to demonstrate the entity's compliance with AML/CTF obligations.[345]

A key challenge associated with allowing Australian reporting entities to share SMR-related information with foreign parent entities is ensuring the ongoing security of such information once it is disclosed to an overseas entity and its use and handling is no longer subject to Australian law. In most cases, foreign financial institutions would act in good faith and implement appropriate arrangements to ensure that the information is not misused. However, there may be circumstances where a foreign financial institution fails to treat the SMR-related information as sensitive and confidential. Sanctioning the foreign financial institution in a proportionate and dissuasive manner in these circumstances would be a challenge.

There are a number of models for sharing SMR-related information with foreign parent entities. In the United States, a branch or agency of a foreign bank may disclose a suspicious activity report to its head office outside the United States and a United States depository institution may disclose a suspicious activity report to controlling companies whether domestic or foreign.[346] Banking organisations are required to maintain appropriate arrangements for protecting the confidentiality of suspicious activity reports disclosed in these circumstances. This can include written confidentiality agreements or putting in place arrangements specifying that the head office or controlling company must protect the confidentiality of the suspicious activity reports through appropriate internal controls.[347]

In the United Kingdom, a regulated firm is exempted from the prohibition on sharing SMR-related information where the firm discloses the information to a credit institution or a financial institution that belongs to the same 'group'[348] and is located in a European Economic Area[349] state, or a country imposing equivalent money laundering requirements.[350] A further exemption is provided where the disclosure is from one credit institution to another or from one financial institution to another, and a number of other requirements are met.[351] Under this model, the ongoing security of shared SMR-related information is reliant on the willingness of the credit institution or financial institution receiving the information to deal with the information in accordance with the money laundering and privacy requirements in force in the country where they are located. [352]

---

[345] On 17 August 2015, the AUSTRAC CEO granted the Australian arm of HSBC an exemption from the section 123 tipping-off provisions to share its suspicious matter information with its independent compliance monitor, http://www.austrac.gov.au/media/media-releases/exemption-%E2%80%9Ctipping-off%E2%80%9D-prohibitions-granted-hsbc, (accessed 15 January 2016).

[346] Financial Crime Enforcement Network, Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies, 20 January 2006, https://www.fincen.gov/statutes_regs/guidance/html/sarsharingguidance01122006.html.

[347] *Ibid.*

[348] A 'group' is defined as a group of undertakings, which consists of a parent undertaking, its subsidiaries and the entities in which the parent undertaking or its subsidiaries hold a participation, as well as undertakings linked to each other by a 'relationship' (within the meaning of Article 12(1) of Directive 83/349/EEC).

[349] The European Economic Area includes Iceland, Liechtenstein and Norway and all 28 member states of the European Union.

[350] Subsection 333B(2) of the *Proceeds of Crime Act 2002* (United Kingdom) and subsection 21E(2) of the *Terrorism Act 2000* (United Kingdom).

[351] Section 333C of the *Proceeds of Crime Act 2002* (United Kingdom) and section 21F of the *Terrorism Act 2000* (United Kingdom).

[352] *Ibid.*

The AML/CTF Act should be amended to permit Australian reporting entities to share SMR-related information with foreign parent entities. The ability to share this information will allow some reporting entities and their foreign parent entities to better manage the ML/TF risks associated with the global footprint of their business and, specifically, the risk posed by shared customers, noting that some Australian reporting entities already regularly receive SMR-related information from foreign related entities. The framework for sharing this information should include appropriate safeguards and controls for maintaining the confidentiality of the information.

The AML/CTF Act should also be amended to allow reporting entities to share SMR-related information with external auditors. Auditors are appointed to determine whether reporting entities are complying with their obligations. The quality of SMR-related information provided by a reporting entity to AUSTRAC could be used to demonstrate to an auditor that a reporting entity's ongoing CDD and enhanced CDD measures are effective. However, where such information is provided to an auditor, the auditors should be prohibited from disclosing this information to a third party.

Conclusion

A more flexible and responsive legislative framework is required to govern the sharing of AUSTRAC information that provides clear authorisations for accessing, using and disseminating AUSTRAC information.

The new information-sharing framework should better meet the information needs of agencies and organisations tasked with combating ML/TF and other serious crime, and support collaborative approaches to addressing these threats at the domestic and international level.

More specifically, the amendments to the AML/CTF Act to establish the new framework should:

- update the definition of AUSTRAC information to reflect the full range of information in AUSTRAC's possession
- clarify the scope of the AUSTRAC CEO's powers to collect, retain and disseminate AUSTRAC information
- clarify the scope of powers and obligations for those holding and using AUSTRAC information
- expand the permissible uses of appropriate types of AUSTRAC information
- harmonise secrecy and access provisions under the AML/CTF Act with similar provisions under other legislation (where appropriate), and
- provide for the sharing of SMR-related information within a 'group' of related entities and with auditors.

A principles-based approach may provide a more appropriate, contemporary framework for information-sharing under the AML/CTF Act. Under this approach, legislative principles could be established for authorising access to AUSTRAC information and identifying permissible uses of AUSTRAC information. This approach should expand access to, and the permissible uses of, AUSTRAC information by appropriate bodies consistent with the broader policy objective of improved information-sharing and dissemination that is supported by the Heads of Commonwealth Operational Law Enforcement Agencies. This broader policy objective also underpins aspects of the National Organised Crime Response Plan.[353] A clearer framework will also help ensure that information collected under the AML/CTF regime is handled appropriately as recommended by the ALRC.

[353] Australian Government, *National Organised Crime Response Plan 2015-18*, 2015.

The safeguards, protections, powers and controls that apply under this framework also need to be reviewed and better targeted to cover confidential and sensitive information, and applied consistently, regardless of who is holding the information.

The proposal for a new framework for sharing AUSTRAC information is likely to result in the sharing of greater amounts of personal information. In some cases, the sharing of personal information may involve agencies or bodies which have not previously had access to such information and include agencies or bodies that may not be subject to the Privacy Act or equivalent obligations. In view of this, these proposals may have privacy risks and impacts that should be identified, considered and appropriately addressed as part of developing and implementing these proposals.

Recommendations

Recommendation 14.1

The Attorney-General's Department, in partnership with AUSTRAC and in consultation with other government agencies, should develop a simplified model for sharing information collected under the AML/CTF Act that is:

- responsive to the information needs of agencies tasked with combating ML/TF and other serious crimes
- supports collaborative approaches to combating ML/TF and other serious crime at the national and international level, and
- establishes appropriate safeguards and controls that are readily understood and consistently applied.

Recommendation 14.2

Subject to appropriate controls and safeguards, the AML/CTF Act should be amended to permit reporting entities to disclose suspicious matter report-related information to foreign parent entities and external auditors.

15. Audit, information-gathering and enforcement

Introduction

The audit, information-gathering and enforcement powers of the AML/CTF Act are set out in Parts 13, 14 and 15 of the Act.

The AML/CTF Act also provides for a range of civil and criminal sanctions for non-compliance with certain obligations. Several criminal offences relating to providing false and misleading documents or information are set out in Part 12 of the AML/CTF Act.

Audit powers

The audit provisions under Part 13 provide for the appointment of authorised officers to conduct audits and outline the powers of these officers, including the use of monitoring warrants.[354] Part 13 also sets out the powers of the AUSTRAC CEO to require a reporting entity to appoint an external auditor to audit the entity's AML/CTF processes and systems and its compliance with AML/CTF obligations, and require an entity to undertake and submit an ML/TF risk assessment.

Information-gathering powers

The information-gathering powers under Part 14 support AUSTRAC's regulatory function and enable authorised officers to issue a notice requiring a person to provide information or documents relevant to the operation of the AML/CTF Act, Rules and Regulations.[355] Other sections of the AML/CTF Act provide additional information-gathering powers related to transaction reporting and the registration of remittance providers.[356]

Enforcement powers and offence provisions

The AUSTRAC CEO has a number of powers under Part 15 of the AML/CTF Act to enforce compliance with AML/CTF obligations.[357] These include powers to:

- apply to the Federal Court for a civil penalty order (for the imposition of a pecuniary penalty) for the contravention of civil penalty provisions
- issue remedial directions to a reporting entity for the contravention of civil penalty provisions
- accept enforceable undertakings from reporting entities, and
- apply to the Federal Court for an injunction, comprising restraining injunctions or performance injunctions, in response to a reporting entity's non-compliance with its AML/CTF obligations.

---

[354] An authorised officer is defined under section 5 of the AML/CTF Act and generally means the AUSTRAC CEO or a person for whom an appointment as an authorised officer is in force under section 145.

[355] The *Crimes Legislation Amendment (Powers, Offences and Other Measures) Act 2015* received Royal Assent on 26 November 2015 and included amendments to address constraints identified by AUSTRAC with the operation of its information-gathering powers under section 167 of the AML/CTF Act. These amendments will allow for self-incriminating material to be given as evidence in a broader range of civil and criminal proceedings under section 169.

[356] Sections 49 and 50 of the AML/CTF Act; section 75N of the AML/CTF Act.

[357] The *Crimes Legislation Amendment (Powers, Offences and Other Measures) Act 2015* received Royal Assent on 26 November 2015 and included amendments to enable AUSTRAC to take a more flexible approach to obtaining information or documents under subsection 203(e) of the AML/CTF Act. The amendments give the authority issuing the notice the flexibility to stipulate time frames for compliance that appropriately fit the circumstances of the request.

Authorised officers, customs officers and police officers may also issue infringement notices where they have reasonable grounds to believe that a person has contravened an infringement notice provision.[358]

Criminal sanctions are available for a limited number of offences relating to failure to comply with obligations, with the most severe offences punishable by 10 years imprisonment and/or 10,000 penalty units.[359]

Consultation

Audit and information-gathering powers

Partner agencies proposed a number of amendments to the AML/CTF Act to strengthen the information-gathering powers, particularly the power of agencies to obtain information from reporting entities through notices issued under section 49.

Section 49 permits the AUSTRAC CEO and a number of Commissioners and CEOs of AUSTRAC partner agencies to issue a written notice to a reporting entity or any other person requiring further information to be provided in relation to a TTR, IFTI or SMR. [360] Partner agencies have reported varying degrees of compliance by reporting entities with section 49 notices. One agency suggested the creation of a criminal offence (similar to section 211 of the *Proceeds of Crime Act 2002*) for failure to comply would improve compliance. Partner agencies noted that the utility of civil penalty orders for the failure to comply with section 49 notices is diminished because the penalty orders can only be applied for by the AUSTRAC CEO, regardless of which agency originally issued the notice. [361]

Partner agencies raised similar concerns with the power to issue notices under section 50. Section 50 permits the AUSTRAC CEO or the Commissioner of Taxation to issue a written notice requiring a reporting entity to request information about the identity of holders of foreign credit and debit cards. However, only the AUSTRAC CEO can apply for a civil penalty order if a reporting entity fails to comply with the notices.

Some industry stakeholders raised concerns that the section 49 power was being used inconsistently by partner agencies and, at times, being used to fill gaps in the AML/CTF Act's transaction reporting requirements. They recommended a standard template be introduced for section 49 notices and that any gaps in the transaction reporting framework to be rectified by amendments to the AML/CTF Act or Rules.

AUSTRAC also proposed that the range of tools available for compliance testing be expanded beyond auditing powers.

Enforcement of AML/CTF Act obligations

Partner agencies considered that the civil and criminal offences regime under the AML/CTF Act could be strengthened to enhance enforcement efforts and more effectively deter non-compliance by reporting entities, particularly criminally complicit entities engaged in systematic non-compliance in support of large-scale, serious crime.

---

[358] Section 184 of the AML/CTF Act.

[359] See, for example, sections 136 (False or misleading information) and 137 (Producing false or misleading documents) of the AML/CTF Act.

[360] The Commissioner of the Australian Federal Police, the CEO of the Australian Crime Commission, the Commissioner of Taxation, the Comptroller-General of Customs and the Integrity Commissioner are permitted to issue a written notice under section 49(1). Investigating officers carrying out an investigation in connection with the matters raised in the TTR, IFTI or SMR also have the ability to issue such notices.

[361] Subsection 176(1) of the AML/CTF Act states 'Only the AUSTRAC CEO may apply for a civil penalty order'.

Some agencies submitted that the existing enforcement powers lacked proportionality and that civil penalties were not effective in deterring (criminally complicit) non-compliance. They proposed that the expanded use of infringement notices would better support AUSTRAC's enforcement strategies, as would a tiered penalty system, involving both civil and criminal penalties, for serious non-compliance and criminally complicit service providers.

However, some industry stakeholders contended that the use and availability of infringement notices should not be expanded, especially as they considered there was uncertainty about some obligations for reporting entities under the AML/CTF regime.[362]

Partner agencies, and AUSTRAC, noted that the process of applying to the Federal Court for a civil penalty order as a remedy for contraventions of AML/CTF obligations is costly and time consuming for both AUSTRAC and the reporting entity. They suggested that options for achieving expedited, and less expensive, enforcement outcomes should be explored.

Findings of the MER

The MER rated Australia as partially compliant with the FATF standard on the powers of financial institution supervisors.[363] The key deficiencies identified in the MER included:

- AUSTRAC's powers to inspect documents and require production of documents require either consent, or a court order or warrant
- a reporting entity can refuse or revoke permission for an authorised officer to enter the reporting entity's premises, potentially requiring the use of a warrant, and
- AUSTRAC does not have the power to withdraw, restrict or suspend a reporting entity's licence (except for remitters), with these powers instead lying with regulators who do not have express AML/CTF obligations.[364]

The MER also noted that there are no enforcement powers applicable to many DNFBPs, as most sectors are not regulated under the AML/CTF Act.[365] Issues in relation to coverage of the DNFBP sector are considered in *Chapter 4.2: Regime scope – Designated non-financial businesses and professions.*

The MER rated Australia as partially compliant with the FATF standards on criminal and civil sanctions[366] on the basis that:

- the range of sanctions available for AML/CTF breaches is limited, as the only civil and criminal penalties that can be imposed on the regulated sector must be imposed by a court
- DNFBPs are unable to be sanctioned for breaching AML/CTF obligations, as these sectors are not regulated under the AML/CTF Act, and
- penalties under the AML/CTF Act do not apply to the senior management of a reporting entity where it is the reporting entity that commits a breach of the AML/CTF obligations.

The MER noted that Australia has a best practice targeted financial sanctions (TFS) regime relating to terrorism, terrorism financing and proliferation of weapons of mass destruction (WMDs) under which

[362] *Chapter 19: Definitional issues* considers these areas of uncertainty identified by stakeholders.
[363] FATF Recommendation 27 (Powers of supervisors).
[364] Similar concerns are noted in relation to casino regulators in FATF Recommendation 28 (Regulation and supervision of designated non-financial businesses and professions).
[365] FATF Recommendation 28 (Regulation and supervision of designated non-financial businesses and professions).
[366] FATF Recommendation 35 (Sanctions).

financial institutions are obligated to freeze a person or entity's assets automatically upon that person or entity being designated by the United Nations. Despite this, the FATF found there was inadequate monitoring or supervision of the financial sector for compliance with these obligations by any competent supervisory authority, including AUSTRAC.

Discussion

Compliance testing powers

One of AUSTRAC's key regulatory goals is to assist reporting entities to strengthen their AML/CTF programs. This is achieved through educating and monitoring reporting entities, as well as working with reporting entities to improve compliance.

AUSTRAC conducts a range of supervisory activities to improve and promote compliance with AML/CTF obligations, ranging from low intensity or 'engagement' activities such as providing guidance and conducting forums to high intensity or 'escalated' activities such as on-site assessments.

The AUSTRAC CEO also has the power under Part 13 of the AML/CTF Act to appoint an external auditor carry out an audit of reporting entity's compliance with AML/CTF obligations, or specified aspects of those obligations. Before the AUSTRAC CEO can exercise this power, there must be reasonable grounds to suspect that the reporting entity has contravened, is contravening, or is proposing to contravene the AML/CTF Act, the regulations or the AML/CTF Rules.[367]

AUSTRAC has proposed that the AUSTRAC CEO be provided with additional tools for assessing the effectiveness of reporting entities' AML/CTF program and compliance with AML/CTF programs. This includes tools that allow AUSTRAC to gain an accurate spot check of an entity's day-to-day compliance with its CDD and transaction and suspicious matter reporting obligations. Some regulators have the power to conduct covert assessments for the purposes of testing compliance. For example, state and territory health departments monitor business's compliance with restrictions on the sale of tobacco to minors through covert actions.[368]

Options for enhancing AUSTRAC's ability to proactively undertake compliance testing should be explored in consultation with industry and government stakeholders to assist AUSTRAC to promote compliance with AML/CTF obligations and more effectively target supervisory activities.

Adopting standardised regulatory powers

The *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act) provides for a standard suite of provisions in relation to monitoring and investigation powers, as well as provisions regulating the use of civil penalties, infringement notices, enforceable undertakings and injunctions. The Regulatory Powers Act commenced on 1 October 2014, but only has effect where Commonwealth Acts are drafted or amended to trigger the standard provisions of the Regulatory Powers Act.

While the AML/CTF Act already includes most of these powers, the Act should be amended to adopt the model provisions under the Regulatory Powers Act. The relevant Regulatory Powers Act provisions offer greater clarity and certainty for AUSTRAC and reporting entities, and are designed to facilitate better compliance outcomes and more effective and consistent application of enforcement powers. The Regulatory Powers Act also includes operational safeguards, and maintains Parliamentary scrutiny over

[367] Subsection 162(2), AML/CTF Act.
[368] See, for example, New South Wales Department of Health, *Monitoring Compliance with the Sales to Minors' Prohibition – Procedures Manual,* 20 December 2010, http://www0.health.nsw.gov.au/policies/gl/2010/GL2010_016.html.

application of the Act to specific regulatory regimes. The adoption of Regulatory Powers Act powers also supports government policy of securing greater regulatory consistency.

Part 3 of the Regulatory Powers Act creates a framework for gathering material that relates to the contravention of offence and civil penalty provisions of an Act. These evidence-gathering powers should be available to AUSTRAC – they are consistent with AUSTRAC's regulatory role and are more effective and provide greater clarity than the existing information-gathering powers in the AML/CTF Act. Unlike the powers contained in Part 3 of the Regulatory Powers Act, the existing information-gathering powers under the AML/CTF Act neither provide a power to search for evidentiary material, nor a power to seize evidentiary material.

Additional powers under the AML/CTF Act not provided for in the Regulatory Powers Act should be retained.[369] These powers are specific to the AML/CTF framework and the enforcement of AML/CTF obligations.

One of the deficiencies identified in the MER was that AUSTRAC's powers to inspect documents and require production of documents require either consent or a court order or warrant. While the investigation powers in the Regulatory Powers Act would provide AUSTRAC with broader and better means of obtaining evidence, the exercise of these powers would still rely on either consent being given, or on the issuing of a warrant.

Australia's legal system has an established procedure for authorities to issue warrants and this power is readily exercised by law enforcement agencies (including AUSTRAC). It is not recommended that any change be made to the existing warrant process for requiring the production of documents.

Expanding the scope of remedial directions

The AUSTRAC CEO has the power to issue remedial directions under section 191 of the AML/CTF Act. Under this power, the AUSTRAC CEO can direct a reporting entity to take specified action to ensure the reporting entity does not commit any future breaches of their AML/CTF obligations. A civil penalty may apply to a failure to comply with a remedial direction.

Where a reporting entity has failed to comply with AML/CTF obligations in the past, the AUSTRAC CEO cannot issue a remedial direction to require the reporting entity to retrospectively comply with the relevant obligation.

The inability to issue remedial directions to require retrospective compliance has particular implications where a reporting entity has failed to comply with its obligations to submit transaction or compliance reports. To retrospectively enforce compliance with these obligations – and require the entity to submit the required reports – currently AUSTRAC must resort to enforceable undertakings or a court-issued injunction.

Expanding the power of the AUSTRAC CEO to issue remedial directions to require reporting entities to retrospectively rectify contraventions and lodge the required reports would provide a simpler means for AUSTRAC to secure reporting entity compliance.

Expanding the use of infringement notices

Infringement notices can be imposed by an authorised officer, a police officer or a customs officer under the AML/CTF Act if they have reasonable grounds to believe that a person has contravened an

[369] These include the power to issue a remedial direction, external audit powers relating to ML/TF risk assessments and powers to give statutory notices.

infringement notice provision. If the infringement notice penalty is paid within the required time frame, any liability in relation to the alleged contravention is discharged and no criminal or civil penalty proceedings will be brought.

The use of infringement notices under the AML/CTF Act is restricted to the following contraventions:

- failure to enrol on the Reporting Entities Roll (subsection 51B(1))
- failure to notify changes of enrolment details (subsection 51F(1))
- failure to give reports about movements of physical currency (subsection 53(3))
- failure to give reports about movements of bearer negotiable instruments (subsection 59(4))
- providing certain remittance services if unregistered or in breach of a condition of registration (subsections 74(1), (1A), (1B) and (1C)), and
- failure to notify the AUSTRAC CEO of certain matters (subsection 75M(1)).

Since 2013, AUSTRAC has issued four infringement notices to reporting entities. The highest pecuniary penalty imposed through these notices was AUD336,600 to a registered remittance network provider for a range of contraventions involving the provision remittance services through unregistered affiliates.

Non-compliance with regulatory requirements under the AML/CTF Act can take a number of forms. For example, partner agencies that issue notices under section 49 indicated that reporting entities often fail to:

- respond within the designated time frame
- provide the required or complete information
- provide the necessary information to allow an offence or suspect to be identified (in an SMR), and
- respond in a coordinated manner (for example, relevant documents are provided at different times).

Some partner agencies reported ongoing non-compliance with section 49 notices by some reporting entities.

Non-compliance with these notices can delay or frustrate investigations into serious crimes and ideally such non-compliance should be dealt with swiftly and summarily. However, to take action against a reporting entity that contravenes a section 49 notice, AUSTRAC must conduct civil proceedings through the courts. This process is costly and time consuming and does not always allow AUSTRAC to respond in a timely and proportionate manner to secure reporting entity compliance.

A number of AUSTRAC's partner agencies have suggested expanding the use of infringement notices under the AML/CTF Act to cover a range of other minor offences that are regulatory in nature, but for which civil and criminal penalties are currently the only available sanctions. These include the following offences:

- failure to lodge an SMR in the required time where there is clear evidence that a suspicion was formed and the report was not lodged (subsection 41(2))
- failure to lodge a TTR in the required time (subsection 43(2))
- failure to lodge an IFTI in the required time (subsection 45(2))
- failure to lodge an AML/CTF compliance report by the required date (subsection 47)
- failure to provide further information on request within the required time (subsection 49(2))

- failure to provide information about the identity of holders of foreign credit cards and foreign debit cards (subsection 50(7))
- failure to have an AML/CTF program (subsection 81(1)), and
- failure to make and retain records of an AML/CTF program (subsections 116(2), (3) and (4)).

Applying infringement notice provisions to contraventions of these obligations would give the AUSTRAC CEO additional, more expedient means for promoting and encouraging compliance, as an alternative to applying for a civil penalty order through the Federal Court. The provisions would give the CEO the flexibility to consider factors such as the seriousness of the breach, the size and sophistication of the reporting entity and the likely deterrent effect of a civil penalty or a fine, before deciding the most appropriate response. This would also address the FATF's criticism that the range of sanctions for AML/CTF breaches, particularly those that can be directly applied by AUSTRAC, is limited.

If the use of infringement notices is expanded, the power to issue notices for non-compliance should also be expanded to relevant AUSTRAC partner agencies that are able to issue written notices and directions under the AML/CTF Act. For example, if an agency has the power to issue a section 49 notice, that agency should also have the power to issue an infringement notice if a person or reporting entity fails to comply with the notice.[370] The Commissioner of Taxation should have a similar power to issue an infringement notice in relation to failures to comply with a section 50 notice.

Extending the power to impose infringement notices to those agencies that can impose requirements on reporting entities is a more efficient way of responding to non-compliance than the current situation, which compels partner agencies to refer such enforcement action to AUSTRAC.

Some industry stakeholders did, however, caution against creating further infringement notice provisions. They considered that the power to impose infringement notices should not be expanded while there was uncertainty over the application of the AML/CTF Act. This review makes a number of recommendations to clarify the scope and application of the AML/CTF Act, providing reporting entities with greater certainty about their AML/CTF obligations. This should accommodate industry concerns about the expansion of infringement notices provisions.

Greater flexibility in dealing with civil penalty orders

In addition to infringement notices, civil penalty orders may also apply to contraventions of the section 49 and 50 information-gathering powers. However, where there is a contravention, only the AUSTRAC CEO has the power to apply for a civil penalty order under the AML/CTF Act, no matter which agency issued the original notice.

Other agencies with information-gathering powers under the AML/CTF Act should have the power to apply for a civil penalty order for contraventions of notices they issue under subsections 49(1), 50(2) and 50(5). Such a power would enable those agencies to more effectively use and enforce their information-gathering powers without having to rely on AUSTRAC to address any non-compliance.

Consistency in use of information-gathering powers

To promote consistency in the use of information-gathering powers across different agencies, AUSTRAC should develop template section 49 and 50 notices. The use of standard forms will also assist reporting entities to comply with their obligations.

[370] This includes the ATO, AFP, ACC, the Comptroller of Customs and ACLEI (see subsection 49(1) of the AML/CTF Act).

A number of stakeholders raised concerns that the section 49 power in particular was sometimes being used to fill gaps in the AML/CTF Act's transaction reporting requirements. That is, agencies are using the information-gathering powers to systematically seek information that reporting entities are not required to include in transaction reports submitted to AUSTRAC. This issue will be considered as part of AUSTRAC's current project to combat foreign fighters by enhancing its data capture and integrity process for transaction reports.[371]

Application of sanctions to directors and senior managers

Currently, most sanctions under the AML/CTF Act can apply to natural persons as well as reporting entities. This includes where it is the senior manager or director who breaches the AML/CTF Act or Rules.

The MER raised concerns that these sanctions do not extend to directors and senior managers of a reporting entity where it is the reporting entity that has breached the AML/CTF Act or Rules. To address this, the AML/CTF Act should be amended to provide that sanctions for breaches of the AML/CTF Act or Rules can also apply to senior managers and directors in appropriate circumstances.[372]

Licensing requirements

The MER noted that currently currency exchange businesses in Australia are not licensed or registered (under the AML/CTF Act or any other legislation).[373]

The MER also noted that AUSTRAC does not have the power to withdraw, restrict or suspend reporting entities licenses, except for remitters. For the majority of reporting entities, licensing powers are the responsibility of other Commonwealth, state or territory regulators whose primary focus is not AML/CTF compliance. For example, the MER considered that:

- APRA is not explicitly empowered to revoke a bank's license for a breach of the AML/CTF Act, and [374]
- state and territory casino licensing authorities do not have express AML/CTF responsibilities and not all casino licencing legislation requires consideration of the associates of the applicants.[375]

Proposals to change licensing requirements to comply with the FATF standards would involve consultation with several Commonwealth, state and territory regulators and likely require changes to a wide range of legislation. Such changes should be explored with the relevant government agencies outside of this review process.

Supervision of compliance with Australian sanction laws

While Australia's TFS framework complies with the FATF standards, the MER found that Australia does not adequately monitor or supervise reporting entities for compliance with the terrorism, terrorism financing and proliferation financing TFS regimes.

DFAT has primary responsibility for administering Australian sanction laws and maintains a 'Consolidated List' of all persons and entities who are subject to TFS or travel bans.[376]

---

[371] See *Chapter 6: Reporting obligations* for further information.
[372] Section 28 of the *Monetary Authority of Singapore Act* provides one example of how this could be achieved.
[373] See FATF Recommendation 26 (Regulation and supervision of financial institutions).
[374] See FATF Recommendation 27 (Powers of supervisors).
[375] See FATF Recommendation 28 (Regulation and supervision of designated non-financial businesses and professions).
[376] See DFAT's website for further information: http://dfat.gov.au/international-relations/security/sanctions/pages/consolidated-list.aspx, (accessed 15 January 2016).

Australia implements TFS primarily through the *Charter of the United Nations Act 1945* and the *Autonomous Sanctions Act 2011* and their implementing regulations. These programs are administered by DFAT, in coordination with other relevant agencies. Everyone subject to Australian jurisdiction, including financial institutions and DNFBPs, has an obligation to freeze any assets they may hold of a person or entity designated for sanctions. They are also prohibited from making assets available to designated persons or entities.

Australia's TFS framework implements financial sanctions that are within the FATF's mandate (that is, terrorism, terrorism financing and proliferation of WMDs and its financing)[377]. Australia also implements a number of other TFS that reflect Australia's broader obligations under international law, foreign policy objectives or other areas of international concern.

While DFAT administers Australian sanction laws, including processing applications for sanctions permits, DFAT is not a supervisory agency. Consideration should therefore be given to which agency would be most appropriate to undertake systematic sanctions compliance monitoring. Integrating sanctions supervision and compliance engagement within the AML/CTF regulatory regime could provide benefits to financial institutions which, in many instances, currently operate a single AML/CTF and sanctions compliance function. This could be achieved, for example, by requiring reporting entities to address their sanctions risk as part of developing an AML/CTF program. It will be necessary to assess whether AUSTRAC has the resourcing capacity to enhance its role in relation to supervising compliance by its regulated population in relation to Australian sanction laws.

As noted above, Australia's overall TFS framework is much broader than the TFS that relate to the AML/CTF regime. While expanding AUSTRAC's supervisory role to include the supervision of Australia's entire TFS framework is outside the scope of the review, it would be inefficient to consider supervision of FATF-mandated TFS regimes without also considering Australia's broader TFS framework.

Recommendations

Recommendation 15.1

AUSTRAC and the Attorney-General's Department should explore options for expanding AUSTRAC's compliance testing tools in consultation with industry and government stakeholders.

Recommendation 15.2

The AML/CTF Act should be amended to adopt the model regulatory powers set out in the *Regulatory Powers (Standard Provisions) Act 2014*, while maintaining the existing powers in the AML/CTF Act relating to remedial directions, external audits, ML/TF risk assessments and statutory notices.

Recommendation 15.3

The AML/CTF Act should be amended to expand the remedial directions power to allow AUSTRAC to direct reporting entities to remedy past contraventions of AML/CTF reporting obligations.

Recommendation 15.4

The AML/CTF Act should be amended to expand the infringement notice provisions under subsection 184(1A) to include a wider range of minor offences established under the AML/CTF Act that are regulatory in nature.

[377] This includes the TFS regimes in relation to Al Qaida, the Taliban, counter-terrorism, DPRK and Iran. See DFAT's website for further information: http://dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/Pages/sanctions-regimes.aspx, (accessed 15 January 2016).

Recommendation 15.5

The AML/CTF Act should be amended to give agencies that already have the power to issue notices to a person or reporting entity under sections 49 and 50 of the AML/CTF Act an additional power to issue infringement notices or apply for civil penalties if that person or entity fails to comply with such a notice.

Recommendation 15.6

AUSTRAC should create template section 49 and 50 notices for use by all relevant agencies.

Recommendation 15.7

The AML/CTF Act should be amended to clarify that sanctions for breaches of the AML/CTF Act or Rules by reporting entities can also apply to senior managers and directors in appropriate circumstances.

Recommendation 15.8

AUSTRAC and the Department of Foreign Affairs and Trade should explore the feasibility of AUSTRAC monitoring and supervising compliance with Australian sanction laws.

16. Administration of the Act

Part 16 of the AML/CTF Act provides for the following matters:

- the establishment and functions of AUSTRAC
- the office, functions and appointment of the AUSTRAC CEO
- the staff of AUSTRAC
- reports and information (including annual reports)
- directions by the Minister, and
- the making of Rules.

The functions of the AUSTRAC CEO underpin the CEO's powers. These functions relate to:

- retaining, compiling, analysing and disseminating eligible collected information
- providing advice and assistance, in relation to AUSTRAC information, to the persons and agencies who are entitled or authorised to access AUSTRAC information under Part 11 of the AML/CTF Act
- advising and assisting reporting entities in relation to their obligations under the AML/CTF Act, Rules and Regulations
- advising and assisting the representatives of reporting entities in relation to the entities' compliance with the AML/CTF Act, Rules and Regulations, and
- promoting compliance with the AML/CTF Act, Rules and Regulations.[378]

The functions of the AUSTRAC CEO may also include any other functions that are conferred on the CEO under the AML/CTF Act, Regulations or any other law of the Commonwealth.

Consultation

Industry stakeholders did not provide any comments on the provisions of Part 16.

The findings of the MER

The MER examined AUSTRAC's two complementary roles as Australia's FIU and AML/CTF regulator.

The MER rated Australia as compliant with the FATF's standard that requires countries to establish an FIU with specific functions and powers related to receiving, analysing and disseminating financial intelligence.[379]

Issues relating to AUSTRAC's role as the AML/CTF regulator[380] are considered in *Chapter 15: Audit, information-gathering and enforcement*.

Discussion

General presumption of powers

Unlike the CEOs of other Australian government agencies that perform regulatory or intelligence functions, the AUSTRAC CEO does not have an explicit power to carry out his or her functions.[381]

[378] Section 212 of the AML/CTF Act.
[379] FATF Recommendation 29 (Financial intelligence unit).
[380] The MER rated Australia partially compliant with FATF Recommendation 27 (Powers of supervisors).

The AML/CTF Act should be amended to address this issue and give the AUSTRAC CEO a power to do all things necessary or convenient for, or in connection with, the performance of his or her functions.

This is a standard power used to give statutory authorities the power to perform their functions.[382]

Similarly, while the functions of the AUSTRAC CEO currently include 'retaining, compiling, analysing and disseminating eligible collected information', Part 16 should be amended to include an explicit power for the AUSTRAC CEO to collect and receive information under the AML/CTF Act.

Extending the functions of the AUSTRAC CEO

The scope of the CEO's functions under Part 16 requires updating to reflect the full range of work performed by AUSTRAC. This includes the role played by AUSTRAC in supporting international and collaborative efforts to combat money laundering, terrorism financing and other serious crimes, as well as other efforts to support government policy-making, industry education, expanded typologies, public alerts, and academic research. Such a change would support the recommended reforms to the secrecy and access provisions in the AML/CTF Act.[383]

Recommendations

Recommendation 16.1

The AML/CTF Act should be amended to:

(a) give the AUSTRAC CEO the power to do all things necessary or convenient to be done for, or in connection with, the performance of his or her duties, and

(b) expand the scope of the functions of the AUSTRAC CEO to include:

- retaining, compiling and analysing AUSTRAC information
- facilitating access to, and the sharing of, AUSTRAC information to support domestic and international efforts to combat money laundering, terrorism financing and other serious crimes, and
- disseminating AUSTRAC information, where appropriate, to support government policy-making, industry education, public education and academic research.

[381] See section 22 of the *Australian Sports Anti-Doping Authority Act 2006* and section 19 of the *Australian Crime Commission Act 2002*.
[382] Office of Parliamentary Counsel, *Drafting Direction No. 36 – Statutory and other bodies*, October 2012, p. 45, http://www.opc.gov.au/about/docs/drafting_series/DD3.6.pdf.
[383] See *Chapter 14: Secrecy and access* for further information.

17. Exemptions process

Exemptions from complying with AML/CTF obligations can be provided under the AML/CTF Act or the AML/CTF Rules, or prescribed by an exemption instrument or modification issued by the AUSTRAC CEO.[384]

The AUSTRAC CEO may also grant exemptions from obligations under the FTR Act.

Since 2006, the AUSTRAC CEO has granted approximately 120 exemptions to reporting entities in accordance with AUSTRAC's Exemption policy.[385] Applications for exemptions are assessed on a case-by-case basis and granted where there is evidence that a service, or the circumstances surrounding the provision of a service, poses a low ML/TF risk.

Consultation

Industry stakeholders considered that the application process for exemptions is protracted, resource intensive, costly and inaccessible to smaller reporting entities.

Some stakeholders also suggested that AUSTRAC provide more exemptions for classes of services that they consider pose low ML/TF risks. This includes:

- for hotels and clubs, raising the electronic gaming machine exemption threshold from 15 machines to 25 machines
- for gaming providers, removing the need for a customer to be identified within 90 days of opening an account if the customer wishes to close the account and withdraw a balance of less than AUD10,000, and
- for financial services providers, creating an exemption for secured equipment finance facilities.

The findings of the MER

The MER concluded that exemptions from AML/CTF obligations granted by AUSTRAC were inconsistent with the FATF standards because they were not granted solely on the basis of a demonstrated low ML/TF risk.[386] In reaching this conclusion, the MER referred to subsection 213(3) of the AML/CTF Act which requires the AUSTRAC CEO, in performing his or her functions under the Act, to consider ML/TF risk as just one of several other matters. The MER also stated there was no provision for ongoing review of exemptions granted by AUSTRAC.

The MER considered that the Australian exemptions regime may diminish the application of CDD in some situations envisaged by the FATF standards.[387] See *Chapter 5: Customer due diligence* for further consideration of this issue.

Discussion

Industry requests for exemptions

Industry stakeholders supported the inclusion of an exemptions framework under the AML/CTF regime, but considered that there was room to improve the exemption process. Stakeholders that had applied for

[384] Section 248 of the AML/CTF Act provide for exemptions and modifications of AML/CTF obligations by the AUSTRAC CEO.
[385] AUSTRAC, *Exemption policy*, http://www.austrac.gov.au/about-us/policies/exemption-policy, (accessed 15 January 2016).
[386] FATF Recommendation 1 (Assessing risks and applying a risk-based approach). See criterion 1.6 of the FATF Methodology or paragraph a2.7of the MER.
[387] FATF Recommendation 10 (Customer due diligence).

exemptions indicated that the process was resource intensive, protracted and costly. Other stakeholders appeared unaware of the option to apply for an exemption or considered that they did not have the capacity and/or resources to successfully pursue such an application.

The application process for exemptions should be reviewed by AUSTRAC in consultation with industry to establish a more accessible, streamlined and expedient process. AUSTRAC should also develop guidelines to assist reporting entities to understand what they need to do to complete an application and publish appropriate service delivery timeframes for determining applications.

Industry stakeholders submitted numerous proposals for specific exemptions for low ML/TF risk services during the consultation process. This suggests there is scope for AUSTRAC to adopt a proactive and systematic approach to providing exemptions for classes of low ML/TF risk services rather than relying on individual reporting entities to shoulder the burden of proving a particular exemption is reasonable and justified. A more proactive and systematic approach to providing exemptions for low ML/TF risk services would generate ongoing regulatory efficiencies and be consistent with the Government's better regulation agenda.

Addressing issues identified in the MER

The MER's main criticism of the exemptions process under the AML/CTF Act was that the level of ML/TF risk is not the sole consideration in granting exemptions from AML/CTF obligations.

There are a range of matters that the AUSTRAC CEO must consider in performing his or her functions, including the granting of exemptions and modifications. These matters include the integrity of the financial system, crime reduction, the desirability of adopting a risk-based approach, regulatory burden, economic efficiency, competitive neutrality, competition and privacy.[388]

While the ML/TF risks should be a prime consideration when determining such exemptions, other important policy considerations need to be balanced against those ML/TF risks. This includes considering whether a regulatory measure places an unnecessary financial and administrative burden on regulated entities or significantly disrupts the efficient conduct of business while delivering limited benefits in terms of reducing crime and protecting the integrity of the financial system.

The AML/CTF Act should be amended to specify the matters the AUSTRAC CEO must consider when determining exemptions. ML/TF risk should be the prime consideration, but other matters should also be taken into account once low ML/TF risk has been established.

AUSTRAC should also review exemptions at appropriate intervals to assess whether the exemptions are still appropriate, particularly where the ML/TF risk profile which informed the exemption decision may have changed. This process should be formalised in AUSTRAC's *Exemptions Policy*.

[388] Subsection 212(3) of the AML/CTF Act.

Recommendations

Recommendation 17.1

The AML/CTF Act should be amended to set out the specific matters that the AUSTRAC CEO must take into account when determining exemptions, with the level of ML/TF risk posed being the prime consideration.

Recommendation 17.2

AUSTRAC should adopt a more proactive approach to identifying opportunities to reduce unnecessary regulatory burden where the designated service, or the circumstances in which the designated service is provided, poses a low ML/ TF risk.

Recommendation 17.3

AUSTRAC should, in consultation with industry, simplify and streamline the application process for reporting entities seeking exemptions from AML/CTF obligations and develop guidance to assist reporting entities to navigate the new process.

Recommendation 17.4

AUSTRAC should amend its *Exemption Policy* to specify:

- time frames for AUSTRAC to determine exemption applications, and
- time frames for reviewing the continued appropriateness of exemptions granted.

18. Financial Transaction Reports Act 1988

The AML/CTF Act operates alongside the *Financial Transaction Reports Act 1988* (FTR Act).

The FTR Act was introduced in 1988 to assist in administering and enforcing taxation laws as well as other Commonwealth, state and territory legislation. With the introduction of the AML/CTF Act in 2006, certain parts of the FTR Act were repealed or became inoperative. However, the FTR Act continues to impose some regulatory requirements for 'cash dealers' and solicitors.

A cash dealer must submit significant cash transaction reports (SCTRs) and suspect transaction reports (SUSTRs) to AUSTRAC, while solicitors must report SCTRs. SCTRs are equivalent to the TTR reporting obligation under the AML/CTF Act and SUSTRs are equivalent to the SMR reporting obligation.

Cash dealers are defined in section 3 of the FTR Act to include a wide range of businesses. However, the FTR Act reporting obligations do not apply if the same service is captured under the AML/CTF Act as a designated service and if the relevant transaction occurred after the AML/CTF Act reporting obligations commenced. This means the majority of cash dealers do not have reporting obligations under the FTR Act, as they have overriding obligations under the AML/CTF Act instead.

In practice, the only entities which retain reporting obligations under the FTR Act are:

- businesses that sell traveller's cheques, such as Australia Post and travel agents (SUSTR and SCTR reporting obligations) [389]
- insurance intermediaries, such as motor vehicle dealers and travel agents (SUSTR and SCTR reporting obligations)
- general insurance providers, such as motor vehicle dealers (SUSTR and SCTR reporting obligations), and
- solicitors (SCTR reporting obligations).

Consultation

Stakeholders supported the repeal of the FTR Act to remove duplication and regulatory inefficiencies between the two Acts.

Discussion

The remaining reporting obligations under the FTR Act should be incorporated into the AML/CTF Act, particularly as the operation of the Acts leads to overlap and regulatory inefficiencies for government, industry and the public, without any demonstrable benefit.

The repeal of the FTR Act would ensure a more efficient use and application of AUSTRAC resources. For example, AUSTRAC would no longer need to apply resources to monitor compliance with the FTR Act or maintain IT systems to receive and analyse transaction reports submitted under this legislation. Repealing the FTR Act would also be consistent with the Government's better regulation policy by removing regulatory inefficiencies where, for example, reporting entities have separate and distinct obligations under both the AML/CTF Act and the FTR Act.

[389] Under the AML/CTF Act, the issuing, cashing or redeeming of a traveller's cheque 'in the capacity of issuer' are all designated services, but not the selling of traveller's cheques. This means that a person who sells traveller's cheques retains residual obligations under the FTR Act.

The SCTRs and SUSTRs submitted to AUSTRAC by entities under the FTR Act are a valuable source of financial intelligence and should be transitioned to the AML/CTF Act, with the following caveats:

- **selling of traveller's cheques**: Due to the marked decline in the use of traveller's cheques, AUSTRAC should conduct an ML/TF risk assessment on whether the designated services associated with traveller's cheques should continue to be regulated under the AML/CTF Act.[390]
- **solicitors**: *Chapter 4.2: Regime scope – Designated non-financial businesses and professions* considers the application of broader AML/CTF Act regulation to solicitors. The cost-benefit analysis of regulating legal practitioners under the AML/CTF regime recommended in *Chapter 4.2* should consider the existing reporting obligations for solicitors under the FTR Act.
- **motor vehicle dealers (as insurance intermediaries and general insurance providers):** *Chapter 4.2: Regime scope – Designated non-financial businesses and professions* considers the application of broader AML/CTF Act regulation of motor vehicle dealers.[391] The cost-benefit analysis of regulating motor vehicle dealers recommended in *Chapter 4.2* should consider the existing reporting obligations for motor vehicle dealers under the FTR Act.
- **other insurance intermediaries and general insurance providers:** The FATF standards only require life insurance and investment-related insurance products to be regulated and not general insurance.[392] Therefore, the FTR Act reporting requirements for these cash dealers (primarily travel agents) should not be transferred to the AML/CTF Act.

The repeal of the FTR Act will result in the repeal of the Financial Transaction Reports Regulations 1990. Amendments will be required to the AML/CTF Act and Rules to address any associated transitional issues.[393]

Recommendations

Recommendation 18.1

Repeal the FTR Act and Regulations and amend the AML/CTF Act and Rules to:

(a) retain reporting requirements in relation to traveller's cheques, motor vehicle dealers and solicitors while the broader consideration of AML/CTF Act regulation of these businesses occurs, and

(b) address any transitional issues resulting from the repeal of the FTR Act and Regulations.

Recommendation 18.2

In the repeal of the FTR Act, insurance intermediaries and general insurance providers, apart from motor vehicle dealers, should not retain their reporting obligations.

[390] See *Chapter 4.1: Regime scope – Existing designated services* for further discussion.
[391] Motor vehicle dealers are 'high-value dealers' as they are involved in the buying and selling of high-value commodities.
[392] See the FATF's definition of 'financial institution' in the FATF Recommendations.
[393] For example, provisions preserving secrecy and access provisions in relation to SUSTRs or information-gathering notices in relation to SCTRs and SUSTRs.

19. Definitional issues

Section 5 of the AML/CTF Act defines key terms and concepts used in the Act. Definitions are also set out in Part 1.2 of the AML/CTF Rules. Stakeholders identified a number of definitions which they considered required amending or clarifying. Some definitions are considered within the relevant chapters of this report, with the remaining definitions considered separately below.

AML/CTF Act definitions

Account

Section 5 defines 'account' to include a credit card account, a loan account and an account of money held in the form of units in a cash management trust or a trust of a kind prescribed by the AML/CTF Rules. The term is used in a number of the designated services in table 1 of section 6 of the AML/CTF Act.[394] Stakeholders advised that this definition had created uncertainty for industry, as a number of other types of accounts were not expressly included (for example, deposit, transaction and debit card accounts).

The list of accounts included in the definition is not exhaustive. That is, deposit, transaction and debit card accounts are not excluded from the definition. However, because certain types of account are listed, the definition has created the impression that they are excluded. To provide clarity and certainty, the definition should be simplified to remove the list of accounts, leaving 'account' to retain its ordinary meaning. This should be supplemented by guidance explaining what types of account could be included in the definition.

A number of submissions also commented on whether the definition of account sufficiently captured new payment methods. See *Chapter 4.2: Regime scope – Payment types and systems* for further discussion of this issue.

Control test

Section 11 of the AML/CTF Act provides that where it is necessary to test if a person controls a company or a trust, the control test be determined in the same manner as set out in sections 1207Q or 1207V of the *Social Security Act 1991*. This 'control test' is also used to determine residency under section 14 of the AML/CTF Act and shell bank affiliation under section 15 of the AML/CTF Act.

Stakeholders considered that it was inappropriate for the AML/CTF Act to rely on the control test used in the Social Security Act because of the broad application of the test under that Act.

For example, if an individual passes the Social Security Act control test for a company, so do all of their 'associates'. An individual's associate is defined broadly under the Social Security Act to include, for example, their second cousins. When applied to the AML/CTF Act, this interpretation could lead to the conclusion that the company is considered to be resident in each jurisdiction in which a second cousin of the controlling individual resides. This interpretation is significantly broader than that intended by the AML/CTF Act.

To address this issue, the control test under the AML/CTF Act should be redrafted to apply more narrowly. The FATF's definition of beneficial owner provides a useful foundation for the redrafted definition.[395]

---

[394] Items 1-4, 14-16, 18-20A of table 1, section 6 of the AML/CTF Act. Account is also used in the definitions for the designated services in items 11-13 of table 3, section 6 of the AML/CTF Act.

[395] The FATF Recommendations define 'beneficial owner' to be 'the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement'. 'Ultimately owns or controls' is defined to 'refer to situations in which ownership/control is exercise through a chain of ownership or by means of control other than direct control'. This definition is already used as the base for the beneficial owner definition in Part 1.2 of the AML/CTF Rules.

Credit and debit card

One stakeholder proposed that the AML/CTF Act definitions of 'credit card' and 'debit card' should be amended so they are linked to the definitions used in section 12DL of the *Australian Securities and Investments Commission Act 2001* (ASIC Act). Currently, credit and debit cards are defined in section 5 of the AML/CTF Act as having the same meaning as in Schedule 2 to the *Competition and Consumer Act 2010* (CC Act). Credit and debit cards are defined in section 39 of the CC Act.

The ASIC Act and CC Act definitions are similar. However, the ASIC Act definitions specify that they only include cards that are 'financial products'. The section 39 definitions in the CC Act are broader as they are not limited to financial products.

The current link between the AML/CTF Act definitions and the CC Act definitions is problematic, due to complications caused by subsection 131A(2)(d) of the CC Act. Subsection 131A(2)(d) states that the CC Act definitions do not, in fact, apply to credit and debit cards that are financial products. This qualification has created confusion for reporting entities, as it is unclear whether this limitation under subsection 131A(2)(d) also applies to the definitions under the AML/CTF Act (with the result that credit and debit cards that are financial products are excluded from the AML/CTF Act definitions).

The AML/CTF Act is intended to apply to credit and debit cards that are financial products. To clarify this, section 5 of the Act should be amended to include the text of the section 39 credit and debit card definitions. This will avoid any confusion which arises due to subsection 131A(2)(d) of the CC Act.

Factoring and forfaiting

The items 8 and 9 designated services of table 1 of table 6 of the AML/CTF Act cover two related financing arrangements:

- Item 8: **factoring** a receivable, where the receivable is factored in the course of carrying on a factoring business.
- Item 9: **forfaiting** a bill of exchange or a promissory note, where the bill or note is forfaited in the course of carrying on a forfaiting business.

The terms 'factoring' and 'forfaiting' are not defined in the AML/CTF Act or Rules. One stakeholder considered that factoring should be defined in the AML/CTF Act (or Rules) to clarify whether it includes:

- the forfaiting designated service, and
- different types of factoring, such as reverse factoring (supply chain financing).

While factoring and forfaiting are two very similar financial arrangements (a supplier sells their accounts or notes receivable to another person), they are currently two separate designated services under the AML/CTF Act because factoring relates to receivables and forfaiting relates to the bills of exchange and promissory notes. However, prescribing them as separate designated services has led to confusion within industry as to whether the services are exclusive or complementary.

To clarify the issue, the two designated services should be combined into one overarching designated activity.[396] In combining the two designated services, a definition should be developed to clarify whether the different types of factoring, such as reverse factoring, are included.

Loan

Loan is defined in section 5 of the AML/CTF Act. Paragraphs (a)-(d) set out activities that are included within the definition, while paragraphs (e)-(g) set out activities that are not included.

[396] See *Chapter 4.1: Regime scope – Existing designated services* for further information.

Partner agencies commented that the exclusions in (e)-(g) are so broad so as to almost cancel out the inclusions at paragraphs (a)-(d). The definition should be redrafted and simplified to provide greater clarity about what is included within the definition of loan.

Signatory

Section 5 defines 'signatory', in relation to an account with an account provider, to mean the person, or one of the persons, on whose instructions (whether required to be in writing or not and whether required to be signed or not) the account provider conducts transactions in relation to the account. Signatories are the customer of a number of designated services.[397] Industry considered that signatory should be redefined to apply more narrowly. One stakeholder used an example of a department store to illustrate this concern.

CASE STUDY 15: SIGNATORIES AT A DEPARTMENT STORE

A department store has 40 separate cash registers, each of which has EFTPOS facilities. Each payment through a cash register may be seen as a transaction on the account of the store owner. Therefore, each store cashier is a person who conducts a transaction on behalf of the store owner. Following this interpretation, each cashier is a signatory and therefore could be a customer receiving a designated service.

In this example, if cashiers are considered customers receiving a designated service, AML/CTF obligations will apply to each transaction – for example, the obligation to verify a cashier's identity – an outcome which is not intended under the AML/CTF Act. Similarly, a large corporation with numerous signatories to its accounts will attract CDD obligations for each signatory, an issue that would be exacerbated where a corporation frequently changes signatories (although this impact may be mitigated by AML/CTF Rules limiting the reportable details required for signatories[398]).

The focus of the obligations relating to signatories should be clarified and the definition of signatory should be amended so it applies more narrowly to persons with authority to authorise payment transactions.

Other stakeholders sought clarification as to whether people with online access to accounts were signatories. It is impractical for the definition of signatory to anticipate every situation where a person has online access to an account. Rather it is appropriate that a reporting entity would consider this issue as part of its risk-based approach to ML/TF. Instead, more guidance should be developed to provide greater clarity for reporting entities on when a person is a signatory.

The redrafted definition should also include a power under the AML/CTF Rules to amend the definition of signatory to exclude or include persons where the ML/TF risk justifies such an exclusion or addition. This will give the definition flexibility and allow it to remain responsive to new and emerging ML/TF risks.

Stored value card

Industry stakeholders considered that the definition of a stored value card (SVC) under section 5 of the AML/CTF Act does not assist industry's understanding of what a SVC is.

[397] Items 2, 3, 18A, 19A and 20A of table 1 and items 12 and 13 of table 3, section 6 of the AML/CTF Act.
[398] See Chapter 19 of the AML/CTF Rules.

A SVC is currently defined under section 5 of the AML/CTF as:

> ***stored value card*** does not include a debit card or credit card but includes a portable device (other than a debit card or credit card) that:
>
> (a) is capable of:
>
> (i) storing monetary value in a form other than physical currency; or
>
> (ii) being used to gain access to monetary value stored in such a form; and
>
> (b) is of a kind prescribed by the regulations.

Stakeholders considered that, as no SVC has been prescribed by regulation, no product on the market actually falls within the definition of SVC.

The definition of a SVC in section 5 is intended to be inclusive, rather than exclusive. That is, the definition should carry its 'ordinary' meaning – that of a portable device that can store monetary value in a non-physical form, or be used to access monetary value in that form. A type of SVC should not have to be prescribed by regulation to fall within the definition of an SVC.

The definition of SVC should be redrafted to provide industry with greater clarity as to what products meet the definition of a SVC. The definition should remain broad and inclusive to ensure that future technological developments will be captured by the definition. The definition should also be able to include SVCs that are entirely digital and do not utilise a physical 'card'.

Derivative and security

Section 5 of the AML/CTF Act defines 'derivative' as having the same meaning as in Chapter 7 of the *Corporations Act 2001*, where this term is defined as an arrangement as set out in section 761D of that Act. Section 5 of the AML/CTF Act similarly defines 'security' by reference to section 92 of the Corporations Act, but disregards subsections 92(3) and (4). Derivatives and securities then appear in the items 33 and 35 designated services of table 1 of section 6 of the AML/CTF Act.

One stakeholder considered that by relying on the Corporations Act to define derivative and security, the AML/CTF Act applies to a wide range of instruments, transactions and relationships that need not be issued by a financial institution as defined by the FATF.[399] This stakeholder considered that a wide range of executory contracts that are not, in substance, financial services, could meet the AML/CTF Act definition of a derivative and therefore attract regulatory obligations under the AML/CTF regime.

For example, one definition of derivative in the Corporations Act includes any arrangement for a future provision of any kind of consideration, where 'the amount of consideration or the value of the arrangement' varies by reference to 'the value or amount of something else (of any nature whatsoever and whether or not deliverable)'.[400] The stakeholder considered that a gift card could technically fall within this definition – while the gift card will have a stated dollar value, the *value of the arrangement* will vary depending on whether, for example, the goods the card holder wishes to purchase are on sale or otherwise discounted.

Under this interpretation, a seller of gift cards could then be providing a designated service by selling a derivative under the item 35 designated service and therefore have obligations under the AML/CTF Act.[401] The same seller would be unlikely to have licencing obligations under the Corporations Act due to the application of exemptions under that Act.[402] These exemptions, however, are not included within the basic

[399] The FATF Recommendations defines a 'financial institution' to include any natural or legal person who conducts as a business 'trading in money market instruments (cheque, bills, certificates of deposit, derivatives etc.)' for or on behalf of a customer'.
[400] Regulation 7.1.104(2)(c) of the *Corporations Regulations 2001*.
[401] Issuers of stored value cards are captured under the regime under the section 6, table 1, item 23 designated service.
[402] See for example Regulation 7.6.01(1)(m) of the *Corporations Regulations 2001*.

definition of derivatives within the Corporations Act, and so are not applicable to the AML/CTF Act definition. Similar issues could arise because of the AML/CTF Act's reliance on the broad definition of security used in the Corporations Act.

The potentially wide interpretation of derivative and security used within the AML/CTF Act could result in confusion as to whether AML/CTF obligations apply to arrangements not intended to be covered by the AML/CTF regime. The definition of derivative should not apply, for example, to non-financial products where there is no obligation on the product provider to hold an AFS license under the Corporations Act.

Despite these issues, the Corporations Act does provide a suitable framework for the regulation of derivatives and securities in Australia. It is appropriate that the derivative and security definitions used in the AML/CTF Act remain linked to those used in the Corporations Act (rather than draft new definitions that are specific to the AML/CTF Act). Any arrangements inadvertently caught under the AML/CTF Act due to its reliance on Corporations Act definitions should be exempted from the AML/CTF Act through amendments to the AML/CTF Rules.[403]

AML/CTF Rules definitions

Acceptable identification documents

Part 1.2 of the AML/CTF Rules defines the 'reliable and independent documentation' that reporting entities can use to identify customers. This documentation includes:

(1) an original primary photographic identification document

(2) an original primary non-photographic identification document, and

(3) an original secondary identification document.

A note to the definition explicitly advises that this is an 'inclusive' definition (rather than 'exhaustive'):

> *Note* This is not an exhaustive definition. A reporting entity may rely upon other documents not listed in paragraphs (1) to (3) above as reliable and independent documents, where that is appropriate having regard to ML/TF risk.

The documents listed in paragraphs (1) to (3) are also defined in Part 1.2. However, these definitions are exhaustive rather than inclusive.

This has led to confusion amongst reporting entities, as a document may not fall within the exhaustive definition of 'primary photograph identification document' but could fall within the inclusive 'reliable and independent documentation' definition. This can lead to reporting entities rejecting identification documentation that may otherwise be reliable and independent.

For example, Singapore's National Identity Card contains a photograph and the person's fingerprint, but not a person's signature. Primary photographic identification document is defined to mean 'a national identity card issued for the purpose of identification that contains a photograph and the signature of the person in whose name the document is issued'. So while Singapore's National Identity Card could be considered to be reliable and independent documentation, the card does not fall within the definition of 'primary photographic identification document' due to the lack of a signature, which is a confusing outcome.

The definitions of an 'original primary photographic identification document', an 'original primary non-photographic identification document', and an 'original secondary identification document' should be redefined to be 'inclusive' definitions consistent with the 'reliable and independent documentation'

[403] See, for example, Chapter 22 of the AML/CTF Rules which already exempts certain types of transactions relating to the over-the-counter derivatives markets relating to the wholesale price of electricity, gas or renewable certificates.

definition. The definition of 'primary photographic identification document' should also be amended to recognise identity documents which have unique identifiers such as biometric markers instead of signatures.

Certified copy definition

A document can be certified as a true copy of the original for the purposes of the AML/CTF regime by any person listed in the definition of certified copy under paragraph 1.2.1 of the AML/CTF Rules. A range of domestic persons are included, as well as persons who are authorised as a notary public in a foreign country.

Stakeholders suggested that the list of persons who can certify a document in foreign countries be expanded and aligned with the domestic list to better facilitate identifying customers who are not in Australia.

Listing the specific overseas equivalents for every foreign country would be impractical and overly prescriptive. A more practical approach would be to expand the list to include the foreign equivalent of those persons listed in the domestic list. This would enable reporting entities to use the risk-based approach to decide whether a foreign person is equivalent to the domestic list and receive certified copies of documents from a wider range of foreign counterparts. Such a change should be supplemented by guidance to assist reporting entities understand who may be a foreign equivalent.

Managed investment scheme

Companies that issue or sell interests in managed investment schemes (MIS) are providing a designated service under item 35 of table 1 of section 6 of the AML/CTF Act. An MIS is defined in paragraph 1.2.2 of the AML/CTF Rules to have the same meaning as within the Corporations Act. Industry considered that, due to its reliance on the definition used in the Corporations Act, the AML/CTF Rules definition of MIS is inappropriately broad.

One stakeholder considered that the definition is so broad that it could include any scheme which was in substance offered to the public as an investment. This means that AML/CTF compliance obligations would apply to schemes not considered by the FATF standards to be 'financial institution activities' and not intended to be covered under Australia's AML/CTF regime, such as the operation of class action lawsuits.

The stakeholder further noted that while the Corporations Act definition of an MIS is extremely broad, exemptions within the Corporations Act narrow the definition. However, these exemptions do not apply to the definition used within the AML/CTF Rules. For example, section 601ED(1) of the Corporations Act provides that an MIS is not required to be registered under that Act if the MIS has 20 or fewer members and has not been promoted by a person whose business is to promote MIS. While this MIS is not required to register with ASIC, it continues to meet the definition of an MIS within the AML/CTF Rules and so could attract AML/CTF compliance obligations as an item 35 designated service. The AML/CTF Rules do, however, serve to mitigate the impact of this issue by exempting certain types of MIS from being designated services under item 35.[404]

The definition of an MIS in the AML/CTF Rules should be redrafted so as to apply only to the types of MIS intended to be regulated under the AML/CTF Act. However, the definition should retain an underlying link to the definition used in the Corporations Act to ensure that new products and markets are able to be regulated under the AML/CTF Act.

[404] See Chapter 21 of the AML/CTF Rules.

The definition should be redrafted with consideration to any existing exemptions under the Corporations Act and AML/CTF Rules. The redrafting process would need to carefully consider whether incorporating any such exemptions into the redrafted MIS definition would increase or decrease the ML/TF risk.

Related to the entity providing the designated service

Chapter 36 provides that reporting entities do not have AML/CTF obligations when providing a designated service to a customer that is related to them. One of the ways a reporting entity is considered to be related to its customer is if the two entities are related bodies corporate under the Corporations Act.

One stakeholder considered that reliance on this definition is unduly limiting. The stakeholder recommended that the definition be extended to include relationships between any other entities that have real and tangible economic links, such as those between members of partnership or joint ventures, and between trustees and entities held with the trust structure.

Chapter 36 provides a reporting entity with a full exemption from AML/CTF obligations for designated services that it provides to bodies that are related to the entity. The exemption under Chapter 36 should only be extended to relationships that entail a sufficiently strong economic link between entities, and where the level of ML/TF risk associated with the relationship justifies such an exemption.

For example, joint venture and trust structures can be created and dissolved with relative ease and do not constitute a sufficiently real and tangible link between entities to justify extending the exemption to include these structures. There is a risk that these structures could be created deliberately to enable reporting entities to avoid AML/CTF obligations. By contrast, partnerships could have a sufficiently real and tangible economic link to merit their inclusion among the exemptions under Chapter 36, where justified by the level of ML/TF risk. A potential example is where both partners are bodies corporate.

Recommendations

Recommendation 19.1

The AML/CTF Act should be amended to:

(a) remove the list of accounts in the definition of 'account'

(b) replace the 'control test' in the AML/CTF Act with a test based on the FATF's beneficial owner definition

(c) replace the definitions of 'credit card' and 'debit card' with definitions identical to those in section 39 of Schedule 2 of the *Competition and Consumer Act 2010*

(d) combine the 'factoring' and 'forfaiting' designated services and clarify whether it includes different types of factoring, such as reverse factoring

(e) redraft the definition of 'loan' to clarify what is included within the definition

(f) redraft the definition of 'signatory' so that it more narrowly applies to persons with authority to authorise payment transactions and also include a power to make Rules to amend the definition, and

(g) redraft the definition of 'stored value card' to provide industry with greater guidance as to what a stored value card can include, while remaining broad, inclusive and sufficiently flexible to cover virtual cards.

Recommendation 19.2

The AML/CTF Rules should be amended to:

(a) limit the application of the AML/CTF Act definitions of 'derivative' and 'security' so that they only apply to schemes intended to be covered by the AML/CTF Act

(b) make the definitions of an 'original primary photographic identification document', an 'original primary non-photographic identification document', and an 'original secondary identification document' inclusive

(c) include national identity cards issued by foreign countries that include unique identifiers rather than signatures (such as biometric identifiers) in the definition of 'primary photographic identification document'

(d) expand the definition of 'certified copy' to include foreign equivalents to the domestic list

(e) redraft the definition of 'managed investment scheme' in the AML/CTF Rules so it applies only to schemes intended to be covered by the AML/CTF Act, and

(f) expand the circumstances in which a reporting entity is related to its customer in Chapter 36 of the AML/CTF Rules to include partnerships where justified by the ML/TF risk.

20. Table of recommendations

CHAPTER	NO.	RECOMMENDATION
Chapter 2: Overarching issues	2.1	The AML/CTF Act should be simplified to enable reporting entities to better understand and comply with their AML/CTF obligations.
	2.2	The AML/CTF Rules should be simplified, rationalised and presented in a user-friendly format to improve accessibility and understanding of obligations.
	2.3	The AML/CTF Act and Rules should adopt the technology neutrality principle.
	2.4	AUSTRAC should consider further opportunities to provide greater guidance and publish feedback on compliance outcomes and the value of financial intelligence.
	2.5	Reforms to the AML/CTF Act and Rules that have a regulatory impact should be co-designed by government and industry.
	2.6	A government working group should be established to consider international developments in combating terrorism financing and consider the appropriateness of these measures for the Australian context.
Chapter 3: Objects of the Act	3.1	The AML/CTF Act should be amended to include objects that relate to the following concepts: • implementing measures to detect, deter and disrupt money laundering, the financing of terrorism, the proliferation of weapons of mass destruction and its financing and other serious crimes • responding to the threat posed by money laundering, the financing of terrorism, the proliferation of weapons of mass destruction and its financing and other serious crimes by providing regulatory, national security and law enforcement officials with the information they need to detect, deter and disrupt these crimes • supervision and monitoring of compliance by reporting entities with Australian sanction laws (subject to consideration in Chapter 15 of this report), and • promoting public confidence in the Australian financial system.

CHAPTER	NO.	RECOMMENDATION
	3.2	The AML/CTF Act should be amended to insert general principles for the administration of the Act that provide for the following: • AML/CTF obligations under the AML/CTF Act, Rules and Regulations should be proportionate to the ML/TF risks faced by reporting entities • regulatory, national security and law enforcement agencies should have access to the information they need to detect, deter and disrupt money laundering, the financing of terrorism, the proliferation of weapons of mass destruction and its financing, contraventions of Australian sanction laws and other serious crimes (subject to consideration in Chapter 15 of this report), and • AML/CTF obligations under the AML/CTF Act, Rules and Regulations should be designed and implemented in a way that minimises and appropriately addresses the privacy risks and impacts associated with the handling of personal information.
Chapter 4.1 : Regime scope: Existing designated services	4.1	The AML/CTF Act should be amended to delete the following from table 1 of section 6: • Item 51 (collecting physical currency, or holding physical currency from or on behalf of a person), and • Item 53 (delivering physical currency to a person).
	4.2	AUSTRAC should conduct an assessment of the ML/TF risks posed by the issuing, selling and cashing/redeeming of traveller's cheques and whether these services should continue to be regulated under Australia's AML/CTF regime.
	4.3	AUSTRAC should conduct an assessment of the ML/TF risks posed by stored value cards and the continued appropriateness of the thresholds in the stored value card designated services.
	4.4	AUSTRAC should conduct an assessment of the ML/TF risks posed by the services provided by cheque cashing facilities with a view to regulating these services under the AML/CTF Act if they are determined to pose a high ML/TF risk.
	4.5	The use of the term 'in the course of carrying on a business' should be qualified for the activities currently within tables 2 and 3 of section 6 of the AML/CTF Act to ensure that only activities routinely or regularly provided by a reporting entity are captured under AML/CTF regulation.
Chapter 4.2: Regime scope: Designated non-financial businesses and professions	4.6	The Attorney-General's Department and AUSTRAC, in consultation with industry, should: (a) develop options for regulating lawyers, conveyancers, accountants, high-value dealers, real estate agents and trust and company service providers under the AML/CTF Act, and (b) conduct a cost-benefit analysis of the regulatory options for regulating lawyers, accountants, high-value dealers, real estate agents and trust and company service providers under the AML/CTF Act.
Chapter 4.3: Regime scope: Payment types and systems	4.7	AUSTRAC should closely monitor the ML/TF risks associated with new payment types and systems (including front-end applications), to ensure gaps do not develop in Australia's AML/CTF regime.

CHAPTER	NO.	RECOMMENDATION
	4.8	The AML/CTF Act should be amended to ensure that digital wallets are comprehensively captured by AML/CTF regulation.
	4.9	The AML/CTF Act should be amended to expand the definition of e-currency to include convertible digital currencies not backed by a physical 'thing'.
	4.10	The AML/CTF Act should be amended to regulate activities relating to convertible digital currency, particularly activities undertaken by digital currency exchange providers.
Chapter 4.4 : Regime scope: Offshore service providers of designated services	4.11	AUSTRAC should identify designated services that pose a high ML/TF risk when provided to an Australian customer by an offshore-based business.
	4.12	The Attorney-General's Department, in partnership with AUSTRAC, should develop an appropriate model for applying AML/CTF obligations under the AML/CTF Act to high-risk designated services provided by offshore service providers.
	4.13	AUSTRAC should monitor the ML/TF risks posed by designated services offered by offshore service providers that fall outside the scope of Australia's AML/CTF regime.
Chapter 5: Customer due diligence	5.1	The AML/CTF Act should be simplified to explicitly require reporting entities to implement the core customer due diligence obligations.
	5.2	The AML/CTF Rules for customer due diligence should be rationalised and simplified as a priority, using plain language to facilitate ease of use and supplemented by enhanced guidance.
	5.3	AUSTRAC should consider and explore other reliable options, including those utilising new technologies, as alternatives to the existing minimum know your customer requirements for individual customers.
	5.4	The safe harbour and simplified verification procedures under the AML/CTF Rules should be rationalised into a single simplified customer due diligence procedure.
	5.5	AUSTRAC should consider expanding the availability of simplified customer due diligence to designated services and customers that have a minimal or low ML/TF risk.
	5.6	The AML/CTF Rules should explicitly allow for use of self-attestation to identify individual customers using a risk-based approach only as a measure of last resort where a customer's identity cannot otherwise be reasonably obtained or verified.
	5.7	The AML/CTF Rules should allow reporting entities to accept disclosure certificates certified by an acceptable officer using a risk-based approach.
	5.8	AUSTRAC and industry representatives should develop guidance to assist reporting entities to conduct customer due diligence on customers that may experience difficulty accessing services provided by reporting entities because they are unable to comply with the more conventional methods for proving identity.

CHAPTER	NO.	RECOMMENDATION
	5.9	The AML/CTF Act should be amended to explicitly prohibit reporting entities from providing a regulated service if the applicable customer identification procedure cannot be carried out and require reporting entities to consider making a suspicious matter report in such situations.
	5.10	AUSTRAC should conduct an ML/TF risk assessment on whether the customer due diligence threshold for casinos and other gaming providers should change.
	5.11	The AML/CTF Rules should be amended to require reporting entities to conduct specific enhanced customer due diligence measures (in line with the FATF standards) at the time of pay out where the beneficiary or beneficial owner of a life insurance policy is a politically exposed person and a higher ML/TF risk is identified.
	5.12	The AML/CTF Act should be amended to expand the ability of reporting entities to rely on customer identification procedures performed by a third party, subject to the following conditions: (a) where the third party agrees to being relied on, the relying business remains ultimately responsible for customer due diligence measures, and (b) where the third party is outside of Australia, the third party is subject to appropriate regulation and similar customer identification requirements as are applicable in Australia.
	5.13	AUSTRAC should permit access to the Reporting Entities Roll, subject to appropriate privacy restrictions, in a similar manner to the Remittance Sector Register.
Chapter 6: Reporting obligations	6.1	AUSTRAC to conduct an assessment on the viability and impacts of changes to the IFTI reporting regime to: (c) provide exemptions for IFTIs below a certain threshold, relating to specific low ML/TF risk designated services (d) expand IFTI reporting requirements to include the reporting of transactions undertaken using credit/debit cards, and (e) expand the scope of information reported to AUSTRAC. .
	6.2	AUSTRAC should assess the ML/TF risks associated with international transactions that involve the withdrawal of cash from ATMs located in Australia using foreign issued cards.
	6.3	The AML/CTF Act should be amended to better align the electronic funds transfer instructions requirements with the FATF standards for wire transfers.

CHAPTER	NO.	RECOMMENDATION
	6.4	The AML/CTF Act and Rules should be amended to simplify and streamline transaction reporting obligations and produce regulatory efficiencies. This process should include: (a) consideration of extending the funds transfer chain definition to providers of designated remittance arrangements (b) reviewing the value of requiring transaction reports to be submitted by two entities involved in the one transaction, and (c) allowing threshold transaction reports and international funds transfer instructions to be submitted as one report when they relate to the same transaction.
	6.5	Changes to reporting requirements should occur concurrently with the proposed changes arising from AUSTRAC's Foreign Fighters Initiative.
	6.6	AUSTRAC and the Attorney-General's Department should closely monitor the progress of the New Payments Platform and continue to engage with its primary participants.
Chapter 7: AML/CTF programs	7.1	The AML/CTF Act and Rules should be amended to merge and streamline the Part A and Part B requirements for AML/CTF programs into a single requirement for reporting entities to develop, implement and maintain an AML/CTF program that is effective in identifying, mitigating and managing their ML/TF risks.
	7.2	The AML/CTF Act should be amended to impose an obligation on reporting entities to report serious breaches of AML/CTF obligations to AUSTRAC in a timely manner. These amendments should also allow for any pecuniary penalty that may apply to a self-reported breach to be reduced or waived, where appropriate, and be accompanied by AUSTRAC guidance.
	7.3	The AML/CTF Rules should be amended to: (a) require reporting entities to incorporate information provided by AUSTRAC or other relevant authorities on high ML/TF risks into their risk assessments (b) incorporate information provided by AUSTRAC or other relevant authorities on high ML/TF risks into their risk assessments (c) describe the roles and functions of an AML/CTF compliance officer and associated AML/CTF compliance arrangements (d) guarantee the independence of the reviewer of AML/CTF programs, and (e) require reporting entities to identify, mitigate and manage the ML/TF risks posed by new technologies.
	7.4	AUSTRAC should develop guidance to assist reporting entities to: (a) assess their ML/TF risks and develop AML/CTF programs, and (b) determine how often independent reviews of their AML/CTF programs should be conducted.
	7.5	The AML/CTF Act and Rules should be amended to replace the designated business group and joint AML/CTF program construct with a framework that allows an AML/CTF program to incorporate all reporting entities within a corporate group.

CHAPTER	NO.	RECOMMENDATION
	7.6	The AML/CTF Act and Rules should be amended to require reporting entities to: (a) apply AML/CTF measures to its foreign branches and subsidiaries that are consistent with requirements under the AML/CTF Act where the AML/CTF measures in the other country are less strict than Australia's, and (b) inform AUSTRAC where the foreign host country of foreign branches and subsidiaries does not permit the proper implementation of these AML/CTF measures.
	7.7	The AML/CTF Rules should be amended to require reporting entities that operate branches or subsidiaries located in foreign countries to have the AML/CTF programs for these branches or subsidiaries reviewed by an independent auditor when required by AUSTRAC. The reporting entity should also be required to provide the audit report to AUSTRAC.
Chapter 8: Record-keeping	8.1	The AML/CTF Act should be amended to establish an explicit requirement that sufficient transaction records must be made and kept by reporting entities to enable reconstruction of individual transactions.
	8.2	The AML/CTF Rules should be amended to establish an obligation that reporting entities maintain their AML/CTF records in a format that allows the records to be provided to AUSTRAC and partner agencies swiftly.
	8.3	AUSTRAC should develop guidance to assist reporting entities to understand what records they should keep.
Chapter 9: AML/CTF compliance reports	9.1	AUSTRAC should develop, in consultation with industry, a new compliance reporting process that is relevant to the information needs of AUSTRAC and reduces unnecessary regulatory burden.
Chapter 10: Correspondent banking	10.1	The AML/CTF Act and Rules should be amended to simplify and streamline the correspondent banking obligations commensurate with the FATF standards and establish a one-step process for conducting due diligence assessments on respondent financial institutions that is consistent with the FATF standards.
	10.2	The AML/CTF Rules should be amended to require financial institutions to consider the quality of ML/TF supervision conducted in the country of the respondent institution as part of the due diligence assessment.
	10.3	The AML/CTF Act should be amended to: (a) broaden the definition of correspondent banking in line with international approaches and consistent with the FATF standards (b) require financial institutions to undertake specific due diligence in relation to payable-through accounts consistent with the FATF standards, and (c) prohibit financial institutions from entering into a corresponding banking relationship with an institution that is able to enter into a correspondent banking relationship with a shell bank.

CHAPTER	NO.	RECOMMENDATION
Chapter 11: Remittance sector	11.1	A government-industry working group should be established to develop options for strengthening regulatory oversight of remitters, including consideration of the existing enforcement power and penalty regimes, under the AML/CTF Act.
	11.2	The definition of a designated remittance arrangement in the AML/CTF Act should be amended to ensure that non-remittance businesses are not unintentionally regulated as remitters under the AML/CTF Act.
	11.3	The AML/CTF Act and Rules should be amended to explicitly require remittance network providers to monitor their affiliates' compliance and report to AUSTRAC on breaches and remedial action as required.
	11.4	The AUSTRAC CEO should be allowed to: (a) deregister remitters that are not conducting remittance activities (as evidenced by a lack of reporting or other relevant activity) (b) ban individuals from involvement in the management or business of a remitter based on a demonstrated lack of suitability, fitness or propriety, and (c) publish refusals and notices detailing the circumstance of a cancellation of the registration of a remitter.
Chapter 12: Cross-border movement of physical currency and bearer negotiable instruments	12.1	The current cross-border reporting regime for physical currency and BNIs in the AML/CTF Act should be replaced with a consolidated requirement to report 'cash' of AUD10,000 or more. For the purposes of Part 4 of the AML/CTF Act, cash should be defined as: • physical currency • bearer negotiable instruments (see Recommendation 12.2) • bullion, and • an object or instrument specified in the AML/CTF Rules.
	12.2	The current definition of a bearer negotiable instrument under the AML/CTF Act should be amended to include: • gaming chips or tokens • plaques or letters of credit, and • an object or instrument specified in the AML/CTF Rules.
	12.3	The Attorney-General's Department, AUSTRAC and the Department of Immigration and Border Protection should investigate the feasibility of establishing cross-border reporting obligations in relation to stored value cards.
	12.4	The powers under sections 199 and 200 of the AML/CTF Act should be broadened to allow police and customs officers to search and seize 'cash' where there is: • a suspicion of money laundering, terrorism financing or other serious criminal offences, or • where there has been a breach of the cross-border reporting requirements under the AML/CTF Act.
	12.5	The AML/CTF Act should be amended to increase the civil penalty available for failing to comply with the cross-border 'cash' reporting requirement in line with international standards.

CHAPTER	NO.	RECOMMENDATION
	12.6	Sections 199 and 200 of the AML/CTF Act should be amended to provide for a civil penalty for a breach of these provisions.
	12.7	The AML/CTF Act should be amended to allow the definition of 'eligible place' to be expanded to include other designated areas (for the purposes of the AML/CTF Act) by way of regulation.
Chapter 13: Countermeasures		No recommendations.
Chapter 14: Secrecy and access	14.1	The Attorney-General's Department, in partnership with AUSTRAC and in consultation with other government agencies, should develop a simplified model for sharing information collected under the AML/CTF Act that is: • responsive to the information needs of agencies tasked with combating ML/TF and other serious crimes • supports collaborative approaches to combating ML/TF and other serious crime at the national and international level, and • establishes appropriate safeguards and controls that are readily understood and consistently applied.
	14.2	Subject to appropriate controls and safeguards, the AML/CTF Act should be amended to permit reporting entities to disclose suspicious matter report-related information to foreign parent entities and external auditors.
Chapter 15: Audit, information-gathering and enforcement	15.1	AUSTRAC and the Attorney-General's Department should explore options for expanding AUSTRAC's compliance testing tools in consultation with industry and government stakeholders.
	15.2	The AML/CTF Act should be amended to adopt the model regulatory powers set out in the *Regulatory Powers (Standard Provisions) Act 2014*, while maintaining the existing powers in the AML/CTF Act relating to remedial directions, external audits, ML/TF risk assessments and statutory notices.
	15.3	The AML/CTF Act should be amended to expand the remedial directions power to allow AUSTRAC to direct reporting entities to remedy past contraventions of AML/CTF reporting obligations.
	15.4	The AML/CTF Act should be amended to expand the infringement notice provisions under subsection 184(1A) to include a wider range of minor offences established under the AML/CTF Act that are regulatory in nature.
	15.5	The AML/CTF Act should be amended to give agencies that already have the power to issue notices to a person or reporting entity under sections 49 and 50 of the AML/CTF Act an additional power to issue infringement notices or apply for civil penalties if that person or entity fails to comply with such a notice.
	15.6	AUSTRAC should create template section 49 and 50 notices for use by all relevant agencies.
	15.7	The AML/CTF Act should be amended to clarify that sanctions for breaches of the AML/CTF Act or Rules by reporting entities can also apply to senior managers and directors in appropriate circumstances.

CHAPTER	NO.	RECOMMENDATION
	15.8	AUSTRAC and the Department of Foreign Affairs and Trade should explore the feasibility of AUSTRAC monitoring and supervising compliance with Australian sanction laws.
Chapter 16: Administration of the Act	16.1	The AML/CTF Act should be amended to: (a) give the AUSTRAC CEO the power to do all things necessary or convenient to be done for, or in connection with, the performance of his or her duties, and (b) expand the scope of the functions of the AUSTRAC CEO to include: • retaining, compiling and analysing AUSTRAC information • facilitating access to, and the sharing of, AUSTRAC information to support domestic and international efforts to combat money laundering, terrorism financing and other serious crimes, and • disseminating AUSTRAC information, where appropriate, to support government policy-making, industry education, public education and academic research.
Chapter 17: Exemptions process	17.1	The AML/CTF Act should be amended to set out the specific matters that the AUSTRAC CEO must take into account when determining exemptions, with the level of ML/TF risk posed being the prime consideration.
	17.2	AUSTRAC should adopt a more proactive approach to identifying opportunities to reduce unnecessary regulatory burden where the designated service, or the circumstances in which the designated service is provided, poses a low ML/ TF risk.
	17.3	AUSTRAC should, in consultation with industry, simplify and streamline the application process for reporting entities seeking exemptions from AML/CTF obligations and develop guidance to assist reporting entities to navigate the new process.
	17.4	AUSTRAC should amend its *Exemption Policy* to specify: • time frames for AUSTRAC to determine exemption applications, and • time frames for reviewing the continued appropriateness of exemptions granted.
Chapter 18: Financial Transactions Reports Act 1988	18.1	Repeal the FTR Act and Regulations and amend the AML/CTF Act and Rules to: (a) retain reporting requirements in relation to traveller's cheques, motor vehicle dealers and solicitors while the broader consideration of AML/CTF Act regulation of these businesses occurs, and (b) address any transitional issues resulting from the repeal of the FTR Act and Regulations.
	18.2	In the repeal of the FTR Act, insurance intermediaries and general insurance providers - apart from motor vehicle dealers - should not retain their reporting obligations.

CHAPTER	NO.	RECOMMENDATION
Chapter 19: Definitional issues	19.1	The AML/CTF Act should be amended to: (a) remove the list of accounts in the definition of 'account' (b) replace the 'control test' in the AML/CTF Act with a test based on the FATF's beneficial owner definition (c) replace the definitions of 'credit card' and 'debit card' with definitions identical to those in section 39 of Schedule 2 of the *Competition and Consumer Act 2010* (d) combine the 'factoring' and 'forfaiting' designated services and clarify whether it includes different types of factoring, such as reverse factoring (e) redraft the definition of 'loan' to clarify what is included within the definition (f) redraft the definition of 'signatory' so that it more narrowly applies to persons with authority to authorise payment transactions and also include a power to make Rules to amend the definition, and (g) redraft the definition of 'stored value card' to provide industry with greater guidance as to what a stored value card can include, while remaining broad, inclusive and sufficiently flexible to cover virtual cards.
	19.2	The AML/CTF Rules should be amended to: (a) limit the application of the AML/CTF Act definitions of 'derivative' and 'security' so that they only apply to schemes intended to be covered by the AML/CTF Act (b) make the definitions of an 'original primary photographic identification document', an 'original primary non-photographic identification document', and an 'original secondary identification document' inclusive (c) include national identity cards issued by foreign countries that include unique identifiers rather than signatures (such as biometric identifiers) in the definition of 'primary photographic identification document' (d) expand the definition of 'certified copy' to include foreign equivalents to the domestic list (e) redraft the definition of 'managed investment scheme' in the AML/CTF Rules so it applies only to schemes intended to be covered by the AML/CTF Act, and (f) expand the circumstances in which a reporting entity is related to its customer in Chapter 36 of the AML/CTF Rules to include partnerships where justified by the ML/TF risk.

21. Glossary

ABN	Australian Business Number
ACC	Australian Crime Commission
ACIP	Applicable customer identification procedure
ACLEI	Australian Commission for Law Enforcement Integrity
ACR	Annual compliance report
ADI	Authorised deposit-taking institution
AFP	Australian Federal Police
ALRC	Australian Law Reform Commission
AML/CTF	Anti-money laundering and counter-terrorism financing
AML/CTF Act	*Anti-Money Laundering and Counter-Terrorism Financing Act 2006*
AML/CTF Regulations	*Anti-Money Laundering and Counter-Terrorism Financing (Prescribed Foreign Countries) Regulation 2016*
AML/CTF Rules	*Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)*
App	Front-end application
APRA	Australian Prudential Regulation Authority
ASIC	Australian Securities & Investments Commission
ATO	Australian Taxation Office
AUD	Australian dollar
AUSTRAC	Australian Transaction Reports and Analysis Centre
BNI	Bearer negotiable instrument
CAD	Canadian dollar
CBM-BNI	Cross-border movement of bearer negotiable instrument report
CBM-PC	Cross-border movement of physical currency report
CDD	Customer due diligence
CIT	Cash-in-transit
CTR Act	*Cash Transaction Reports Act 1988*
DBG	Designated business group
Designated service	A service listed in section 6 of the AML/CTF Act
DFAT	Department of Foreign Affairs and Trade
DNFBP	Designated non-financial business or profession
DVS	Document Verification Service
DPRK	Democratic People's Republic of Korea (North Korea)
EFTI	Electronic funds transfer instruction
FATF	Financial Action Task Force
FinCEN	Financial Crime Enforcement Network (United States of America)

FOI Act	*Freedom of Information Act 1982*
FTR Act	*Financial Transaction Reports Act 1988*
GBP	British pound
EUR	Euro
FIU	Financial intelligence unit
IFTI	International funds transfer instruction
ISIL	Islamic State in Iraq and the Levant
LCA	Law Council of Australia
KYC	Know your customer
MER	Mutual evaluation report
ML/TF	Money laundering and terrorism financing
NPP	New Payments Platform
NZD	New Zealand Dollar
PEP	Politically exposed person
Reporting entity	A person or business which provides a designated service
RNP	Remittance network provider
RSR	Remittance sector register
SCTR	Significant cash transaction report
SGD	Singapore dollar
SMR	Suspicious matter report
SRA	Solicitor Regulation Authority (United Kingdom)
SUSTR	Suspicious transaction report
SVC	Stored value card
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TCSP	Trust and company service provider
TFS	Targeted financial sanctions
TTR	Threshold transaction report
UNSCR	United Nations Security Council Resolution
USD	United States dollar
WMD	Weapons of mass destruction

22. Appendices

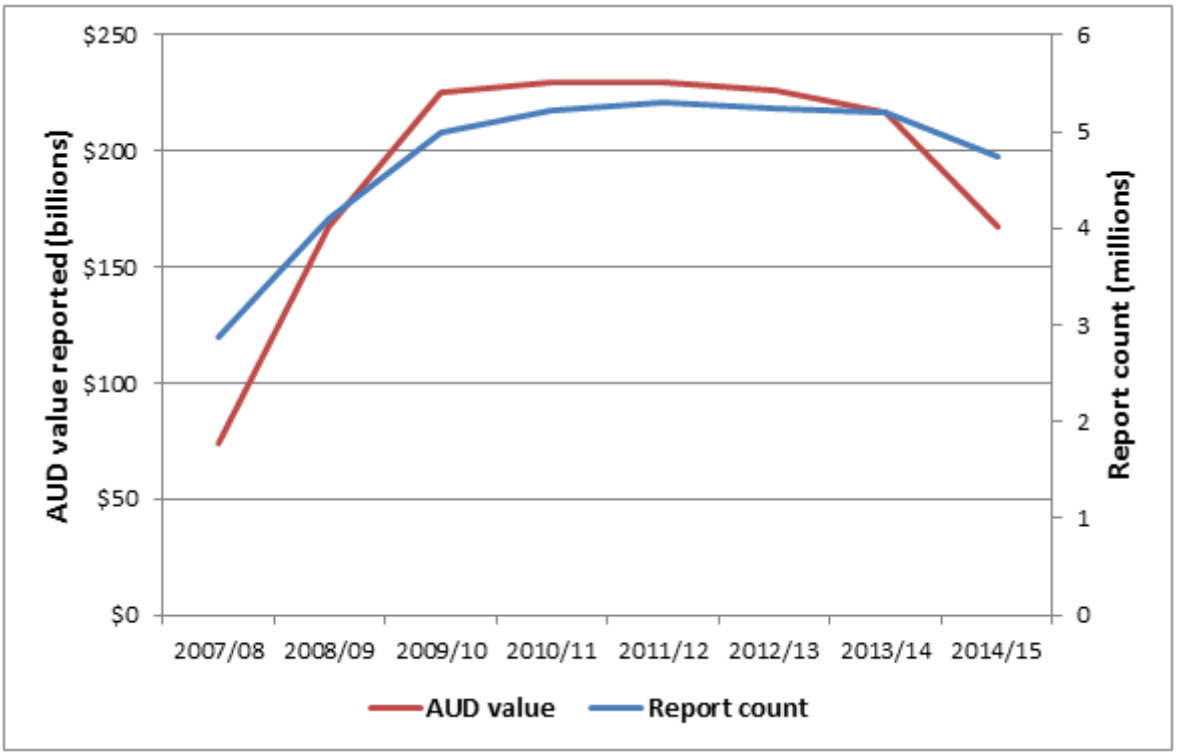
Appendix 1 – Industry and partner agency consultation meetings

Meeting	Participants
19 September 2014	
Non-government organisations	Uniting Church in Australia, Synod of Victoria and Tasmania, Transparency International Australia, Australian Council for International Development, OXFAM
24 September 2014	
Gaming sector: Gaming machines	Australian Hotels Association, ClubsNSW, Mercury Group Victoria Inc, ALH Group Pty Ltd
Gaming sector: Casinos	Casinos and Resorts Australasia
Gaming sector: Wagering	Australian Wagering Council, Australian Bookmakers Association Limited, TattsGroup
Cash-in-transit sector	Australian Security Industry Association Limited, Linfox Armaguard, Prosegur
25 September 2014	
Remittance sector	Western Union
Remittance sector	UAE Exchange, Hai Ha, MoneyGram, EZ Money, OzForex Group, RIA
26 September 2014	
AML compliance	AML Master
2 October 2014	
AML compliance	Yarra Valley Associates
19 November 2014	
Banking/finance sector: Australian Financial Markets Association	Australian Financial Markets Association, Western Union, Bank of America Merrill Lynch, Westpac, Morgan Stanley, ANZ, NAB, UBS, AMP
Banking/finance sector: Financial Services Council	Financial Services Council, BT Financial Group, HWL Ebsworth, K&L Gates, Schroders, Perpetual, Commonwealth Bank of Australia, Minter Ellison Lawyers, Bell Asset Management, Vanguard, KPMG
Banking/finance sector: Customer Owned Banking Association	Customer Owned Banking Association, Teachers Mutual Bank, Maritime, Mining & Power Credit Union, Heritage Bank, CUA, Community First Credit Union, Greater Building Society, The University Credit Society, People's Choice Credit Union, Bankmecu, Beyond Bank, Victoria Teachers Mutual Bank
25 November 2014	
Banking/finance sector: Australian Finance Conference	Australian Finance Conference, Toyota Finance Australia Limited, Pepper Group, Marubeni Equipment Finance
Banking/finance sector: Australian Bankers' Association	Australian Bankers' Association, Commonwealth Bank of Australia, Macquarie, Westpac, ANZ, ING Direct, HSBC
17 December 2014	
New payment methods	PayPal

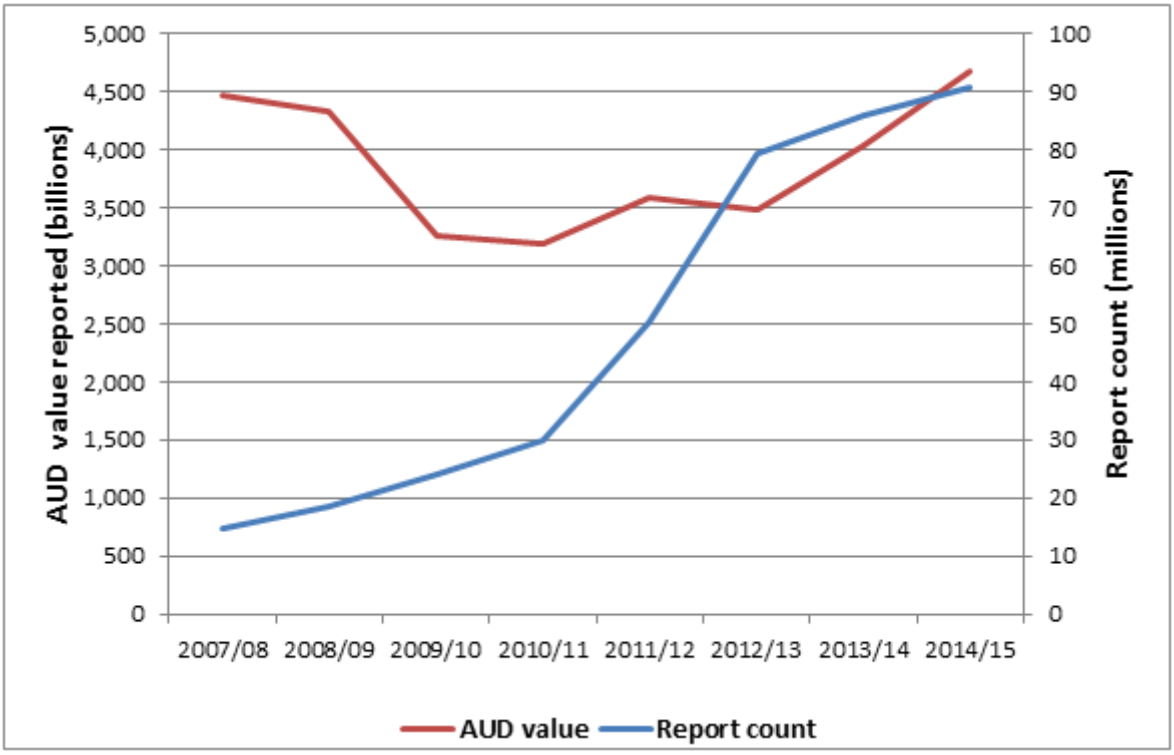
Meeting	Participants
28 January 2015	
Government agencies	Australian Crime Commission, Australian Federal Police, Attorney-General's Department, Australian Security and Intelligence Organisation, Australian Taxation Office, Australian Transaction Reports and Analysis Centre, Department of Foreign Affairs and Trade, Department of Human Services, Department of Immigration and Border Protection, Australian Customs and Border Protection Service, Inspector-General of Intelligence and Security, Office of the Australian Information Commissioner, Treasury, New South Wales Crime Commission
24 March 2015	
Remittance sector	Australian Remittance and Currency Providers Association
Legal sector	Financial Services Committee, Law Council of Australia
AML compliance	GRC Institute
New payment methods	PayPal
8 May 2015	
Superannuation	Australian Institute of Superannuation Trustees
Privacy	Australian Privacy Foundation

Appendix 2 – Financial intelligence data

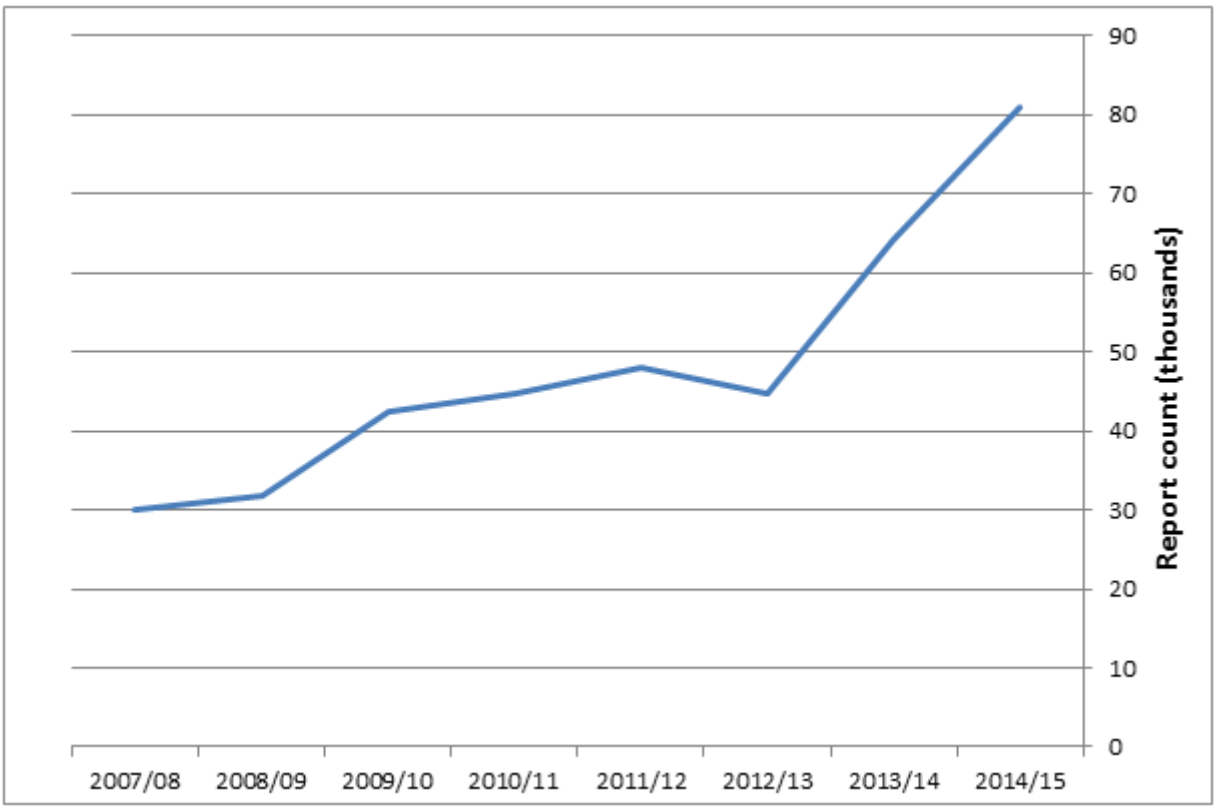
GRAPH 1: VOLUME AND VALUE OF REPORTING FROM JULY 2007 TO JUNE 2015 – TTR AND SCTR



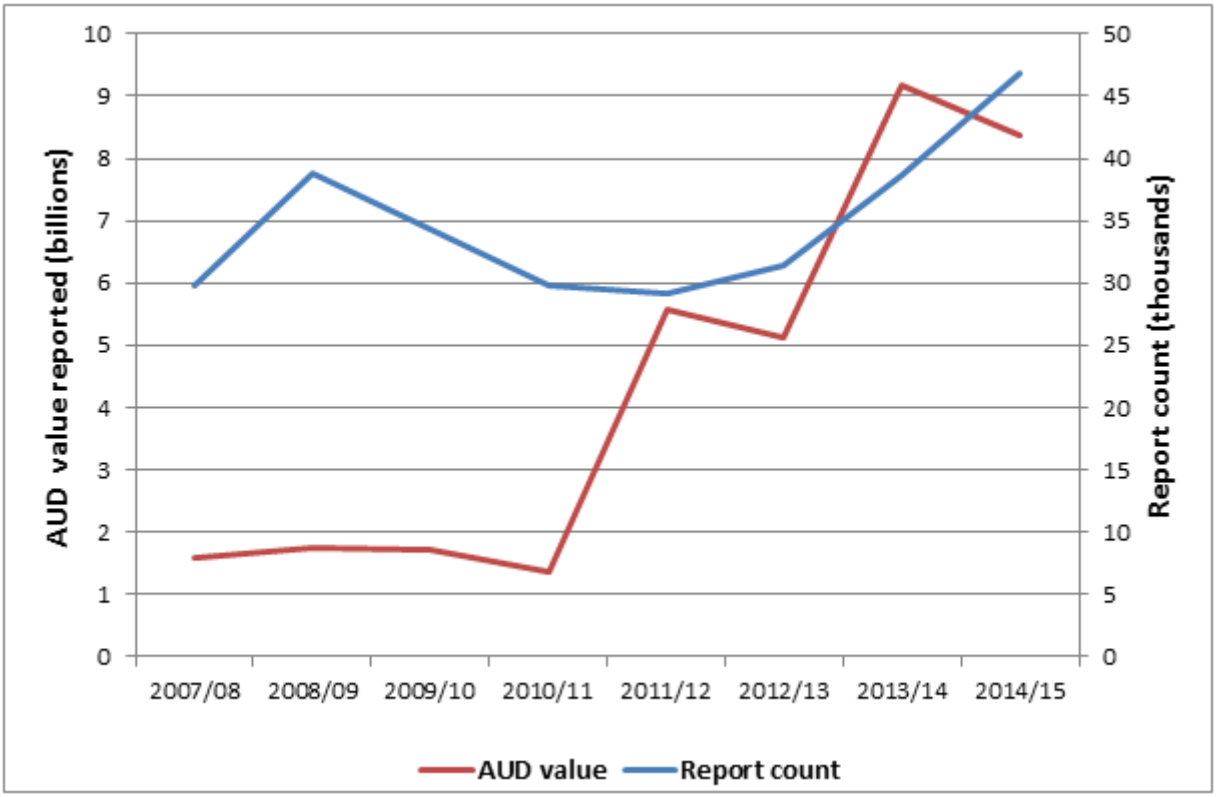
GRAPH 2: VOLUME AND VALUE OF REPORTING FROM JULY 2007 TO JUNE 2015 – IFTI



GRAPH 3: VOLUME OF REPORTING FROM JULY 2007 TO JUNE 2015 – SMR AND SUSTR



GRAPH 4: VOLUME AND VALUE OF REPORTING FROM JULY 2007 TO JUNE 2015 – CBM-PC



GRAPH 5: VOLUME AND VALUE OF REPORTING FROM JULY 2007 TO JUNE 2015 – CBM-BNI