Parliamentary Joint Committee on Law Enforcement

Inquiry into financial related crime

September 2015

ISBN 978-1-76010-289-0

This document was printed by the Senate Printing Unit, Parliament House, Canberra

The Committee

Members

Mr Craig Kelly MP	LP, NSW (Chair) (from 4.3.15)
Senator the Hon Lisa Singh	ALP, TAS (Deputy Chair)
Senator Sean Edwards	LP, SA
Mr Chris Hayes MP	ALP, NSW (from 16.7.14)
Senator Chris Ketter	ALP, QLD (from 1.7.14)
Senator David Leyonhjelm	LDP, NSW (from 25.11.14)
Mr Russell Matheson MP	LP, NSW
Senator Barry O'Sullivan	NATS, QLD (from 1.7.14)
Ms Maria Vamvakinou MP	ALP, VIC
Mr Jason Wood MP	LP, VIC

Former Members

The Hon Justine Elliot MP (ALP, NSW) (from 5.12.13 to 16.7.14)
Senator Mark Furner (ALP, QLD) (from 12.11.13 to 30.6.14)
Senator the Hon Stephen Parry (LP, TAS) (from 2.12.13 to 30.6.14)
Mr Bert van Manen MP (LP, QLD) (from 10.12.13 to 4.3.15)

Secretariat

Mr Stephen Palethorpe, Secretary
Ms Jedidiah Reardon, Acting Principal Research Officer
Mr Josh See, Senior Research Officer
Ms Rosalind McMahon, Administrative Officer

PO Box 6100
Parliament House
CANBERRA ACT 2600
Telephone: (02) 6277 3419
Facsimile: (02) 6277 5809
Email: le.committee@aph.gov.au
Internet: www.aph.gov.au/le_ctte

Table of Contents

Abbreviations

ABA	Australian Banker's Association
ABS	Australian Bureau of Statistics
ACBPS	Australian Customs and Border Protection Service
ACC	Australian Crime Commission
ACCC	Australian Competition and Consumer Commission
ACORN	Australian Cybercrime Online Reporting Network
ACLEI	Australian Commission for Law Enforcement Integrity
AFP	Australian Federal Police
AFS	Australian Financial Service
AGD	Attorney-General's Department
AGS	Australian Government Solicitor
AIC	Australian Institute of Criminology
AML/CTF	*Anti-money laundering and Counter-Terrorism Financing Act 2006*
ARS	Alternative Remittance Sector
ASIC	Australian Securities and Investments Commission
ATO	Australian Taxation Office
AUSTRAC	Australian Transaction Reports and Analysis Centre
CCA	*Competition and Consumer Act 2010*
CDPP	Commonwealth Director of Public Prosecutions
CEO	Chief Executive Officer
CoAG	Council of Australian Governments
DNFBPs	Designated non-financial businesses and professions
DVS	Document Verification System
FATF	Financial Action Task Force
HOCOLEA	Heads of Commonwealth Operational Law Enforcement Agencies
IMF	International Monetary Fund

IVTS	Informal Value Transfer Systems
NAAJA	Northern Territory Australian Aboriginal Justice Agency
NCPA	National Credit Providers Association
NCCP Act	*National Consumer Credit Protection Act 2009*
NCLRC	National Criminal Law Reform Commission
NIITF	National Indigenous Intelligence Taskforce
NISS	National Identity Security Strategy
NJCEOs	National Justice CEOs forum
NT Police	Northern Territory Police
PJCIS	Parliamentary Joint Committee on Intelligence and Security
RBA	Reserve Bank of Australia
SAPOL	South Australia Police
SCAG	Standing Committee of Attorneys-General
SCLJ	Standing Council on Law and Justice
SMSF	Self-managed superannuation
the committee	Parliamentary Joint Committee on Law Enforcement
TIA Act	*Telecommunications (Interception and Access) Act 1979*
UNODC	United Nations Office on Drugs and Crime

Recommendations

Recommendation 1

2.47 The committee recommends that the government review the operations and outcomes of each law enforcement taskforce approximately 12 months prior to its conclusion in order to determine whether it should be made an ongoing taskforce.

Recommendation 2

2.55 The committee recommends that the government introduce amendments to the *Crimes (Currency) Act 1981* to give the RBA administrative responsibilities and the AFP law enforcement responsibilities with respect to counterfeit note collections and investigations.

Recommendation 3

3.34 The committee recommends that subject to appropriate safeguards including adequate privacy and oversight arrangements, the government designate the ATO as a 'criminal law-enforcement agency' under the *Telecommunications (Interception and Access) Act 1979*, for the purpose of protecting public finances from serious criminal activities such as major tax fraud.

Recommendation 4

3.59 The committee recommends the Government consider the extension of the AML/CTF regulations to cover 'second tier' professions in the current *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* review.

Recommendation 5

3.67 The committee recommends the government introduce amendments to the *Australian Crime Commission Act 2002* to enable AUSTRAC to become a full member of the ACC Board.

Recommendation 6

4.16 The committee recommends that the government review the penalties prescribed under financial services legislation administered by ASIC, with a view to achieving a better balance between non-compliance by licensed operators and unlicensed operations.

Recommendation 7

4.22 The committee recommends that ASIC consider and then implement mechanisms to make its response to internet-based financial related crimes far more expeditious.

Recommendation 8

4.27 The committee recommends that the Australian National Audit Office conduct a performance audit of ASIC's technological capacity, and provide a report to the Parliament outlining ASIC's technological requirements and capabilities, and the extent to which any deficiencies may hamper ASIC's regulatory responsibilities.

Recommendation 9

4.29 The committee recommends that ASIC strive to improve its relationships with the private sector in order to better detect and deter financial related crimes.

Recommendation 10

4.45 The committee recommends that AUSTRAC consider and then implement mechanisms to increase its regulatory oversight of the activities of unregistered remitters.

Recommendation 11

6.53 The committee recommends the Attorney-General's Department review the arrangements for victims of identity crime to obtain a Commonwealth victim certificate.

Recommendation 12

6.64 The committee recommends that financial institutions which issue debit and credit cards create an 'opt in' function that requires customers to consent to contactless payment technology features being activated on their cards.

Recommendation 13

7.46 The committee recommends the government fund targeted financial literacy education programs for Indigenous communities. These programs must be translated into local Indigenous languages, be specific to the local community circumstances and be delivered in a culturally appropriate manner.

Recommendation 14

7.63 The committee recommends the government implement the recommendations from the National Indigenous Intelligence Task Force report relating to the prevention of financial crime and improved governance in Indigenous organisations.

Chapter 1

Background and terms of reference

1.1 On 5 March 2014, the Parliamentary Joint Committee on Law Enforcement (the committee) initiated an inquiry into financial related crime, pursuant to paragraph 7(1)(g) of the *Parliamentary Joint Committee on Law Enforcement Act 2010*.

1.2 The terms of reference required the committee to examine the effectiveness of current Commonwealth law enforcement legislation and administrative arrangements that target serious and organised financial related crime, including money laundering and identity fraud:

(1) The character, prevalence and impact of financial related crime in Australia;

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

(3) The involvement of organised crime;

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

(5) In relation to identity fraud—credit card fraud in particular;

(6) The operation and effectiveness of Commonwealth legislation, administrative arrangements and law enforcement strategies;

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

(8) The interaction of Commonwealth, state and territory legislation and law enforcement activity;

(9) The extent and effectiveness of relevant international agreements and arrangements;

(10) The need for any legislative or administrative reform; and

(11) Any related matters.

Report structure

1.3 Following this introductory chapter, this report is divided into six substantive chapters.

1.4 Chapter 2 broadly examines issues relating to the use of Commonwealth law enforcement agency powers and taskforces in addressing financial related crime. In particular two of these taskforces, *Wickenby* and *Eligo*, are assessed not only in terms of their overall effectiveness, but also whether they demonstrate a need for any changes to the longevity of Commonwealth law enforcement taskforces. Chapter 2 also examines the recent announcement of the Serious Financial Crime Taskforce, and commentary relating to Momcilovic v The Queen [2011] HCA 34 (*Momcilovic*).

1.5 Chapter 3 discusses several issues surrounding telecommunications interception powers and financial related crime. Specifically, it examines the

proposition that the Australian Taxation Office (ATO) and the Australian Securities and Investments Commission (ASIC) ought to be granted telecommunications interception powers, outside of multi-agency taskforces. Further, it examines the regulatory roles that ASIC and the Australian Transactions Reports and Analysis Centre (AUSTRAC)[1] play in regulating financial service providers. Finally, it examines the interplay of Australia's international Anti Money Laundering/Counter-Terrorism Financing obligations.

1.6 Chapter 4 examines many issues relating to financial service providers, including: banks; remittance providers; and the self-managed superannuation sector. This chapter examines additional issues to those assessed in Chapter 3, particularly in relation to ASIC and AUSTRAC and their roles as regulators for different financial service providers. Particular interest is paid to issues of disproportionate penalties, and the 'de-banking' of the independent remittance industry.

1.7 Chapter 5 considers issues associated with collaboration between law enforcement agencies and the private sector, with particular focus on financial service providers.

1.8 Chapter 6 examines issues related to technology and the increasing incidences of identity crimes in Australia. It examines the use of digital currencies and the 'Darknet' to facilitate financial related and other crimes, as well as the effects of new technologies, like contactless payments. Chapter 6 also examines some of the strategies available to both the private sector and law enforcement agencies for identity verification, including the Document Verification System.

1.9 Finally, Chapter 7 considers issues raised by the National Indigenous Intelligence Taskforce (NIITF), and the particular vulnerabilities of Indigenous communities to financial related crime. In this context, the chapter also examines the need for additional education, financial literacy and improving governance capabilities in Indigenous communities, including through the provision of information in Indigenous languages.

Conduct of inquiry

1.10 The committee advertised the inquiry in *The Australian* and on the internet. The committee also invited submissions from interested organisations, individuals and government bodies. The committee received 23 submissions. A list of individuals and organisations that made public submissions, together with other information authorised for publication is provided at Appendix 1.

1.11 The committee held public hearings in Darwin, Sydney and Canberra on 8, 9 and 10 September 2014 respectively. The witnesses who appeared before the committee are listed in Appendix 2.

1.12 The committee thanks the organisations and individuals that made written submissions, and those who gave evidence at the public hearings.

---

1 Please note, this also includes consideration of the question of AUSTRAC's membership of the Australian Crime Commission Board.

Financial related crime—background

Increasing threat

1.13 The risks of financial related crime are expanding exponentially due to the higher reliance on electronic means to pay for goods and services as well as transfer money. While this is not a new trend, the increasing sophistication of the serious and organised crime threat results in the need for Commonwealth law enforcement agencies, together with state and territory partners and the finance sector, to ensure that they co-operate as effectively as possible.

Need for collaboration

1.14 Given the speed at which financial related crimes may be committed, law enforcement agencies must collaborate effectively and efficiently with the private sector to strengthen the security of financial products and services. The committee's report details some of the successful instances of cross-agency and agency-industry co-operation that has led to significant progress in deterring and disrupting financial crimes perpetrated by serious and organised crime groups.

Financial related crime—types, prevalence and impacts

1.15 'Financial related crime' encompasses activities 'ranging from fraud through to the active manipulation of the stock market, or laundering the proceeds of crime.'[2] The International Monetary Fund defines financial related crime as 'any non-violent crime resulting in financial loss.'[3] In its submission, the Australian Federal Police (AFP) identify the following components within financial related crime:

- money laundering;
- identity crime;
- serious and complex fraud; and
- corruption.[4]

1.16 Submitters broadly agreed that the impact of financial crime is highly significant.

1.17 For instance, AUSTRAC submitted that serious and organised crimes cost Australia up to $15 billion annually.[5] Australia's anti-money laundering and counter-terrorism financing regulator argued:

> Money laundering threatens Australia’s prosperity, undermines the integrity of our financial system and funds further criminal activity that impacts on

2 ACC, *Financial Crimes*, www.crimecommission.gov.au/organised-crime/crime-types/financial-crimes, (accessed 1 May 2015).

3 AFP, *Submission 6*, p. 1.

4 AFP, *Submission 6*, p. 1.

5 AUSTRAC, *Submission 10*, p. 4.

> community safety and wellbeing. For these reasons, strategic intelligence assessments recognise money laundering as a critical risk to Australia.[6]

1.18 Similarly the AFP outlined the broader impacts of financial related crime which it said:

> ...poses a significant and growing threat to Australia's national security as it subverts, exploits and distorts legitimate markets and economic activity. This crime type also undermines the ongoing stability of Australian institutions and Governments by having a corrosive impact on community confidence.[7]

1.19 The ACC included in its list of the impacts of financial crime:

- increasingly volatile exchange rates and interest rates due to unanticipated transfers of illicit funds;
- damage to the reputation of individual sectors and businesses;
- damage to the country's financial reputation;
- loss of consumer confidence in businesses;
- negative effects on economic growth when resources are diverted to less productive activities;
- reduced ability to attract foreign investment; and
- increased costs of security and regulation.[8]

1.20 Financial related crime presents a unique set of challenges for Australian law enforcement agencies, as well as for private sector organisations such as banks and other financial institutions.

1.21 The ACC noted that because financial crimes 'cover a broad range of activities often combining licit and illicit financial transactions' it can be difficult to gauge the true extent of the criminal activity.[9] In addition to this difficulty, the ACC observed that opportunities for financial crimes have increased due to globalisation, advances in technology, and changes in the way financial transactions and business are conducted.[10] The approaches used by perpetrators are highly diverse and can range from crude to sophisticated, for example:

---

6 AUSTRAC, *Submission 10*, p. 4.

7 AFP, *Submission 6*, p. 1.

8 ACC, *Financial Crimes*, www.crimecommission.gov.au/organised-crime/crime-types/financial-crimes, (accessed 1 May 2015).

9 ACC, *Financial Crimes*, www.crimecommission.gov.au/organised-crime/crime-types/financial-crimes, (accessed 1 May 2015).

10 ACC, *Financial Crimes*, www.crimecommission.gov.au/organised-crime/crime-types/financial-crimes, (accessed 1 May 2015).

- looking through a person's rubbish for bank and credit card statements, using pre-approved credit offers and tax information, or obtaining old gas and electricity bills and using their personal information to apply for a bank loan;
- 'ponzi' or pyramid investment schemes, where criminals typically offer victims an unrealistically high rate of return on investments;
- facilitation of money laundering; and
- insider trading.[11]

1.22 A key challenge for law enforcement in combatting financial crime is access to data held by financial institutions, commonwealth agencies and other police jurisdictions. With an increasingly globalised world, a further critical factor for law enforcement is addressing the increasing sophistication of financial crime, especially the use of technology:

> Financial crime is becoming increasingly sophisticated, often due to the interconnected nature of global financial markets and the virtual world that we live in now and the role of technology in facilitating most of our financial transactions. It is also instructive that, of the national criminal target lists that the Australian Crime Commission have identified, up to 70 per cent are either internationally based or have international connections.
>
> So the connectivity in both domestic and international markets is quite a critical factor.[12]

1.23 This complex and ever evolving type of criminal activity naturally presents significant challenges for law enforcement agencies. Over the course of the inquiry, the committee heard evidence from numerous witnesses and submitters of the efforts to combat financial related crime.[13]

1.24 The committee has made numerous substantive recommendations that it believes will greatly enhance the ability of individuals, service providers and law enforcement agencies to better protect themselves from financial related crime in Australia.

---

11 ACC, *Financial Crimes*, www.crimecommission.gov.au/organised-crime/crime-types/financial-crimes, (accessed 1 May 2015).

12 Mr Chris Dawson APM, Chief Executive Office, Australian Crime Commission, *Committee Hansard*, 10 September 2014, p. 1.

13 See for example: AFP, *Submission 6*, p. 1; AGD, *Submission 9*, p. 1.

Chapter 2

Powers and taskforces

2.1 Over the course of the inquiry the committee heard from numerous witnesses and submitters about the value of multi-agency taskforces in addressing certain jurisdictional issues.

2.2 This chapter examines the evidence relating to three specific areas, all of which engage different aspects of Commonwealth law enforcement agency relationships.

2.3 Firstly, the committee heard about the impressive results of multi-agency taskforces. Two taskforces, *Project Wickenby* and *Taskforce Eligo*, were cited by Commonwealth law enforcement agencies as examples of effective cross-agency collaboration, especially in instances where agencies have different information gathering and sharing powers.[1]

2.4 Secondly, this chapter addresses a specific example raised by Commonwealth law enforcement agencies of inefficiency within a multi-agency relationship. For example, officials from the Reserve Bank of Australia (RBA) suggested that their relationship with the AFP could be strengthened through administrative changes to processes for counterfeit note investigations.

2.5 Finally, this chapter examines the *Momcilovic*[2] decision that was queried by state and territory police as potentially raising procedural legal questions for state and territory police in Australia.

Federal multi-agency taskforces

2.6 The ACC and AFP argued that multi-agency taskforces had played an enormously beneficial role for Commonwealth and state and territory law enforcement agencies. Further, the ATO argued one of the benefits of multi-agency taskforces was the ability of agencies to share data under prescribed circumstances. Normally, agencies, like the ATO, are prevented from sharing certain information with other law enforcement agency partners for privacy and other legal reasons.

2.7 This section examines some of the significant benefits of multi-agency taskforces, while taking into account the announcement made in the 2015-16 Budget to establish a Serious Financial Crime Taskforce.

Benefits and effectiveness of taskforces

2.8 One critical issue that emerged during the inquiry is whether the full benefits of the taskforces are exploited over the longer term. This was largely due to the

---

1 ACC, *Submission 5*, p. 4.

2 *Momcilovic v the Queen & Ors* [2011] HCA 34.

limited duration of taskforces resulting in officers returning to their 'home' agencies at the taskforces' conclusion.[3]

2.9 One question often raised in evidence was whether taskforces should be made permanent so as to retain the skills and expertise developed in fighting financial related crime. This question is examined in detail below.

2.10 ASIC was supportive of multi-agency taskforces, noting they were an effective method of investigating financial crimes, when specifically funded. ASIC noted that under present arrangements, agencies are restrained in the information that they may share with each other, whereas the use of prescribed taskforces had allowed agencies to share information where authorised and appropriate:

> At present, the general sharing of information between agencies, such as ASIC and the Australian Federal Police (AFP) or the ATO, are severely restricted by our respective obligations around the use and disclosure of confidential information. The ATO, in particular, has significant limitations in disseminating information to other agencies outside of matters that are being investigated by prescribed taskforces such as Project Wickenby.[4]

2.11 The ACC argued that the importance of cooperation in the fight against financial related crime, facilitated through partnerships and taskforces, cannot be underestimated. The ACC submitted that cross-agency collaboration through joint taskforces is effective in combatting financial related crime:

> The fight against serious financial crime is dependent upon comprehensive partnerships between the law enforcement and regulatory community, industry, academia, the broader public and the international community. In the Australian context partnerships are often enhanced through the establishment of key [taskforces] aimed at responding to thematic or individual targeted serious financial crime threats. In recent years, numerous taskforces have focused on addressing aspects of financial crime including a key emphasis on the financial crime activities of organised crime groups operating in Australia, such as [Taskforce] Eligo, the Criminal Asset Confiscation Taskforce, Project Wickenby, and [Taskforce] Galilee.[5]

2.12 The ATO addressed potential concerns surrounding the use of private taxpayer information in joint taskforces. Under current arrangements, the ATO is not allowed to disclose taxpayer information with other agencies unless specific requirements are met:

> Taxpayers entrust sensitive financial information to the ATO in order to allow it to administer the tax system. Accordingly, the law treats information about taxpayers in the ATO's possession as confidential ('protection information').

---

3 ASIC, *Submission 21*, p. 6.

4 ASIC, *Submission 21*, p. 6.

5 ACC, *Submission 5*, p. 4.

> The legislative framework for this confidentiality, and the limited exceptions under which protected information can be disclosed, is found in…the *Taxation Administration Act 1953 (Cth)*.[6]

2.13 The ATO explained the restrictions around sharing of protected information with other Commonwealth agencies:

> Tax law allows protected information to be disclosed for the investigation of an offence punishable by at least 12 months in prison. Commonwealth, state and territory law enforcement agencies thereby use protected information to investigate specific cases of financial crime such as fraud.
>
> However, the use and on-disclosure of information disclosed under this exception can only be used for that specific purpose. The information cannot be obtained as part of criminal intelligence activities before a specific offence is identified, nor can the information be used for intelligence purposes.[7]

2.14 Further, the ATO submitted that protected information can also be shared with members of taskforces for any of the taskforces purposes. In these instances, criminal intelligence activities conducted as part of taskforce activities enable a more proactive and effective approach. The ATO argued:

> The more streamlined information-sharing environment created by a prescribed taskforce offers a substantial advantage to the ATO in supporting law enforcement agencies to deal with priority threats.
>
> The prescribed taskforce provisions were modelled on a specific legislative exception that exists for agencies involved in Project Wickenby.[8]

Information sharing

2.15 The committee heard evidence from government agencies regarding information sharing between agencies for the purposes of taskforces.[9] This report particularly examines two multi-agency taskforces, Project Wickenby (*Wickenby*) and Taskforce Eligo (*Eligo*), both of which resulted in significant advances in the detection and prosecution of financial related crime.

2.16 Further details of the use and sharing of sensitive law enforcement information and intelligence in the contexts of *Wickenby* and *Eligo* are discussed below.

---

6 ATO, *Submission 7*, p. 4.

7 ATO, *Submission 7*, p. 4.

8 ATO, *Submission 7*, p. 4.

9 For example: Mr Richard Grant, National Manager, Investigations, Australian Crime Commission, *Committee Hansard*, 10 September 2014, p. 6.

Project Wickenby

2.17 As mentioned above, *Wickenby* was specifically raised by submitters as an example of an effective taskforce that drew together expertise and staff from different agencies, working collaboratively to achieve common goals.[10] For example, the ATO noted that *Wickenby* was successful insofar as it had:

- recouped tax that had been avoided or evaded;
- reduced funds flowing to secrecy jurisdictions; and
- successfully prosecuted promoters and facilitators of abusive use of overseas secrecy jurisdictions.[11]

Establishment of taskforce

2.18 *Wickenby* was established in 2006 to 'protect the integrity of Australia's financial and regulatory systems by preventing people from promoting or participating in the abusive use of secrecy jurisdictions.'[12]

2.19 Operations and activities carried out in Australia as part of *Wickenby* included:

- civil audits and risk reviews undertaken by the ATO, and civil investigations conducted by the ASIC;
- criminal investigations conducted by the Australian Crime Commission (ACC), Australian Federal Police (AFP) and ASIC;
- prosecutions and other legal action undertaken by the Attorney-General's Department (AGD), the Commonwealth Director of Public Prosecutions (CDPP), and the Australian Government Solicitor (AGS)
- administrative actions, including audits, banning people from the financial services industry and using data from the Australian Transaction Reports and Analysis Centre (AUSTRAC) to track money moving in and out of Australia; and
- proceeds of crime action, including action to restrain property and seek its forfeiture.[13]

2.20 *Wickenby* was composed of 7 federal agencies together with the ATO as lead agency. The *Wickenby* partner agencies were AUSTRAC, ASIC, ACC, AFP, AGD, AGS and the CDPP.[14]

---

10 ATO, *Submission 7*, p. 3.

11 ATO, *Submission 7*, p. 5.

12 ATO, *Project Wickenby*, www.ato.gov.au/General/The-fight-against-tax-crime/In-detail/Tax-crime/Project-Wickenby/ (accessed 4 June 2015).

13 ATO, *Project Wickenby*, www.ato.gov.au/General/The-fight-against-tax-crime/In-detail/Tax-crime/Project-Wickenby/ (accessed 23 June 2015).

2.21 Notably, *Wickenby* was the first time the full range of Australian Government resources were used to address illegal overseas schemes that posed threats to the integrity of Australia's financial and regulatory systems.[15]

Results of Wickenby

2.22 As at 31 January 2015, *Wickenby* had resulted in numerous successes, including having raised $2.163 billion in liabilities, and completing 4848 audits. An additional 102 audits remain underway as at 4 June 2015.[16]

2.23 Further, *Wickenby* resulted in charges being laid against 76 people and 44 convictions.[17]

2.24 The total amount of money recouped by *Wickenby* to 31 January 2015 was $920.68 million.[18]

2.25 The ATO's representatives spoke strongly in favour of the positive impact of *Wickenby*, arguing it had demonstrated its effectiveness as a template for Commonwealth agency responses to financial related crime. Mr Brett Martin, Assistant Commissioner, Indirect Tax, Compliance Strategy and Government Relations at the ATO, noted that as *Wickenby* was due to conclude in 2015, it is important to ensure that its work continues in some form:

> With Project Wickenby coming to a close [in 2015], we need to work out how to keep the pressure on those who decide to engage in finance related crime behaviours. To that end, the ATO has worked with the ACC and the AFP to determine how best to use the existing resources and frameworks to respond to specific instances of high-priority, serious financial crime in a more coordinate and effective manner.[19]

2.26 While emphasising the effectiveness of taskforces more broadly, ATO officials also noted that it was necessary in certain circumstances to obtain exemptions from some tax secrecy provisions, often cited by other law enforcement agencies as problematic within their investigations:

> Project Wickenby has a specific statutory authority exception in tax secrecy provisions, allowing us to share information for the purpose of that task

---

14 ATO, Project Wickenby, www.ato.gov.au/General/The-fight-against-tax-crime/In-detail/Tax-crime/Project-Wickenby/ (accessed 4 June 2015).

15 ATO, Project Wickenby, www.ato.gov.au/General/The-fight-against-tax-crime/In-detail/Tax-crime/Project-Wickenby/?page=1#Who_we_are (accessed 4 June 2015).

16 ATO, Project Wickenby, www.ato.gov.au/General/The-fight-against-tax-crime/News-and-results/Project-Wickenby---getting-results/ (accessed 4 June 2015).

17 ATO, Project Wickenby, www.ato.gov.au/General/The-fight-against-tax-crime/News-and-results/Project-Wickenby---getting-results/ (accessed 4 June 2015).

18 ATO, Project Wickenby, www.ato.gov.au/General/The-fight-against-tax-crime/News-and-results/Project-Wickenby---getting-results/ (accessed 4 June 2015).

19 Mr Brett Martin, Assistant Commissioner, Indirect Tax, Compliance Strategy and Government Relations, ATO, *Committee Hansard*, 10 September 2014, p. 21.

> force. That specific exception will cease on 30 June 2015. The exceptions for disclosure to a prescribed taskforce will remain, but they will rely on the prescription of a taskforce by regulation.[20]

2.27 With law enforcement agencies, especially the ATO, arguing that access to confidential information of taskforces is critical to their success, agencies also reiterated that non-ATO agencies do not normally have exemptions from the legal requirement of taxpayer confidentiality.[21]

2.28 The ATO's submission provides an instance where the ATO was unable to assist a police investigation relating to credit card and identity fraud:

> This restriction has prevented the ATO from assisting law enforcement on a number of occasions. In one example, state police were investigating credit card fraud involving identity fraud. Police obtained notices of assessment used as proof of identity to open bank accounts, which it suspected of being forged. The ATO was prohibited by law from confirming to the police whether the TFN actually belonged to the individual named on the forged notice.[22]

2.29 Law enforcement agencies argued that operating within a prescribed taskforces meant that information could be shared between the ATO and non-ATO agencies in a sensitive and appropriate way. Sharing information in this manner would not be in conflict with provisions in tax law that prohibit the disclosure of tax file numbers by the ATO to third parties.[23]

Lessons from Wickenby

2.30 The AFP submitted that it valued *Wickenby*-like methods to inter-agency cooperation to achieve 'whole of government' approaches to the detection, disruption and prosecution of financial related crime.[24]

2.31 The AFP noted that the original request to establish *Wickenby* by the Heads of Commonwealth Law Enforcement Agencies (HOCOLEA) had also required the development of comprehensive and effective multi-agency taskforces 'that can respond flexibly to threats from serious and organised crime impacting on the Commonwealth.'[25]

2.32 The AFP submission further strengthens the argument for the retention of the effective taskforce model established by *Wickenby*:

---

20 Mr Brett Martin, Assistant Commissioner, Indirect Tax, Compliance Strategy and Government Relations, ATO, *Committee Hansard*, 10 September 2014, p. 21.

21 ATO, *Submission 7*, p. 5.

22 ATO, *Submission 7*, p. 5.

23 Mr John Ford, Assistant Commissioner, Private Groups and High Wealth Individuals, Tax Crime, ATO, *Committee Hansard*, 10 September 2014, p. 21.

24 AFP, *Submission 6*, p. 9.

25 AFP, *Submission 6*, p. 9.

> In accordance with the [Heads of Commonwealth Law Enforcement Agencies] task, and with the cessation of Project Wickenby funding in June 2015, the AFP, ATO and Australian Crime Commission (ACC) are working together to identify cooperative multi-agency approaches, within existing resources and frameworks, to enhance the Commonwealth's ability to respond to specific instances of high priority financial crime in a more coordinated and effective manner.[26].

2.33 *Wickenby* concluded on 1 July 2015.[27] The work of *Wickenby* will be continued through the establishment of the Serious Financial Crime Taskforce, which is discussed below.[28]

Taskforce Eligo

2.34 Another example of cross-agency collaboration is the Eligo National Taskforce (*Eligo*), which was established by the ACC Board in December 2012.

2.35 *Eligo* involved the ACC, AUSTRAC and the AFP working together to reduce risks inherent in the Alternative Remittance Sector (ARS) and other Informal Value Transfer Systems (IVTS). Those systems are further examined in chapter 4.

2.36 AUSTRAC published the *National Threat Assessment on Money Laundering* in 2011 that found the overall money laundering threat from the ARS was 'high'. A joint analysis produced by the ACC, AFP and AUSTRAC in June 2012 concluded that a nationally coordinated approach to identifying and responding to high risk remitters was required. The ACC Board subsequently established *Eligo*:

> ...to take a coordinated and collective approach against high-risk remitters and IVTS operating in Australia to reduce their adverse impact on Australia and its national economic wellbeing.[29]

2.37 *Eligo* was intended to disrupt remitters and IVTS operators who were assessed as posing a high money laundering risk, and 'to implement crime prevention strategies aimed at optimising the use of the current *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF) regime.'[30]

2.38 The ACC argued that *Eligo*, by focusing on instances where ARS and IVTS were being used to launder proceeds of crime, was able to identify criminal activities and criminal groups previously unknown to law enforcement agencies.[31]

---

26 AFP, *Submission 6*, p. 9.

27 ATO, *Submission 7*, p. 5.

28 The Hon Joe Hockey MP, Media Release, *Serious Financial Crime Taskforce* (5 May 2015), www.joehockey.com/media/media-releases/details.aspx?r=480 (accessed 4 June 2015).

29 ACC, *Submission 5*, p. 15.

30 ACC, *Submission 5*, p. 16.

31 ACC, *Submission 5*, p. 16.

Results of Eligo

2.39 Since its establishment, *Eligo* has restrained more than $580 million worth of drugs and assets, including $26 million in cash. It has also disrupted 18 serious and organised crime groups, and identified 128 criminal targets previously unknown to law enforcement agencies.[32]

Serious Financial Crime Taskforce

2.40 On 5 May 2015, the Hon Joe Hockey MP, the Treasurer, announced that the Commonwealth Government would establish a new taskforce to fight serious and organised financial crime. The taskforce would include officers from the ATO, ACC, AFP, AGD, AUSTRAC, ASIC, CDPP and ACBPS. The Treasurer's media release notes:

> The Taskforce will build on the good work already done by Project Wickenby which finishes in 2015. It will enable the best practice and experience gained to be continued, and for agencies to extend their cooperative work across the broader serious financial crime risk.
>
> ...
>
> The Serious Financial Crime Taskforce will have an unquantifiable positive benefit on the financial wellbeing of members of the community who, without the Taskforce, may be victims of financial crime. It will also help ensure all taxpayers pay their fair share of tax.[33]

2.41 Budget Paper No. 2 outlines the financial allocation for the taskforce over four years will total $127.6 million,[34] with an additional $3.2 million GST component to be paid to State and Territory governments.[35] Further, the paper notes:

> The measure is estimated to increase revenue by $419.7 million and expenses by $130.8 million with a net improvement to the Budget of $288.9 million in fiscal terms over the forward estimates period.[36]

Committee view

2.42 The committee notes the clear advantages of multi-agencies taskforces, and believes that agencies have demonstrated the effectiveness of taskforce arrangements in appropriately sharing information and intelligence that may not be possible in non-taskforce settings.

2.43 The committee recognises the significant results from both *Project Wickenby* and *Taskforce Eligo*, and believes these multi-agency taskforces have clearly demonstrated the enormous benefit to the Australian community of law enforcement

---

32 ACC, *Submission 5*, p. 16.

33 The Hon Joe Hockey MP, Media Release, *Serious Financial Crime Taskforce* (5 May 2015), www.joehockey.com/media/media-releases/details.aspx?r=480 (accessed 4 June 2015).

34 Treasury, *Budget Paper No.2 2015-16*, p. 30.

35 Treasury, *Budget Paper No.2 2015-16*, p. 30.

36 Treasury, *Budget Paper No.2 2015-16*, p. 30.

agency collaboration. The committee agrees that the advantages of multi-agency taskforces are significant, and generally far outweigh the administrative costs associated with their establishment. Indeed, the projection that the establishment of the Serious Financial Crime Taskforce will yield the Australian tax payer nearly $300 million over a four year period clearly demonstrates that this approach has multiple benefits for both the Australian Government and community.

2.44 The committee is however concerned that disbanding taskforces may not adequately build on the skills and benefits of such collaborative work. Therefore, the committee strongly supports the creation of the Serious Financial Crime Taskforce and believes it will build on the significant successes of *Wickenby*. Had the government not established the Serious Financial Crime Taskforce, given the outstanding achievements of *Wickenby*, the committee would have recommended that such a taskforce be formed.

2.45 Noting that this new taskforce will generate net revenue for the government of almost $300 million over four years, the committee is of the view that the taskforce should continue for as long as it is detecting, disrupting and prosecuting financial related crime.

2.46 To fully capture the long-term benefits of multi-agency taskforces, the committee supports the introduction of a standardised review process for taskforces prior to their conclusion. This review process would involve an examination of the operations and outcomes of each law enforcement taskforce approximately 12 months prior to its conclusion in order to determine whether it should be made an ongoing arrangement.

Recommendation 1

2.47 The committee recommends that the government review the operations and outcomes of each law enforcement taskforce approximately 12 months prior to its conclusion in order to determine whether it should be made an ongoing taskforce.

Counterfeit note double handling

2.48 The committee heard evidence relating to the complex administrative arrangements in place for investigations of counterfeit bank notes by the Reserve Bank of Australia (RBA) and AFP. The RBA noted that it had raised this issue with the AGD in 2009 during the review into the *Crimes (Currency) Act 1981*. The RBA noted that while other reforms have taken precedence, it is committed to streamlining the investigation of counterfeit bank notes.[37]

2.49 The RBA explained that since 2009 it has undertaken much of the administrative work relating to counterfeit bank note investigations, whereas the AFP was originally responsible for administration and investigation. Mr Keith Drayton, Deputy Head of the Note Issue Department, RBA noted that:

37 RBA, *Submission 17*, pp 3–4.

> …we still have this situation where under the legislation all the counterfeits have to go to the AFP, which essentially means that the AFP has to act as a post box collector and emptier. The counterfeits go to a post box and the AFP has to empty it and deliver it to [the RBA], which detracts them from their investigative obligations.[38]

2.50 While current legislative arrangements require that an AFP officer is posted to the RBA, there would be significant efficiencies achieved if the relationship between the RBA and AFP was re-examined. Mrs Michelle Bullock, the Assistant Governor (Currency) at the RBA explained:

> ...[the AFP] are best at investigating and enforcing, and anything that takes their focus away from that—administrative, data entry and that sort of thing—is not good. It is better if we work as a team with them. We take on the administration and we take on all the boring bits and we feed them the information in a timely fashion, which they can then investigate.[39]

2.51 The AFP noted that the administrative arrangement was being examined by the AGD, and agreed that it did not support the current arrangement. The APF's preference was for a streamlined approach that allowed the RBA to act as 'post box' for counterfeit note investigation processing.[40]

Committee view

2.52 The committee agrees with the evidence presented by the RBA and AFP that the administrative arrangement should be re-worked. It seems illogical to continue to require 'double handling' of counterfeit notes when that has the potential to delay or frustrate law enforcement investigations or the collection of counterfeit currency.

2.53 The committee believes this would free up AFP resources to focus on investigative tasks, as opposed to administrative ones.

2.54 The committee agrees that the arrangement should be streamlined through legislative change to the *Crimes (Currency) Act 1981*.

Recommendation 2

2.55 The committee recommends that the government introduce amendments to the *Crimes (Currency) Act 1981* to give the RBA administrative responsibilities and the AFP law enforcement responsibilities with respect to counterfeit note collections and investigations.

---

38 Mr Keith Drayton, Deputy Head, Note Issue Department, Reserve Bank of Australia, *Committee Hansard*, 9 September 2014, p. 20.

39 Mrs Michelle Bullock, Assistant Governor (Currency), Reserve Bank of Australia, *Committee Hansard*, 9 September 2014, p. 21.

40 Mr Michael Phelan, Deputy Commissioner Operations, Australian Federal Police, *Committee Hansard*, 10 September 2014, p. 18.

Jurisdictional issues (the *Momcilovic* case)

2.56 Several witnesses raised the complexity of jurisdictional issues of financial related crime, both domestically and internationally. One example raised by Northern Territory Police (NT Police) and the Victoria Police was the effect of the *Momcilovic*[41] case, in which the High Court was required to rule on whether there were inconsistencies between federal and state offences for drug trafficking.

2.57 The Victorian Government Solicitor's Office has stated:

> A majority of the Court allowed the appeal brought by Ms Momcilovic, setting aside her conviction of drug trafficking and remitting the matter to the County Court of Victoria for a retrial. The decision has implications for the trial of drug trafficking and possession offences in Victoria, the operation and application of the Charter Act and the operation of s 109 of the Commonwealth Constitution where conduct is an offence under both State and Commonwealth laws.[42]

2.58 The NT Police submitted concerns with respect to the interplay of Commonwealth and territory law relating to drugs offences, arguing that there was uncertainty as to which legislation should ultimately be used to lay charges:

> …we have some concerns around issues…legislative primacy, particularly with offences that are committed or potentially committed in the Territory but involving Commonwealth interests and then what legislation bears primacy.[43]

2.59 The NT Police specifically raised the *Momcilovic* matter in the committee's hearing, and outlined the issues the decision has raised:

> What the *Momcilovic* case provided was that an offence can be committed. If we use the Territory as an example, because this case, I believe, was in Victoria. Should an offence be committed here in the Northern Territory and we use Territory powers to execute search warrants, we use Territory powers in order to interview offenders and to [proffer] charges, it may well be the case that, through the decision of *Momcilovic*, we should have used Commonwealth legislation, because of the way the monies may have been held in trust, because of who the true victim of the crime was and how the offence was perpetrated. We are still working through some of those issues, particularly when it comes to financial crime, and trying to make that determination about whose jurisdiction it really rests in, particularly when looking at this ruling of the High Court. As I say, we are currently in a state

41 *Momcilovic v the Queen & Ors* [2011] HCA 34.

42 Victorian Government Solicitor's Office, Case Note, *Momcilovic v The Queen [2011] HCA 34 (8 September 2011)*, http://www.vgso.vic.gov.au/sites/default/files/Case%20Note%20-%20Momcilovic%20v%20The%20Queen.pdf (accessed 29 June 2015).

43 Mr Mark Payne, Assistant Commissioner, Crime and Specialist Services, Northern Territory Police Force, *Committee Hansard*, 8 September 2014, p. 1.

> of flux where we are examining how this affects us in the Northern Territory and what legislative provisions we need alter.[44]

2.60 Victoria Police expressed similar concerns with the *Momcilovic* decision.[45] While noting that Commonwealth legislation overrides state or territory legislation, Assistant Commissioner Fontana argued that Victoria Police were encouraged by the decision to charge persons under Commonwealth legislation:

> ...Commonwealth legislation does override. We do have the authority to use Commonwealth legislation, but it is an issue, particularly in the joined-up arrangements, when you are looking at the constitutional arrangements. It is quite important to get your head around that if you are looking at, say, introducing a national approach for dealing with unexplained wealth. You need to look at the implications of the Constitution and that needs to be tailored for any laws that you are drafting.[46]

2.61 The AGD did not agree with the evidence presented by some witnesses, that the *Momcilovic* decision encouraged state and territory police to use Commonwealth legislation to charge and prosecute for certain offences. In answers to *Questions on Notice*, the AGD noted that the *Momcilovic* decision:

> ...has been considered by the Standing Council of Attorneys-General (SCAG) and the Standing Council on Law and Justice (SCLJ), and by justice agency officials through the National Justice CEOs forum (NJCEOs) and the National Criminal Law Reform Commission (NCLRC).
>
> At the meeting of the Standing Council on Law and Justice in April 2012, Ministers asked the NCLRC to undertake work to review existing means for avoiding constitutional inconsistency between Commonwealth, State and Territory criminal laws, and, if necessary, develop new proposals for avoiding such inconsistency.
>
> In June 2013, following advice from the NCLRC, the NJCEOs agreed that this project required no further consideration on the basis that the risk of inconsistency was low.[47]

2.62 Accordingly, the AGD did not agree that *Momcilovic* requires a national policy response.[48]

Committee view

2.63 The committee notes that while NT Police and Victoria Police both raised concerns with respect to the findings in *Momcilovic*, the National Criminal Law

---

44 Mr Mark Payne, Assistant Commissioner, Crime and Specialist Services, Northern Territory Police Force, *Committee Hansard*, 8 September 2014, p. 7.

45 Mr Stephen Fontana, Assistant Commissioner, Victoria Police, *Committee Hansard*, 9 September 2014, p. 56.

46 Mr Stephen Fontana, Assistant Commissioner, Victoria Police, *Committee Hansard*, 9 September 2014, p. 56.

47 Attorney-General's Department, *Answers to Questions on Notice*, p. 1.

48 Attorney-General's Department, *Answers to Questions on Notice*, p. 1.

Reform Commission, and the National Justice CEOs disagreed, finding the risk of inconsistency was low.

2.64 The committee agrees with the evidence presented by the AGD that *Momcilovic* does not require a national policy response.

Chapter 3
Legislative and regulatory issues

3.1 As discussed in Chapter 2, the effectiveness of prescribed taskforces has been clearly demonstrated by the collaboration between Commonwealth agencies in *Project Wickenby* and *Taskforce Eligo*. Critically however, the issue of information sharing remains somewhat unresolved outside of prescribed taskforces.

3.2 This chapter examines numerous legislative and regulatory issues facing Commonwealth law enforcement agencies, including the ATO, ASIC and AUSTRAC. Amongst other things it examines agency requests for broader powers with which to combat financial related crime as single agencies.

3.3 In the case of AUSTRAC, this chapter outlines the agency's efforts to continue to implement an Anti-Money Laundering/Counter Terrorism Financing (AML/CTF) regime that meets Australia's domestic and international obligations. While this chapter outlines the AML/CTF regime in Australia, further discussion of the AML/CTF regime, especially from the perspective of remittance industry operators, and the 'de-banking' of the remittance industry, is located in Chapter 4.

New telecommunications interception agencies

3.4 During this inquiry the committee heard evidence regarding the need to broaden the telecommunications interception arrangements to include certain individual agencies. In some respects this issue complements the multi-agency taskforce arrangements discussed in Chapter 2. In particular, the committee received evidence with respect to telecommunications interception powers of the ATO and ASIC.

3.5 While support for the ATO's designation as an interception agency[1] was broadly stronger than for ASIC, the committee examined the possibility of both agencies being given increased telecommunications interception powers.

3.6 It is worth noting that during the course of this inquiry ASIC was designated a criminal law enforcement agency by the passage of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*.[2] This legislative change is discussed in greater detail below.

Australian Taxation Office

3.7 In 2012, the committee tabled a report into its inquiry into Commonwealth unexplained wealth legislation and arrangements. The report discussed many aspects

---

1 See, for example: Mr Chris Dawson APM, Chief Executive Officer, Australian Crime Commission, *Committee Hansard*, 10 September 2014, p. 5.

2 *Journals of the Senate*, No. 93–13 May 2013, p. 2594.

of the unexplained wealth arrangements in Australia and included a recommendation to amend the *Telecommunications (Interception and Access) Act 1979* (TIA Act). Specifically, the committee recommended:

> ...amending the *Telecommunications (Interception and Access) Act 1979* so as to allow the Australian Taxation Office to use information gained through telecommunications interception in the course of joint investigations by taskforces prescribed under the *Taxation Administration Act 1953*, for the purpose of the protection of public finances.[3]

3.8 The previous government presented a response to this recommendation in February 2013. In its response, the government formally noted the recommendation, arguing:

> The ability to use intercepted information for an agency's own purposes is currently limited to interception agencies (law enforcement and anti-corruption agencies) that are investigating prescribed offences (generally a serious offence or an offence punishable by imprisonment or a period of at least 3 years). Section 67 of the *Telecommunications (Interception and Access) Act 1979 (TIA Act)* only allows the ATO to deal with existing intercepted information in order to assist with investigations being conducted by these agencies.
>
> Currently, the ATO cannot subsequently use this intercepted information for its own investigations or tax assessments, and cannot request interception information for the ATO's own purposes.
>
> While the Government agrees in principle that amending the information sharing provisions in the TIA Act will allow agencies to more fully cooperate, appropriate limitations on the use of existing intercept information will also need to be assessed. To enable appropriate consideration of this recommendation, the Attorney-General's Department has sought advice from the ATO on how the ATO proposes to use existing intercepted information in its taxation assessment taskforces, including the offences the ATO wishes to investigate using intercepted information. The Department will continue to liaise with the ATO on this issue.[4]

3.9 In evidence to the committee's present inquiry, the ACC supported expanding the TIA Act to enable intelligence sharing with the ATO, arguing:

> The [ACC] is supportive of...broadening out the *Telecommunications (Interception and Access) Act* to promote for instance sharing of that product with the ATO, we believe would collectively strengthen Australia's response to serious and organised crime in the financial sector because some of those limitations both ways, from law enforcement to the ATO and from ATO back to law enforcement, are in our view ripe for some reform to

---

3 Parliamentary Joint Committee on Law Enforcement, *Inquiry into Commonwealth unexplained wealth legislation and arrangements*, Recommendation 7, p. xiv.

4 Government response, Parliamentary Joint Committee on Law Enforcement, *Inquiry into Commonwealth unexplained wealth legislation and arrangements*, pp 3–4.

> enable both the ATO and law enforcement more broadly to address financial crime.[5]

3.10 Below, the committee makes a recommendation regarding the ATO's interception powers under the TIA Act.

Australian Securities and Investments Commission

3.11 ASIC submitted that its inability to receive or intercept telecommunications information, 'seriously hinders [ASIC's] ability to enforce the law in a modern corporate world'.[6] ASIC argued that access to intercepted telecommunications information can be a useful tool:

> ...particularly in the case of market misconduct, which is generally conducted opportunistically and with rapidity, via telephone or text messages (SMS), rather than being planned and documented in writing.[7]

3.12 Further, the fact that ASIC was not an 'interception agency' for the purposes of the TIA Act resulted in what ASIC argued was an illogical situation, where other agencies detect possible market misconduct but could not share the material with ASIC:

> This can lead, for example, to situations where other agencies detect possible market misconduct offences through intercepted information, but cannot pass this on to ASIC. We propose that, where it is appropriate to do so, ASIC should be authorised to receive intercepted telecommunications information from 'interception agencies'.[8]

3.13 In answers to *Questions on Notice*, the AGD explained the strict limitations placed on the TIA regime, noting that only interception agencies were able to apply for an interception warrant to investigate serious offences[9]. The AGD noted:

> Given the highly intrusive nature of this power, interception agency status is restricted to Commonwealth and State and Territory law enforcement and anti-corruption bodies (currently the Australian Crime Commission, the Australian Security Intelligence Organisation, the Australian Commission for Law Enforcement Integrity and the Australian Federal Police). Restricted access to interception powers has been supported by successive Parliaments, including by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in its 2013 Report of the Inquiry into Potential Reforms of Australia's National Security Legislation.[10]

---

5 Mr Chris Dawson APM, Chief Executive Officer, Australian Crime Commission, *Committee Hansard*, 10 September 2014, p. 5.

6 ASIC, *Submission 21*, p. 12.

7 ASIC, *Submission 21*, p. 12.

8 ASIC, *Submission 21*, p. 13.

9 For the purposes of the *Question on Notice*, serious offences are offences with a penalty of at least seven years' imprisonment

10 Attorney-General's Department, *Answers to Questions on Notice*, p. 2.

3.14 The AGD clarified that while ASIC could not apply for an interception warrant in its own right, nor receive intercepted telecommunications by itself, it was able to be provided information by an 'interception agency' in certain specific circumstances:

> …an interception agency may disclose intercepted information to ASIC to further that interception agency's own investigation, including in the course of a joint investigation with ASIC. In such circumstances, any information obtained by ASIC during the investigation can only be used for the purposes of that joint investigation.[11]

3.15 Therefore, the original arrangements meant that ASIC needed to be engaged in a joint investigation with an interception agency to receive telecommunications or obtain warrants under the previous iteration of the TIA Act. Any material obtained in this manner could not be used for ASIC activities which were independent of the joint taskforce.

3.16 ASIC submitted that the *Australian Securities and Investments Commission Act 2001* (ASIC Act) only authorised a 'limited range of search activities', restricting its ability to conduct investigations:

> …the powers under the ASIC Act only authorise a limited range of search activities (e.g. entering premises and taking possession of 'particular' books, which ASIC must attempt to name in applying for a warrant), posing significant practical difficulties for ASIC...[12]

3.17 ASIC argued that the *Crimes Act 1914* (Crimes Act) authorises a much larger range of search activities, including the ability to examine electronic equipment at searched premises. Its submission notes however that the Crimes Act 'only authorises searches relating to suspected criminal offences, whereas the ASIC Act allows for searches relating to all of the provisions under ASIC's jurisdiction, including civil penalty provisions and administrative remedies.'[13]

3.18 ASIC suggested that the 'gaps' in its powers meant that early choices of which search warrant to obtain could later determine what kind of law enforcement action could be taken. ASIC argued that a 'simple but effective' change could be the expansion of its powers with respect to search warrants, so that its powers were as procedurally broad as in the Crimes Act, but allow ASIC to collect information that could be used in any type of enforcement action ASIC may take under the ASIC Act.[14]

Data Retention Bill

3.19 In early 2015, the Parliament considered at length the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015 (the bill). This

---

11 Attorney-General's Department, *Answers to Questions on Notice*, p. 2.

12 ASIC, *Submission 21*, pp 11–12.

13 ASIC, *Submission 21*, p. 12.

14 ASIC, *Submission 21*, p. 12.

section focuses on the Parliamentary Joint Committee on Intelligence and Security (PJCIS) inquiry into the bill, and the evidence below was provided to that inquiry. The inquiry examined two issues that had been raised in the financial related crime inquiry, namely the question of interception powers for both ASIC and the ATO.

3.20 While the legislation itself was the subject to much public interest, several issues from the bill are relevant to the question before the committee about whether ASIC should be allowed telecommunications interception powers.

3.21 The PJCIS report did not explicitly comment on the question of the designation of the ATO as a 'criminal law-enforcement agency' for the purposes of the amended TIA Act.

3.22 The amended TIA Act now includes a definition of 'criminal law-enforcement agency', in addition to the previous term 'enforcement agency'. Criminal law enforcement agencies include the AFP, Police forces of states, corruption commissions, the ACC, ASIC, the Australian Commission for Law Enforcement Integrity (ACLEI) and the Australian Competition and Consumer Commission (ACCC).[15]

3.23 The bill proposed the inclusion of the term 'criminal law enforcement agency' within the revised TIA Act. The explanatory memorandum clarified that the term 'criminal law enforcement agency' would strictly limit those agencies able to access 'stored communications'.[16] This is distinct from the designation of some agencies as 'enforcement agencies', that were able to issue 'historic domestic preservation notices and apply for stored communications warrants':

> Item 3 inserts a definition of 'criminal law-enforcement agency' after section 110 of the TIA Act. The definition removes the ability of enforcement agencies that are not also criminal law-enforcement agencies to issue historic domestic preservation notices under subsection 107J(1) and to apply for stored communications warrants under section 110 of the Act. These amendments recognise that while governments at all levels have charged a range of authorities and bodies with responsibility for investigating or enforcing offences punishable by significant prison terms (at least a three year term) access to stored communications should be limited to agencies with a demonstrated investigative need and practices to safeguard the use and disclosure of information obtained under a stored communications warrant.[17]

3.24 The explanatory memorandum also noted that the inclusion of ASIC and the ACCC as 'criminal law enforcement agencies' implemented a recommendation of the

15 *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*, s110A.

16 Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015, *Revised Explanatory Memorandum*, p. 92.

17 Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015, *Revised Explanatory Memorandum*, p. 92.

Parliamentary Joint Committee on Intelligence and Security (PJCIS) which conducted an inquiry into the bill.[18]

3.25 The PJCIS received evidence from the AGD, Professor George Williams, and the Uniting Church Justice and International Mission Unit that supported the inclusion of ASIC (and, in the case of the Uniting Church Mission, the ATO) as 'criminal law enforcement agencies' for a variety of reasons.

3.26 The AGD argued that ASIC's inclusion as a criminal law enforcement agency would put it on a stronger footing with respect to its use of telecommunications interceptions:

> ASIC's ability to access data at the moment relies on their ability to fall within that very broadly and non-specifically cast definition of 'enforcement agency', which does not identify them by name; it relies on them falling within that broad class of agencies who are involved in enforcement of the criminal law and related functions. A declaration as an agency would actually give very specific certainty that ASIC is prescribed for the purposes of accessing data. And I think if anything it puts them on a stronger footing rather making them more susceptible to challenge on the basis on which they can access the data.[19]

3.27 Professor Williams agreed with the department's view when he expressed surprise that ASIC was not included in the telecommunications interception arrangements, 'given its role in investigating quite serious crimes involving what can be significant criminal penalties.'[20]

3.28 The Uniting Church Justice and International Mission Unit supported the expansion of the definition of a criminal law enforcement agency to include the ATO and ASIC. It argued that the new law would limit the information that criminal law enforcement agencies would be able to access, and suggested that without inclusion of ASIC and the ATO, there was a risk both agencies would suffer a reduction of their capacity to fight financial related crimes.[21]

Committee view

3.29 The committee notes the evidence provided to this inquiry, the committee's former inquiry into unexplained wealth, as well as the PJCIS's inquiry into the data

---

18 Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015, *Revised Explanatory Memorandum*, p. 92.

19 Ms Harmer, *Committee Hansard*, 30 January 2015, p. 70, as cited in Parliamentary Joint Committee on Intelligence and Security, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, p. 198.

20 Professor Williams, *Committee Hansard*, 30 January 2015, p. 6, as cited in Parliamentary Joint Committee on Intelligence and Security, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, p. 199.

21 Uniting Church in Australia, Justice & International Mission Unit, Synod of Victoria and Tasmania, *Submission 76*, p. 9, as cited in Parliamentary Joint Committee on Intelligence and Security, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, p. 199.

retention bill on the question of ASIC's and the ATO's inclusion as a criminal law enforcement agency under the TIA Act.

3.30 Overall the committee notes a consistent level of support for the inclusion of these agencies into the new telecommunications interception regime. The committee further notes that ASIC has already been included as a criminal law enforcement agency under the TIA Act due to the passage of the data retention bill. Accordingly, the committee's further comments relate to the ATO's possible inclusion as a criminal law enforcement agency.

3.31 On balance the committee is persuaded that with appropriate safeguards, including adequate privacy and oversight arrangements, the ATO should be able to access intercepted telecommunications information for the purpose of protecting public finances from serious criminal activities such as major tax fraud. In the committee's view, the multiple prosecutions and recovery of billions of dollars in tax liabilities resulting from Project Wickenby, clearly establishes the demonstrated need for the ATO to become a criminal law-enforcement agency under the TIA Act.

3.32 For these reasons the committee remains supportive of inclusion of the ATO as a criminal law-enforcement agency as per the recommendation in its report into unexplained wealth arrangements in Australia.[22]

3.33 The committee continues to support the inclusion of the ATO as a criminal law-enforcement agency for the purposes of the TIA Act.

Recommendation 3

3.34 The committee recommends that subject to appropriate safeguards including adequate privacy and oversight arrangements, the government designate the ATO as a 'criminal law-enforcement agency' under the *Telecommunications (Interception and Access) Act 1979*, for the purpose of protecting public finances from serious criminal activities such as major tax fraud.

Australian Transaction Reports and Analysis Centre (AUSTRAC)

3.35 AUSTRAC has a central role as regulator for the purposes of the *Financial Transaction Reports Act 1988* (FTR Act) and the AML/CTF Act.[23] This section examines AUSTRAC's role as lead agency with respect to money laundering and terrorism financing. Criticisms of AUSTRAC's role in financial sector regulation are examined in Chapter 4.

3.36 AUSTRAC's submission notes that as Australia's AML/CTF regulator it is responsible for monitoring the compliance of its 'regulated population', and takes enforcement action 'where necessary in relation to breaches of the [AML/CTF Act].'[24]

22 See: paragraphs 3.6–3.7.

23 AUSTRAC, *Submission 10*, p. 4.

24 AUSTRAC, *Submission 10*, p. 4.

3.37 AUSTRAC submitted that it plays a key role in analysing transaction reports and producing financial intelligence products for 41 domestic revenue, law enforcement, national security, human services, regulatory and Commonwealth, state and territory partners in Australia.[25]

3.38 The effectiveness of Australia's AML/CTF regime was outlined by AUSTRAC, which argued:

> AUSTRAC's financial intelligence contributes to multi-agency investigations that target money laundering and tax evasion criminal networks, in addition to a range of predicate crimes such as drug trafficking, fraud, identity crime, people smuggling and national security matters.[26]

CTF/AML legislation and review

3.39 The committee heard evidence that the establishment of the AML/CTF Act had resulted in a regulatory regime that effectively detected and deterred terrorism-financing and money laundering. The Act is currently under review by the AGD as outlined below at paragraph 3.46.[27]

3.40 The operation of the Act includes the five key obligations imposed on reporting agencies:

1. **Enrolment**: all regulated entities need to enrol with AUSTRAC and provide enrolment details as prescribed in the AML/CTF Rules.
2. **Conducting customer due diligence**: regulated entities must verify a customer's identity before providing the customer with a designated service. Regulated entities must carry out ongoing due diligence on customers, and enhanced customer due diligence on high-risk customers.
3. **Reporting**: reporting entities must report suspicious matters, certain transactions above a threshold and international funds transfer instructions.
4. **Developing and maintaining an AML/CTF Program**: reporting entities must have, and comply, with AML/CTF programs which are designed to identity, mitigate and manage the money laundering or terrorist financing risks a reporting entity may face.
5. **Record keeping**: Reporting entities must take and retain certain records (and other documents given to them by customers) for seven years.[28]

3.41 The AGD submitted that the AML/CTF Act was 'a major step in bringing Australia into line with the Financial Action Task Force (FATF) standards and was

---

25 For the purposes of the AML/CTF Act, these are referred to as designated agencies; See also: AUSTRAC, *Submission 10*, p. 4.

26 AUSTRAC, *Submission 10*, p. 1.

27 AGD, *Submission 9*, p. 20.

28 AGD, *Submission 9*, p. 10.

developed in close consultation with industry and other interest groups.'[29] Further examination of the FATF is found from paragraph 3.50.

3.42 Both the AML/CTF Act and regulations[30] establish a risk based approach, with certain risk management strategies in place.[31] AUSTRAC argued that as the AML/CTF regulator, it monitors the compliance of the regulated population and takes enforcement action where necessary.[32]

3.43 The committee heard evidence relating to the effective prevention of money laundering operations through the AML/CTF arrangements. The AGD noted that money laundering is not a victimless white collar crime, but:

> ...an essential component of the ability of criminals to profit from highly damaging crimes like fraud, drugs and firearms trafficking, identify theft and cybercrime. Money laundering has the potential to threaten the integrity of our financial system, funds further criminal activity including terrorism, and ultimately impacts on community safety and wellbeing.[33]

3.44 As at 1 April 2014, AUSTRAC had a 'regulated population' of approximately 13 900 reporting agencies, broken into four categories: banks and other lenders; non-bank financial service providers; gambling and bullion services; and money service businesses and remittance dealers.[34]

3.45 AUSTRAC noted there was scope for the expansion of the 'regulated population' of non-financial businesses and professions, including lawyers and accountants, real estate agents, trust and company service providers, as well as precious metal and stone dealers.[35]

3.46 The AGD detailed the requirement within the AML/CTF Act to review the Act, Rules and Regulations within seven years of the Act's commencement.[36] On 4 December 2013, the Minister for Justice, the Hon Michael Keenan MP, announced a review of the regime pursuant to the Act:

> The review will cover a range of issues including: the objects of the AML/CTF Act; the risk-based approach and better regulation; regime scope; harnessing technology to improve regulatory effectiveness; industry supervision and monitoring; enforcement; reporting obligations; secrecy and access; privacy and record keeping; and international cooperation.[37]

---

29 AGD, *Submission 9*, p. 10.

30 See: Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 No. 1.

31 AGD, *Submission 9*, p. 10.

32 AUSTRAC, *Submission 10*, p. 5.

33 AGD, *Submission 9*, p. 5.

34 AUSTRAC, *Submission 10*, p. 27.

35 AUSTRAC, *Submission 10*, p .41.

36 *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, s 251.

37 AGD, *Submission 9*, p. 20.

3.47 The AGD website notes that public submissions for consultation on the current review closed on 28 March 2014, and that industry roundtables will be held in 2014 and 2015. It is understood that the roundtable consultations will focus on substantive issues raised in submissions to the review.[38]

3.48 To date, the review has received 51 public submissions.[39] The website also notes that 'further roundtables with remaining industry sectors will be held in 2015.'[40]

3.49 No further information on a timeline for the conclusion of the review is available from the AGD website.

Financial Action Task Force

3.50 The statutory review of the AML/CTF Act, as outlined above, is relevant to the ongoing relationship between the Australian Government and the FATF, especially given the FATF's role in providing advisory reports on members' implementation of AML/CTF reforms.

3.51 The AGD submitted that the establishment of the FATF by the Group of Seven (G7) in 1989, and its subsequent expansion post-September 11, had strengthened efforts to combat money laundering and terrorism–financing:

> The main objectives of the FATF are to set global standards and to promote effective implementation of legal, regulatory and operational measures to fight money laundering, terrorist financing and other related threats to the integrity of the international financial system.[41]

3.52 Australia is a founding member of the FATF, with the AGD Secretary, Mr Roger Wilkins, becoming president of the group in July 2014 for a 12 month term.[42]

3.53 The FATF works to ensure an internationally coordinated approach to combating financial crime. Its work has been encouraged by the United Nations Office on Drugs and Crime (UNODC), the IMF and the World Bank.[43]

---

38 AGD, *Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, www.ag.gov.au/consultations/pages/StatReviewAntiMoneyLaunderingCounterTerrorismFinActCth2006.aspx (accessed 5 June 2015).

39 AGD, *Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, www.ag.gov.au/consultations/pages/StatReviewAntiMoneyLaunderingCounterTerrorismFinActCth2006.aspx (accessed 5 June 2015).

40 AGD, *Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, www.ag.gov.au/consultations/pages/StatReviewAntiMoneyLaunderingCounterTerrorismFinActCth2006.aspx (accessed 5 June 2015).

41 AGD, *Submission 9*, p. 7.

42 AGD, *Submission 9*, p. 8.

43 AGD, *Submission 9*, p. 8.

FATF review of Australia's regulatory regime

3.54 The FATF regularly publishes report cards that examine member countries' regulatory arrangements with respect to their international AML/CTF obligations. On 21 April 2015, the FATF published a review of regulatory arrangements in Australia, suggesting there was room for improvement within Australia's AML/CTF regime: 'Australia has a mature regime for combating money laundering and terrorist financing, but certain key areas remain unaddressed...'[44]

3.55 The FATF's review noted:

> While Australia regulates its major money laundering and terrorism financing channels, such as banking, remittance and gaming, it should improve supervision of its regulated sectors. Most designated non-financial businesses and professions (DNFBPs) are still not subject to anti-money laundering/counter-terrorist financing (AML/CTF) requirements and have insufficient understanding of their risks. These include real estate agents and lawyers, which the authorities assessed as high risk for money laundering and terrorist financing. The report concludes that Australia should do more to demonstrate that they are improving AML/CTF compliance by reporting entities and that they are successfully discouraging criminal abuse of the financial and DNFBP sectors.[45]

Committee view

3.56 As outlined above, the FATF's support for an expanded AML/CTF framework is an important consideration for whether the 'second tier' professions, like lawyers, real estate agents and accountants should be included in an expanded AML/CTF regime.

3.57 The committee strongly supports Australia's history of participation in the FATF, and its efforts to combat money laundering and terrorism financing through the AML/CTF Act.

3.58 The committee also supports the FATF's review finding that the government needs to examine whether the 'second tier' professions ought to be included in the AML/CTF regime. The committee notes the ongoing AML/CTF Act review process. In the committee's view this is a suitable mechanism for the consideration of the expansion of Australia's AML/CTF arrangements to include 'second tier' professions.

---

44 FATF, *Australia has a mature regime for combatting money laundering and terrorist financing, but certain key areas remain unaddressed, says FATF*, www.fatf-gafi.org/documents/news/australia-mature-regime-to-combat-money-laundering-terrorist-financing-key-areas-remain-unaddressed.html (accessed 23 June 2015).

45 FATF, *Australia has a mature regime for combatting money laundering and terrorist financing, but certain key areas remain unaddressed, says FATF*, www.fatf-gafi.org/documents/news/australia-mature-regime-to-combat-money-laundering-terrorist-financing-key-areas-remain-unaddressed.html (accessed 23 June 2015).

Recommendation 4

3.59 The committee recommends the Government consider the extension of the AML/CTF regulations to cover 'second tier' professions in the current *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* review.

Expansion of the ACC Board

3.60 One question that was raised during the inquiry was whether or not the composition of the ACC Board should be altered by including AUSTRAC as a full board member.

3.61 ASIC submitted that as an original member of the ACC Board, it has seen the nature of serious and organised crime change and become increasingly sophisticated. ASIC noted that ACC Board members have all been consulted on whether full participation by AUSTRAC should occur:

> As a Board member, the ASIC Chairman was, along with the other Board members, asked to consider the staged inclusion of AUSTRAC on the Board of the ACC. In early 2015, the Chairman supported the resolution to seek the approval of the Inter-Governmental Committee - ACC to begin the process of admitting the AUSTRAC CEO to the ACC Board and agreed to allow the AUSTRAC CEO to attend as a non-voting observer, until such time as the *Australian Crime Commission Act 2002* can be amended to include AUSTRAC as a member of the Board.[46]

3.62 ASIC supports AUSTRAC's evolution and increasing active involvement in law enforcement intelligence operations, as well as its full membership on the ACC Board.[47]

3.63 The question of whether the inclusion of AUSTRAC on the ACC Board would enhance the relationship between the ACC, partner agencies and AUSTRAC, was also raised by Mr Chris Dawson, CEO of the ACC. Mr Dawson contended that significant benefits would arise for law enforcement and the intelligence community through the inclusion of AUSTRAC on the ACC Board.[48]

3.64 The AGD agreed with the ACC, suggesting it was 'a great idea to have AUSTRAC on the ACC Board.'[49]

Committee view

3.65 The committee notes the views of the AGD, ACC and ASIC on the inclusion of AUSTRAC as a full member of the ACC Board.

---

46 ASIC, *Answers to Questions on Notice*, p. 5.

47 ASIC, *Answers to Questions on Notice*, p. 5.

48 Mr Chris Dawson APM, Chief Executive Officer, Australian Crime Commission, *Committee Hansard*, 10 September 2014, p. 7.

49 Mr Iain Anderson, First Assistant Secretary, Criminal Justice Division, Attorney-General's Department, *Committee Hansard*, 10 September 2014, p. 33.

3.66 The committee agrees that AUSTRAC's presence on the ACC Board as a full member would greatly benefit both AUSTRAC and the ACC.

Recommendation 5

3.67 The committee recommends the government introduce amendments to the *Australian Crime Commission Act 2002* to enable AUSTRAC to become a full member of the ACC Board.

Chapter 4

Issues affecting the financial services, remittance and self-managed superannuation sectors

4.1 The committee received evidence relating to the licensing and registration issues facing actors within the financial services sector. While many witnesses agreed that law enforcement agencies were working effectively in deterring financial related crime, some in the finance sector criticised aspects of the law enforcement framework, arguing that significant changes are required.

4.2 This chapter examines regulatory issues from the perspective of financial services providers, and focuses on several areas, including:

- the regulatory environment monitored by ASIC and the questions of disproportionate penalties for registered and unregistered entities;
- questions about ASIC's willingness to take regulatory action against 'live scams';
- registration under the AML/CTF regime, and criticism of AUSTRAC's positioning within the sector as a law enforcement agency;
- criticism of perceived unwillingness of AUSTRAC to take regulatory action and the significant remittance industry 'de-banking' issue;
- risks arising from the IVTS; and
- risks to the self-managed superannuation sector.

4.3 An ongoing theme of the evidence was the perception that the financial services sector registration and licencing regime policed by ASIC was inadequate and unfair, and that ASIC ignored the greater risks posed by unregistered and unlicensed operators. While AUSTRAC's role as regulators has been discussed in Chapter 3, this chapter will examine instances where ASIC and AUSTRAC have used, or attempted to use, their regulatory powers to prevent financial related crime.

Registration by ASIC

4.4 There are two significant issues that were raised with reference to ASIC and its management of its regulatory responsibilities. The first relates to the penalties applied to non-compliance by licensed operators compared with penalties imposed against unlicensed operations. The second relates to ASIC's ability to use its regulatory powers to intervene in ongoing scams in a digital environment, especially when peak bodies and banks have directly contacted ASIC requesting its intervention. These two issues are addressed below.

4.5 Some submitters were critical of aspects of the financial services sector regulations, as well as the role of ASIC itself. The National Credit Providers

Association[1] (NCPA), for example, questioned a regulatory regime wherein licensed operators are penalised more than illegal unlicensed operators.

4.6 ASIC submitted that, as the financial services regulator, it has a responsibility to administer the Australian Financial Services (AFS) licensing regime and 'monitor financial services business to ensure that they operate efficiently, honestly and fairly.'[2]

4.7 ASIC noted its role as a primary law enforcement agency in the fight against financial crime, through its regulation of Australian companies, financial markets, financial services organisations and professionals. ASIC submitted that combatting financial crime was a key part of its role as a regulator:

> Given that financial markets and large pools of savings will attract those with criminal intent, combatting financial crime is a key part of our remit. Where we detect serious misconduct that is intentional, dishonest or highly reckless, we may take criminal enforcement action.[3]

Australian Financial Services Licenses

4.8 ASIC is responsible, under the ASIC Act, for the regulation and licensing of businesses engaged in consumer credit activities, including banks, credit unions, finance companies, and mortgage and finance brokers.[4]

4.9 ASIC is also the corporate regulator which is responsible for ensuring that companies, schemes and related entities meet their obligations under the *Corporations Act 2001*. ASIC registers and regulates corporations at every point, from their incorporation through to their winding up. ASIC is also responsible for ensuring that company directors comply with their responsibilities under the ASIC Act:

> Directors, company officers, auditors, liquidators and market participants play a key role in ensuring that Australia's financial markets are fair and efficient. We take enforcement action against these gatekeepers to promote fair and efficient financial markets.[5]

Penalty regime

4.10 Some submitters, including the NCPA, argued that registered operators who inadvertently breached the AFS regulations (regulated by ASIC) through incorrect legal advice or interpretation would be penalised significantly more than an unlicensed operator. The NCPA suggested that this effectively creates incentives to act as unlicensed operators:

---

1 Please note, the NCPA was previously known as the National Financial Services Federation. Its original name is used for its submission and in the *Hansard* transcripts. The committee attributes this evidence to the NCPA throughout this report.

2 ASIC, *Submission 21*, p. 3.

3 ASIC, *Submission 21*, p. 2.

4 ASIC, *Submission 21*, p. 3.

5 ASIC, *Submission 21*, p. 5.

> The penalty for unlicensed activity, if someone is caught…is one penalty unit for unlicensed activity. The legislation says that you will be fined this amount of money. However, a licensed lender who is doing the right thing and who may unintentionally get it wrong through incorrect legal advice or incorrect interpretation can be fined many times that single penalty unit, even though they are licensed and attempting to do the right thing. We say that the penalty for unlicensed activity needs to be many times that of what an entity trying to do the right thing can be fined.[6]

4.11 The NCPA was also critical of the original policy development of the *National Consumer Credit Protection Act 2009* (NCCP Act), arguing that it was underpinned by incorrect assumptions that would cause significant ongoing issues and result in penalties that cannot adequately discourage unlicensed activities:

> The original Treasury policy development for the NCCP Act 2009 incorrectly assumed that all lenders would apply for and obtain a licence and hence comply with the new Act. As a result, the penalties for unlicensed activity are manifestly inadequate to discourage unlicensed activities.
>
> It appears that the 'prime directive' for the regulator (ASIC) is to focus on the licensed lenders (who are continually bending over backwards to comply with the law) and not the illegal unlicensed entities which were in, or have entered, the market.[7]

4.12 Further, the NCPA argued that because the core objective of the NCCP Act was to ensure ASIC's focus remained on monitoring and reviewing licensed activities, penalties in the Act also focus on breaches of licensed activities as opposed to unlicensed activities.[8] The NCPA insisted that the current regulatory regime was too onerous for licensed lenders, and that businesses attempting to follow regulations could be shut down for minor non-compliance issues:

> Civil and Criminal penalties are now so onerous for licensed lenders complying with the Act for responsible provision of consumer credit that Australian Credit License holders dare not operate outside the Act.
>
> Further-more, after spending ten's, sometimes hundreds of thousands of dollars to gain an Australian Credit License, lenders may have their business shut down for non-compliance. The "incentive" for licensed lender to do the right thing cannot be overstated.[9]

4.13 Finally, the NCPA noted that the maximum penalties for licensed lenders for non-compliance was a $340 000 penalty, in addition to a criminal penalty of up to 200

---

6 Mr Philip Johns, Chief Executive Officer, National Financial Services Federation, *Committee Hansard*, 9 September 2014, p. 22.

7 National Financial Services Federation, *Submission 3*, p. 6.

8 National Financial Services Federation, *Submission 3*, p. 6.

9 National Financial Services Federation, *Submission 3*, p. 6.

penalty units ($34 000) with up to 2 years imprisonment. Conversely, the same maximum penalty applies to unlicensed activities.[10] The NCPA argued:

> In all cases penalties for unlicensed activity should be many times that of those who go to the trouble of applying for a licence and becoming licensed, but who may fall foul of the law.[11]

Committee view

4.14 The committee is concerned that the evidence presented by the NCPA demonstrates disparities within the current financial services licensing and registration system regulated by ASIC. This imbalance is highlighted by the example of the maximum penalty for non-compliance by licensed operators being equal to the maximum penalty for providing unlicensed services. The committee agrees that this has the potential to incentivise unlicensed activities, which in the committee's view should be discouraged as such activities can be used to perpetrate financial scams.

4.15 In this regard the committee notes a recent recommendation of the Senate Economics References Committee 'that the government commission an inquiry into the current criminal and civil penalties available across the legislation ASIC administers.'[12]

Recommendation 6

4.16 The committee recommends that the government review the penalties prescribed under financial services legislation administered by ASIC, with a view to achieving a better balance between non-compliance by licensed operators and unlicensed operations.

ASIC's response to 'live' scams

4.17 The NCPA was especially critical of ASIC's reaction to reports of a scam that misused a member's AFS Licence information. The NCPA extensively detailed the scam that was reported to ASIC for investigation:

> On the day I [Mr Philip Johns, Chief Executive Officer, National Financial Services Federation] found out about it, we…informed by email the ASIC credit team in Sydney. Our organisation lodged on behalf of our member. We called ASIC and reported it via their complaint line. We also send the details of the scam to the ASIC email address: feedback@ASIC.gov.au. We informed our members of the mechanics of the scam. That was on day zero as far as we were concerned. Three days later, the second member reported the same scam. Again, details were sent to ASIC regarding that. On day 3, because the information we had was live data—it had the actual Commonwealth Bank BSB, the account number, the account name and what appeared to be local phone numbers, I passed the information on to

10 National Financial Services Federation, *Submission 3*, p. 6.

11 National Financial Services Federation, *Submission 3*, p. 7.

12 Senate Economics References Committee, *The performance of the Australian Securities and Investments Commission*, June 2014, Recommendation 41, p. xxxi.

> the Australian Bankers' Association, who assigned a person to assist with this. The ABA contacted the Commonwealth Bank to give them notice that these couple of accounts were being used in the scam. I am not sure of the time line the Commonwealth Bank shut that down. On day 6…ASIC rang one of our members and sent an email with receipt of what they called 'concerns received'. From our point of view, it was not concerns; this was hard, cold factual information, including the BSB and account number, of where consumers were depositing money with regard to this scam. That email on day 6 was to set up a teleconference further down the track for the investigators to talk to the members and me.
>
> On day 18, I got an email from the ABA saying he had been advised by ASIC that they had been aware of this type of scam since July. So it had run from July to November before one of our members had picked it up, but ASIC had been aware of it since July. We showed our members the tools on how to scan the internet to see whether their logos, names, licence numbers were being used by other entities on the net. Then a third member picked up their live Australian credit licence number and details being used in a scam. That was also sent to ASIC. On day 101 after we made contact with ASIC, ASIC issued media release 14-040, but, based on the information we got from the ABA, this public warning notice—and it was titled 'ASIC warns Australian borrowers about overseas lending scam'—was 223 days after ASIC supposedly became aware of the issue, which goes to the crux of what we tried to highlight in [our submission].
>
> I had a fairly frank conversation with one of the investigators, who said that basically ASIC (1) does not have the technology to try and track down these scams, (2) does not have the resources to do this and (3) the processes of natural justice, of deciding whether this even falls within ASIC's gamut to investigate then allowing all this, appear to be based…on paper, fax and letter-type dealing with the process rather than the fact that we are in a global economy and these scams are over and done with very rapidly. And they can scam thousands of details very quickly once they are up and running. So that is the time line, and this is why it is a concern.[13]

4.18 The committee subsequently provided this example to ASIC for comment, noting the significant delay in regulatory action when detailed information of the scam had been provided so promptly. In answers to *Questions on Notice* ASIC explained:

> ...in line with our approach to disrupt scams and protect consumers, ASIC determined that the most appropriate regulatory response in the circumstances was to issue a media release to educate members of the public and to disrupt the scam. Following this, ASIC published 14-040MR *ASIC warns Australian borrowers about overseas lending scam* on 10 March 2014 which was in fact about 137 days after ASIC first became aware of the issue.[14]

13 Mr Philip Johns, Chief Executive Officer, National Financial Services Federation, *Committee Hansard*, 9 September 2014, pp 23–24.

14 ASIC, *Answers to Questions on Notice*, p. 4.

Committee view

4.19 The committee is concerned about ASIC's response to the scam against NCPA's members for three reasons. Firstly, whether it took ASIC 223 days or 137 days to respond to the active scam detailed above, the committee considers ASIC's response was extremely tardy. The committee acknowledges that this incident may be an aberration, and may not be representative of ASIC's usual response timeframe. However, on the evidence before the committee, this does not appear to be the case, as ASIC was invited to respond directly to the issue and its response did not contend that this was an isolated incident.

4.20 Even if it is assumed that ASIC's typical handling time is twice as fast as its reaction in this example, the implication is that ASIC's response, from the day it becomes aware of these sorts of financial related crimes, is between 65–110 days. At best this is equivalent to more than 2 months, at worst nearly 4 months.

4.21 As many witnesses have observed, the use of modern technologies makes the transacting of internet scams incredibly rapid. If ASIC is to deal with internet-based financial related crimes in an effective manner into the future, it must improve its response times to preventing and disrupting such criminal activities.

Recommendation 7

4.22 The committee recommends that ASIC consider and then implement mechanisms to make its response to internet-based financial related crimes far more expeditious.

4.23 In this regard the committee notes several recent recommendations of the Senate Economics References Committee in relation to ASIC's complaints handling process.[15]

4.24 The committee also notes the government's response, which states that ASIC 'will undertake a formal review of its complaints management processes in 2016 to ensure that the improvements it has made have led to a more effective handling of alleged misconduct reports.'[16] As part of this formal review, the committee expects ASIC to examine whether a scam, such as the one raised by the NCPA, would be dealt with more effectively and expeditiously through ASIC's improved complaint handling processes.

4.25 The committee's second concern raised by the NCPA evidence is that ASIC's primary action, when presented with details of an active scam, was to issue a press release. In the committee's view ASIC's response by media release does not send a sufficiently robust deterrence message to future internet scammers.

4.26 Mr Johns' account of his discussion with an ASIC investigator raises questions for the committee about ASIC's technological capacity to detect and monitor

---

15 Senate Economics References Committee, *The performance of the Australian Securities and Investments Commission*, June 2014, Recommendations 18–20, pp xxvi–xxvii.

16 Government response, Senate Economics References Committee, *The performance of the Australian Securities and Investments Commission*, (October 2014).

financial related crimes. Critically, the government and the Parliament must be assured that ASIC has the technological capacity to effectively and appropriately deploy its regulatory powers. For this reason the committee recommends an audit of ASIC's technological capabilities.

Recommendation 8

4.27 The committee recommends that the Australian National Audit Office conduct a performance audit of ASIC's technological capacity, and provide a report to the Parliament outlining ASIC's technological requirements and capabilities, and the extent to which any deficiencies may hamper ASIC's regulatory responsibilities.

4.28 The committee is of the view that ASIC needs to build stronger partnerships with the private sector to more effectively interact with relevant organisations to detect and deter financial related crimes. The NCPA's example shows how the intervention by the Australian Bankers' Association prompted action by the Commonwealth Bank to close down the sham accounts. In the committee's view, ASIC should have taken similar action as soon as it became aware of the internet scam.

Recommendation 9

4.29 The committee recommends that ASIC strive to improve its relationships with the private sector in order to better detect and deter financial related crimes.

Registration by AUSTRAC

4.30 Similar to the criticisms detailed above of ASIC, AUSTRAC was also criticised for not taking strong enough compliance action against operators who were not discharging their obligations under the AML/CTF regime, or complying with AUSTRAC's instructions.

4.31 One concern raised by independent remitters was that penalties were poorly targeted, and that licensed operators were often punished more severely than unlicensed operators, who faced little or no financial penalty.

4.32 AUSTRAC's submission discussed the detection of Australian-based remittance services that had been used to launder money. While AUSTRAC did not disclose the proportion of businesses that are engaged in money laundering, it did suggest that:

> ...law enforcement agencies have detected cases where Australia-based remittance businesses are used as a third party to move funds or settle transactions involving two or more foreign countries. Similar to cuckoo smurfing, this involves overseas-based remittance dealers accepting legitimate transfer instructions from innocent parties (for example, to import or export goods) but instead of conducting the transfer themselves they send instructions to Australian counterparts. This is common practice among alternative remittance businesses, as part of their routine settlement of debts, to ease cash flow constraints or take advantage of foreign exchange differences.

> However, some Australian remittance dealers have exploited this opportunity to launder cash from Australian organised crime by transferring it to recipients overseas. Likewise, the overseas remittance dealers supply 'clean' cash to overseas-based crime groups with links in Australia.[17]

4.33 AUSTRAC noted that it was able to impose civil penalties against reporting agencies when they failed to take reasonable steps to comply with their obligations as set out in the AML/CTF Act and associated regulations:

> AUSTRAC has increased its enforcement action since the commencement of the AML/CTF Act in 2006. Most of the obligations under the AML/CTF Act did not come into effect until two years after its commencement, at which time reporting entities were subject to a two-year Policy (Civil Penalty Orders) Principles period. This meant that AUSTRAC could initiate civil penalties against reporting entities only when the entities had failed to take reasonable steps to comply with their obligations. AUSTRAC was well placed, as a result of strengthening its enforcement capability, to take action when non-compliance was identified and the full suite of powers came into effect from 2008.[18]

4.34 To minimise the high risks associated with the remittance sector in general, AUSTRAC noted that changes were enacted to the AML/CTF Act in 2011 to both strengthen the registration requirements for remitters, and to enhance the AUSTRAC CEO's powers to deal with compliance issues.[19]

4.35 While representatives of the independent remittance sector acknowledged that the sector is deemed high risk, they noted that since 2012, many previously unregistered operations had subsequently registered with AUSTRAC.[20]

4.36 AUSTRAC has to date used these new powers (to refuse, suspend or cancel registration) only once. However, it noted that it had placed conditions on the registration of numerous agencies (15 instances as at May 2014), as well as imposing significant financial penalties on remittance network providers for failing to register affiliates and providing services through unregistered affiliates.[21]

4.37 Independent remitters suggested that current regulatory arrangements were not sufficient to deter unregistered remittance operators. Further, they argued that it may be easier for an unregistered remitter to operate than previously:

---

17 AUSTRAC, *Submission 10*, p. 13.

18 AUSTRAC, *Submission 10*, p. 27.

19 AUSTRAC, *Submission 10*, p. 13.

20 Ms Dianne Nguyen, Head of Compliance, Eastern & Allied Pty Ltd, *Committee Hansard*, 9 September 2014, p. 28.

21 AUSTRAC, *Submission 10*, p. 13.

> We have a subset of unregistered remitters now. If the registered remitters …close up shop, and a new flurry of unregistered remitters will come to fill the space that the registered remitters [occupied]…[22]

4.38 AUSTRAC's detractors noted that there was evidence to suggest that unregistered remitters could, and were still, operating effectively without the real threat of regulatory action by AUSTRAC.[23]

4.39 AUSTRAC countered that there was a degree of regulatory engagement with unregistered remitters, citing *Taskforce Eligo (Eligo)* (as discussed in Chapter 3) as an example. AUSTRAC argued that together with other law enforcement agency partners, it is detecting and engaging with unregistered remitters:

> With unregistered remitters, it would not be true to say there is no regulatory engagement with them. You will have heard detailed information, I think, from some of the earlier witnesses about Taskforce Eligo, for example, where we are working with the Australian Crime Commission and others. AUSTRAC, as part of that work, has identified people who have been unregistered.[24]

4.40 In response to criticism of AUSTRAC's engagement of unregistered remitters, AUSTRAC's former CEO, Mr John Schmidt, noted that as at September 2014, there had been prosecutions for some entities that were engaged in criminal behaviour, but that these were in concert with the ACC as part of *Eligo*:

> We do not prosecute. We are the law enforcement agency. So, to the extent that there is a breach of the criminal law, which is a criminal offence, that would be a matter for law enforcement. [25]

4.41 Critically however, Mr Schmidt did note that he was not aware of any prosecutions for 'being unregistered in itself', and noted that unregistered remitters who had been identified had been prosecuted for other (possibly related) criminal activities:

> I am not aware of a prosecution for being unregistered in itself. Having said that, unregistered remitters who have been identified as being engaged in criminal activity have been prosecuted by law enforcement for some of their criminal activities. Now, I cannot tell you, based on that analysis, who would have been potentially liable for prosecution for being unregistered.[26]

---

22 Ms Dianne Nguyen, Head of Compliance, Eastern & Allied Pty Ltd, *Committee Hansard*, 9 September 2014, p. 34.

23 Ms Dianne Nguyen, Head of Compliance, Eastern & Allied Pty Ltd, *Committee Hansard*, 9 September 2014, p. 31.

24 Mr John SCHMIDT, Chief Executive Officer, Australian Transaction Reports and Analysis Centre (AUSTRAC), *Committee Hansard*, 9 September 2014, p. 48.

25 Mr John SCHMIDT, Chief Executive Officer, Australian Transaction Reports and Analysis Centre (AUSTRAC), *Committee Hansard*, 9 September 2014, p. 48.

26 Mr John SCHMIDT, Chief Executive Officer, Australian Transaction Reports and Analysis Centre (AUSTRAC), *Committee Hansard*, 9 September 2014, p. 48.

Committee view

4.42 The points of contention between the disproportionality of regulatory actions against registered and unregistered remitters also feeds into the broader challenges faced by the independent remittance industry. While apparently not on the same scale as the financial services industry (and the aforementioned licensing and penalties issue), the committee agrees that the discrepancies in evidence from remitters and regulators warrants further investigation.

4.43 The committee notes that pressures on the remittance industry, including the 'de-banking' issue (discussed below) could result in a higher use or dependence on unregistered remitters.

4.44 The committee is concerned that, like ASIC, AUSTRAC is not as expeditious in moving against unregistered remitters as it ought to be. The committee believes that AUSTRAC should take a more proactive role in detecting and engaging unregistered remitters.

Recommendation 10

4.45 The committee recommends that AUSTRAC consider and then implement mechanisms to increase its regulatory oversight of the activities of unregistered remitters.

Remittance industry 'de-banking'

4.46 The committee heard from both independent and commercial remittance service providers about ongoing regulatory issues in the sector. Specifically, independent remitters argued that they were being disadvantaged by major commercial banks for two primary reasons.

4.47 Firstly, it was alleged that the major Australian banks were using changes to international anti-money laundering and counter terrorism financing arrangements to justify the closure of remitters' Australian operating bank accounts.

4.48 Secondly, it was claimed that the same major Australian banks were doing so while still offering their own remittance services, for possibly anti-competitive reasons.

4.49 The committee took these allegations extremely seriously, and heard from both the independent remittance sector and major Australian banks and the Australian Bankers Association (ABA) about this significant issue.

Account closures

4.50 Over the course of the inquiry the committee heard from numerous witnesses that the closure of remitters' bank accounts by major Australian banks was having a detrimental effect on the independent remittance industry. These concerns were first raised by representatives of the remitters' industry association, the Australian Remittance and Currency Providers Association, who argued that independent remittance services were being disadvantaged by the closure of their operating bank accounts.

4.51 Mr Crispin Yuen, Head of Compliance at Ria Financial Services Australia Pty Ltd, outlined the impact of the 'de-banking' of remittance businesses:

> Most of the major banks have decided to not bank remittance business, resulting in remittance business not having bank accounts with which to operate. This is now a pressing issue, because a business without a bank account cannot operate, and three of the four major banks have already said no. The Australian Federal Police and the Australian Crime Commission have real issues about the impact of these transactions going underground and being done by private arrangement in an unregulated, unreported way if the sector loses its banking relationships.[27]

Banks' response

4.52 The affected remitters argued that as they were complying with AUSTRAC's regulations they should not be 'de-banked'.[28] The committee invited Australia's four largest commercial banks to respond to the issues raised by the independent remittance sector.

4.53 In correspondence to the committee, Westpac indicated that domestic and international banks are finding it increasingly difficult to provide banking and payment services to remittance operators due to the Australian and international regulatory landscape and the compliance requirements in the banking industry.[29]

4.54 Westpac directed the committee to an ABA blog that summarised some of the key challenges, including that the anti-money laundering scheme in Australia which requires banks to 'know your customers'.[30]

4.55 The ABA blog outlines the domestic and international constraints the ACL/CTF requirements place on Australian banks:

> Australian banks often use overseas banks (usually in the US, UK, and EU as these are the preferred currencies) to facilitate these transactions and the law requires all banks in the value chain to meet regulatory obligations, including risk management to prevent money laundering/terrorism financing and adhere to sanctions across multiple jurisdictions. The expectation of overseas regulators and clearing banks is that international transfers represent transparency, knowing your customer, your customer's customer and who the beneficiaries are. This is not always possible and Australian banks need to take great steps not to breach both foreign and domestic law, including laws on anti-money laundering, counter terrorism financing and sanctions.

---

27 Mr Crispin Yuen, Head of Compliance, Ria Financial Services Australia Pty Ltd, *Committee Hansard*, p. 28.

28 Mr Crispin Yuen, *Committee Hansard*, 9 September 2014, pp 28–29.

29 Westpac, *Correspondence*, p. 1, (2 February 2015).

30 ABA, *The risks of remittances*, www.bankers.asn.au/Media/ABA-Blog/Blogs/The-risks-of-remittances (accessed 29 April 2015).

> Failure to do so could result in any Australian bank that, even unknowingly, violated these laws to be instantly cut off from access to the US, UK or EU financial system, including significant regulatory action and fines which would have a devastating impact on the Australian banks and economy.
>
> Therefore, banks in Australia are assessing the risks of using remittance operators and companies, and in some cases choosing to cease providing services to ensure they do not breach international laws.[31]

4.56 In light of the requirements of financial institutions internationally, Westpac had decided 'that like most Australian banks we are not generally in a position to provide banking services to remittance businesses.'[32]

4.57 Westpac acknowledged that the account closures would affect the independent remittance industry, as well as the businesses and remittance providers that use their services.[33]

Class action by remitters

4.58 Westpac's correspondence also detailed a class action brought against it in November 2014 by a group of remitters. The action was initiated by the remitters in order to reinstate their accounts until alternative finance facilities could be found:

> The class action sought to require Westpac to provide more time to enable remitters to seek alternative banking services. In December [2014], Westpac reached an in principle agreement to settle the class action and this was approved by the Federal Court on 5 January 2015.[34]

4.59 Westpac explained that part of the settlement included keeping banking facilities open until 31 March 2015, 'to allow those customers time to make alternative banking arrangements before...services cease after that date.'[35]

Attorney-General's Department's working group

4.60 Westpac advised the committee that the government has established a working group chaired by AGD and including associated parties (regulators, banks and remittance industry associations) 'to see what longer-term solutions may be possible to support and help make such [remittance] payments in the future.'[36]

4.61 As at 23 June 2015, there is no information available on the progress of the working group, other than indications that its work is ongoing.

---

31 ABA, *The risks of remittance*s, www.bankers.asn.au/Media/ABA-Blog/Blogs/The-risks-of-remittances (accessed 29 April 2015).

32 Westpac, *Correspondence*, p. 1 (2 February 2015)

33 Westpac, *Correspondence*, p. 1, (2 February 2015).

34 Westpac, *Correspondence*, p. 1, (2 February 2015).

35 Westpac, *Correspondence*, p. 1, (2 February 2015).

36 Westpac, *Correspondence*, p. 1, (2 February 2015).

Advice from the ACCC

4.62 The committee subsequently wrote to the ACCC requesting an examination of the substantive question of whether the banks' closure of remitters' accounts amounted to anti-competitive behaviour or a misuse of market power. The ACCC was provided with copies of the committee's Hansard and related correspondence.

4.63 The ACCC's Chairman, Mr Rod Sims, responded:

> I understand that during the course of the inquiry, money remitters have raised a concern that most of the major Australian banks have stopped providing banking services to independent remittance businesses and closed their accounts.[37]
>
> You have asked whether this action may constitute anti-competitive behaviour; given the banks offer their own remittance services.
>
> Like any businesses, banks have the right to choose who they deal with and there are many reasons why a bank may legitimately refuse to supply goods or services.[38]

4.64 The ACCC noted that if the banks had acted collectively to close remitters' accounts, it would raise concerns under the cartel provisions in the *Competition and Consumer Act 2010* (the CCA).[39] The ACCC concluded that:

> …on the basis of the material available, including the Hansard transcript of the Committee's hearing, the letter from Westpac and the submission to the inquiry from the Australian Bankers' Association Inc., there is [no] suggestion that the banks have acted collectively to close remitters' accounts.
>
> Rather, the available material suggests that the major Australian banks have individually decided to stop providing banking services to independent remittance businesses as a way to individually manage their compliance risk and [to] meet their obligations under Anti-Money Laundering and Counter Terrorism Financing regulations.[40]

4.65 The ACCC remarked that if a bank had closed a remitters' account to eliminate the remitter as a competitor to the bank, it could raise concerns under section 46 of the CCA.[41] However, the ACCC noted:

> On the basis of the available material, and assuming that the major Australian banks have market power, there is no suggestion that the banks have closed remitters' accounts for an anti-competitive purpose. Instead, as noted above, it appears that the banks have individually decided to stop

37 ACCC, Correspondence, p. 1. (2 April 2015)

38 ACCC, *Correspondence*, p. 1. (2 April 2015)

39 ACCC, *Correspondence*, pp 1–2. (2 April 2015)

40 ACCC, *Correspondence*, p. 2. (2 April 2015)

41 ACCC, *Correspondence*, p. 2. (2 April 2015)

> providing banking services to independent remittance businesses in order to ensure their availability to meet their regulatory obligations.[42]

4.66 Critically, the ACCC acknowledged the importance of independent remitters to members of migrant communities in Australia, many of whom use remitter services to send money to families and friends overseas. The ACCC noted that the AGD's working group had been established to work through these issues, and offered its assistance to that process.[43]

Committee comment

4.67 The questions relating to the closure of remitters accounts are complex. In the committee's view there needs to be a suitable balance between the constraints of a robust AML/CTF regime and the ability for legitimate remittance service providers to access necessary financial products. The committee acknowledges the ongoing work of the AGD working group to find a satisfactory resolution for independent remitters' services and the communities that use them.

4.68 The committee chooses not to make any recommendations on this issue due to the ongoing considerations by the working group. The committee will monitor the groups' activities going forward, and supports a solution that takes into account the need for a robust AML/CTF regime and does not result in the closure of legitimate independent remittance service providers.

Informal Value Transfer Systems

4.69 As foreshadowed in Chapter 3, the ACC noted that *Eligo* had examined the use of the ARS and IVTS, alternatively known as Hawala, Hundi, Fei ch'ien or Phoe kuan.[44]

4.70 The ACC noted that IVTS are largely used in Australia by global diaspora communities to remit funds outside of the formal financial and banking system:

> IVTS networks represent some of the oldest and most established financial systems in the world and encapsulate a number of value transfer mechanisms that predate the modern Western notion of formal banking. Some IVTS mechanisms used today have existed as far back as 5800 BC, and include Hawala (Middle East, Afghanistan, and Pakistan), Hundi (India), Fei ch'ien (China), and Phoe kuan (Thailand). These IVTS are still in operation across the globe and are often the preferred means of transferring value in many cultures.[45]

4.71 The ACC explained that *Eligo* had been established as a result of the recognition of AUSTRAC's designation of the National Threat Assessment on Money Laundering as 'high'. The ACC Board responded in December 2012 with the establishment of *Eligo*:

---

42 ACCC, *Correspondence*, p. 2. (2 April 2015)

43 ACCC, *Correspondence*, p. 2. (2 April 2015)

44 ACC, *Submission 5*, p. 11.

45 ACC, *Submission 5*, p. 11.

> ...the ACC established Eligo to take a coordinated and collective approach against high-risk remitters and IVTS operating in Australia to reduce their adverse impact on Australia and its national economic wellbeing. The Task Force operates under the ACC's [Targeting Criminal Wealth] Determination, which allowed the ACC to utilise the full breadth of its coercive intelligence collection capabilities. The AFP and AUSTRAC were principal partner agencies involved in Eligo; however, Eligo engaged with numerous domestic and international partners...[46]

4.72 The aim of *Eligo* was to disrupt remitters and IVTS operators assessed as posing a high money laundering risk, and to implement crime prevention strategies that would optimise the use of AML/CTF regulations.[47] *Eligo* resulted in the seizure of more than $580 million in drugs and assets, including in $26 million in cash.[48]

4.73 While this is a significant success, the alternative remittance sector noted that the use of IVTS was still high among certain communities and that the effect of the closure of remitters' accounts would ultimately drive more people to use unregulated services, thus putting themselves at a great financial risk.[49]

4.74 The alternative remitters acknowledged that it was possible to operate in Australia without seeking registration, by establishing banking arrangements offshore:

> **Senator O'SULLIVAN**: Pretend I wake up one day and decide that I am going to become a remitter. I am not going to seek registration in Australia under the government's regulations here. I have just decided to establish my banking arrangements somewhere offshore. Could I function efficiently?
>
> **Mr Bieytes Corro**: Yes, you can. If you do hawala or hundi, yes, you would be able to do it. In that sense, there will not be any real money transfers happening between Australia and Hong Kong. You will just have a bank account there and a bank account here. The money is actually not being transferred. Eventually, you use the banks, if you can, to do a settlement with your counterpart on the other side—but that is unregulated.[50]

Committee view

4.75 The committee is concerned that the effect of the closure of remitters' accounts could lead to a heavier reliance on IVTS systems in some communities, potentially drawing law abiding individuals and families into the sphere of organised and serious criminal groups through a lack of financial and banking safeguards.

---

46 ACC, *Submission 5*, p. 15.

47 ACC, *Submission 5*, p. 16.

48 ACC, *Submission 5*, p. 16.

49 Mr Eduardo Bieytes Corro, Managing Director, Ria Financial Services Australia Pty Ltd, *Committee Hansard*, 9 September 2014, p. 30.

50 Mr Eduardo Bieytes Corro, Managing Director, Ria Financial Services Australia Pty Ltd, *Committee Hansard*, 9 September 2014, p. 30.

4.76 The committee recognises that many IVTS users access those services legitimately, but also acknowledges the high risks that IVTS users are exposed to, due to a lack of regulatory action by either ASIC or AUSTRAC.[51]

4.77 The committee believes that communities should be encouraged to use registered and regulated services. To this end, the committee encourages the government, through its current law enforcement arrangements, to continue to monitor the issues raised both in *Eligo* and by submitters to this inquiry in relation to IVTS.

Self-managed superannuation funds

4.78 The committee took evidence from witnesses that superannuation investments were at particular risk of financial related crime, largely because of the increased technological management of superannuation funds.

4.79 The ABA argued that self-managed superannuation funds (SMSFs) mostly sit seemingly dormant.[52] This fact provides opportunities for criminals if they can get access to the account, and a risk that any unauthorised access may be undetectable for some time. Further, the ABA discussed the increasing use of "phishing" type scams with respect to superannuation:

> That is where we are relying on our electronic detection to pick anomalous behaviour up, but it is not perfect. There are ways around it. That is one of the things that I think is a growing area, and, of course, the criminals would see this as well. They understand that people are saving money in these locations and they are sending out letters saying, 'Roll over your super into this account.' I have received several letters saying, 'This person has left employment and could you please transfer her superannuation fund to this fund.' That was for a member of my family, so I knew it was not real, but there are just phishing expeditions going on to probably all superannuation funds.[53]

4.80 The ABA noted that accountants and lawyers are not subject to current AML/CTF regulations, and referred to them as the 'weakest link' in relation to regulation of SMSFs:

> Accountants are the people who set up SMSFs and, as with any system; criminals go to the weakest link. In the AML-CTF space, the weakest link is the accountants and lawyers because they are not regulated. There is a significant amount of money going into SMSFs and, therefore, there is the potential for those investments to be exploited for that reason for money laundering rather than fraud.[54]

---

51 See Chapter 3.

52 Mr Steven York, Head of Groups Security and Business Resilience, Bank of Queensland, *Committee Hansard*, 9 September 2014, p. 2.

53 Mr Steven York, Head of Groups Security and Business Resilience, Bank of Queensland, *Committee Hansard*, 9 September 2014, p. 2.

54 Mr Paul Stacey, Policy Director, Australian Bankers' Association, *Committee Hansard*, 9 September 2014, p. 2.

4.81 AUSTRAC also raised the vulnerability of SMSFs generally, noting that a significant amount of money in Australia is invested in superannuation funds, which provides significant challenges for law enforcement agencies to monitor. AUSTRAC mentioned the effectiveness of *Task Force Galilee* led by the ACC that targeted 'boiler room scams' in which retirees were phoned and offered investment opportunities that led to significant fraud:

> Historically, one of the ways these scammers got people's names and addresses was through various share registries and other lists which were publicly available. I am not quite sure whether they are now available to the same extent that they were. They say, 'Look, we've got a fantastic investment opportunity for you.' They lure people in. They are very sophisticated. They have websites which look legitimate. Some of the more sophisticated ones would have what appeared to be genuine share trades, which made profits. So they would bait the hook. Then they would invite investors to put more and more money into these schemes or to buy particular shares, which either did not exist or were worthless. Then the money was gone. There have been a number of examples where people have lost significant amounts of funds through scams of that nature. That is a particular area of vulnerability.[55]

Committee view

4.82 The committee is concerned with the evidence that SMSFs are particularly vulnerable to financial related crime. The committee supports the important role of Commonwealth law enforcement agencies in their work monitoring and containing the risks to SMSFs from financial related crime.

4.83 The committee urges law enforcement agencies to continue to develop new and effective methods of detecting and disrupting financial frauds perpetrated against SMSFs.

55 Mr John Schmidt, Chief Executive Officer, AUSTRAC, *Committee Hansard*, 9 September 2014, p. 46.

Chapter 5

Collaboration between law enforcement and the private sector

5.1 This chapter examines the relationships between law enforcement agencies and the private sector, specifically their efforts to collaborate and share information effectively.

5.2 While this chapter examines instances of effective collaboration, there are other examples where greater cooperation between the private sector and law enforcement would have been beneficial.

Law enforcement and private sector collaboration

5.3 Numerous submitters, including the ACC, discussed the importance of the relationship between law enforcement agencies and the private sector, specifically financial institutions' role in fighting financial related crime.[1]

5.4 The ACC's traditional relationship with the private sector (including banks) has been largely legislative and transactional to date. The evolution of serious and organised crime has required law enforcement agencies, like the ACC, to work more closely with banks in a 'trusting and mutually beneficial way'.[2]

5.5 The ATO submitted that proactive engagement with industry is a critical component of its efforts in addressing the risks of taxation crime. Its submission also details the ways in which the ATO provides information to promote awareness of the risks and consequences of tax crime to the community and industry:

> A community that understands the potential damage caused by tax crime can work together to strengthen and protect the tax and superannuation systems which are important community assets.[3]

5.6 The ACC suggested that its coercive powers are immeasurably valuable in investigations, and that its intelligence products are particularly useful in collaboration with the banking sector:

> ...we are working closely with the banks in order that we can provide as much information and assistance to them without transgressing what the [Australian Crime Commission Act] provides. So in a way, because of the intelligence collection powers, the commission has to necessarily adopt a more measured, careful approach to make sure that we do not and should

---

1 ACC, *Submission 5*, p. 19.

2 Mr John Moss, Acting Executive Director, Operations, Australian Crime Commission, *Committee Hansard*, 10 September 2014, p. 1.

3 ATO, *Submission 7*, p. 7.

> not abuse the powers that the commission enjoys. It is different to the traditional policing relationship because of the exceptional powers that the commission has. But having said that, we are openly engaging with the banks. I would be further seeking to broaden the flow [of information] back to the banking sector.[4]

5.7 Victoria Police used the example of *Strike Force Piccadilly* to demonstrate effective collaboration between law enforcement agencies and the private sector. This initiative is a partnership of Victoria Police and key private sector stakeholders, for example the Shopping Centre Council of Australia, the ABA, cash-in-transit firms and the ATM industry association. Victoria Police noted that the task force has resulted in a significant reduction in 'ram' raids [on ATMs] sustained over several years, with explosive gas attacks eliminated in the first year.[5]

5.8 Despite these positive examples of public-private collaborations, South Australia Police (SAPOL) raised concerns relating to the ability of banks and law enforcement agencies to share information. SAPOL's submission notes that there were substantial delays when law enforcement agencies requested information 'from financial institutions served with banker's orders—including follow up requests for additional information and supporting affidavits.'[6] SAPOL further argued that law enforcement agencies should be allowed to set time limits for the production of information by financial institutions.

5.9 SAPOL also questioned, under the general guise of potential legislative reform, whether banking information provided pursuant to search warrants could be received electronically.[7]

5.10 Private sector submitters also raised some concerns about the degree of collaboration with law enforcement agencies. The ABA for example submitted that collaboration between banks and law enforcement was not operating as efficiently as possible, due to the inability of banks to 'contextualise' the information they pass on to law enforcement agencies. The ABA noted:

> Trusted information sharing is absolutely essential to our line of work. It is not an instinct in the Australian system, I think, because of the separation of agencies from corporate life. Corporations do employ people like us [with a law enforcement or security background] to make sure we manage it on our side, but the instinct is not sharing. It has developed. If you look at the [remittance] sector, for example, the Commonwealth has recognised that the private sector owns and operates 94 per cent or 97 per cent of Australian

4 Mr Chris Dawson, Chief Executive Officer, Australian Crime Commission, *Committee Hansard,* 10 September 2014, p. 2.

5 Victoria Police, *Submission 13*, p. 5.

6 South Australia Police, *Submission 12,* p. 4.

7 South Australia Police, *Submission 12,* p. 4.

> critical infrastructure and it has started to react accordingly; to understand and to share. But the instincts still are not there.[8]

5.11 The ABA told the committee that many banks regularly receive requests from law enforcement agencies, in addition to requests from courts and other parts of government. While willing to comply with these requests, the ABA suggested that the relationship between banks and law enforcement agencies would be enhanced if banks were able to refine the request for information contained in warrants:

> I think that sort of reform has to go through which makes it easier for us to have a discussion with law enforcement about what they need rather than having a warrant that says, 'we want everything'. That costs both parties time. But again you run into this part about: what can they share? And, if you have a prudent law enforcement officer, they are more likely not to share as much as they probably could share, and that increases our time. But, if there is a quicker way, we are interested to look at it, because it is dead money for us. You look at our work—for our shareholders, it is dead money.[9]

5.12 Representatives from the ABA argued that the best examples of information sharing occurs where there is effective collaboration between banks and law enforcement, and a clear understanding by banks as to what exactly the law enforcement agency is looking for:

> …the best exchanges occur when there is the ability to exchange information around what law enforcement are actually after. The worst scenario is when you get broad warrants and notices because either law enforcement either do not know what they are after or do not know what might be available. If the notices are tailored to the particular evidentiary or investigation needs, the response time can be much quicker because we can target the search of our records. Also, with law enforcement we have worked on real-time information sharing under particular notices as well.[10]

5.13 The AGD rejected the ABA's view arguing that it would create different classes of organisations with different search warrant compliance arrangements in criminal investigations:

> Any person or organisation that is party to a police investigation is required to comply with relevant laws. The Department does not support creating specific arrangements for banking institutions, as distinct from other organisations or individuals, during investigations of criminal matters. In order to effectively investigate suspected criminal behaviour, it is important that law enforcement should have timely access to all relevant information,

---

8 Mr Damian McMeekin, Head of Group Security, ANZ, *Committee Hansard*, 9 September 2014, p. 4.

9 Mr Steven York, Head of Groups Security and Business Reliance, Bank of Queensland, *Committee Hansard*, 9 September 2014, p. 5.

10 Mr Guy Boyd, Global Head of Financial Crime, Australian and New Zealand Banking Group Ltd, *Committee Hansard*, 9 September 2014, p. 4.

irrespective of the nature of the organisation that is in control or possession of that information.[11]

Committee view

5.14 The committee notes instances, like *Strike Force Piccadilly* in Victoria that demonstrate the enormous benefits of co-operation between law enforcement and private sector financial service providers. The committee strongly encourages law enforcement and financial service providers to continue to collaborate in areas of mutual benefit.

5.15 The committee is not persuaded that law enforcement agencies should share contextual information from search warrants with financial service providers, nor 'tailor' warrants as suggested by the ABA.

5.16 The committee agrees with the points made by the AGD that implementation of such an arrangement would create different classes of organisations providing information to law enforcement. Such an approach may increase barriers to information for law enforcement agencies, increase the complexity around obtaining information between law enforcement and the private sector.

5.17 The committee does believe however, that information sharing can be enhanced through other means, including through the provision of access to the Document Verification System (DVS) that is discussed in Chapter 6.

11 Attorney-General's Department, *Answers to Questions on Notice*, p. 3.

Chapter 6
Technology and identity crimes

6.1 Having examined the regulatory relationships between the private and public sector, together with some crime prevention tools and strategies, the committee now examines the increasing use of technology in financial related crime, together with the increasing incidents of identity crime.

6.2 This chapter examines some of the technological enablers of financial related crime, including the 'Darknet', alternative currencies and the roll out of 'tap and go' technology.

6.3 This chapter also examines the role of iDcare as the lead organisation responsible for providing assistance to victims of identity crime.

6.4 Identity crime and credit card fraud are also examined in the context of new technology. Law enforcement strategies for addressing identity theft, especially the Document Verification System (DVS) are also examined in this chapter.

Technology

6.5 Many submitters and witnesses discussed the significant role that technology plays in facilitating financial related crimes. While technology has always been used for nefarious purposes, many witnesses and submitters emphasised the increasing sophistication of criminals and their reliance on rapidly changing technology.

6.6 The ACC submitted that financial crime is becoming significantly more sophisticated, in large part due to advances in technology. The increased use of technology by financial service users is playing a decisive role in facilitating financial related crime.[1]

6.7 The ACC argued that in the international space, three factors shape the serious and organised crime environment:

> …the infinitely complex, diverse and pervasive nature of serious and organised crime which is fundamentally enabled by globalisation, technology and cyber capabilities...[2]

6.8 The AFP emphasised its concerns with respect to the threat of cybercrime, where financial related crimes are perpetrated against individuals or corporations. The AFP argued that new technologies were allowing organised crime organisations to facilitate advanced and complex criminal acts against Australian interests:

---

1 Mr Chris Dawson APM, Chief Executive Office, Australian Crime Commission, *Committee Hansard*, 10 September 2014, p. 1.

2 ACC, *Submission 5*, p. 7.

> Cybercrime that is undertaken for financial gain is a significant issue for Australia as it is complex, multi-jurisdictional and is generally considered an enabler for financial crime. [3]

6.9 Submitters also raised the increasing use of specific technological tools in financial related crime, like Bitcoin and Darknet, both of which are examined below.

Bitcoin

6.10 Bitcoin is a virtual currency which allows online payments via peer-to-peer transfers between computers, into 'real currency' and provides users with an alternative to traditional banks. Bitcoin transfers are made by online exchange houses that facilitate exchanges between virtual currencies and standard currency.[4] The ACC noted that peer-to-peer transfers of virtual currencies can occur instantaneously without the need for transfers via third parties:

> This offers an entirely legitimate means of transferring value outside of the formal finance sector.
>
> The anonymity that this process affords, and the ease with which virtual currencies can be exchanged within and across borders, make them attractive to serious and organised crime. Virtual currencies are also attractive to individuals seeking to engage in criminal activities and the 'darknet', such as the former Silk Road, which relied solely on Bitcoin for the trade in illicit goods, including illicit drugs.[5]

6.11 The AFP submitted that the increased popularity of online currencies like Bitcoin provides additional opportunities for criminals to hide their identities online due to the lack of regulatory oversight of online currencies.

6.12 The ACC explained that the extent of Bitcoin's use for criminal activities is as yet an unknown quantity:

> Although virtual currencies such as Bitcoin are seen as vulnerable for exploitation by organised crime seeking to facilitate money laundering activities, evidence that this is occurring on a large scale is yet to be identified.[6]

6.13 AUSTRAC submitted that the evolution of digital currencies allowed internet based means of transferring 'real-world values' in lieu of using traditional currencies or physical commodities. AUSTRAC noted that digital currencies allowed individuals and entities to conduct both simple and complex international funds transfers outside standard regulatory arrangements:

> The evolution of digital currencies has led to the development of internet-based, electronic means of transferring ‘real-world’ value. In contrast to traditional physical currencies issued by national governments, digital

3 AFP, *Submission 6*, p. 7

4 ACC, *Submission 5*, Attachment 1, p. 17.

5 ACC, *Submission 5*, Attachment 1, p. 17.

6 ACC, *Submission 5*, Attachment 1, p. 18.

> currencies (such as Bitcoins, SolidCoins and Linden dollars) are issued by commercial enterprises and are not backed by traditional currencies, precious metals or other physical commodities.
>
> Digital currencies potentially allow individuals and entities to conduct quick and complex international funds transfers outside the regulatory requirements of the traditional financial system. Digital currencies that are not backed, either directly or indirectly, by precious metal or bullion are not regulated by the AML/CTF Act.[7]

6.14 AUSTRAC noted that the anonymous nature of digital currencies may appeal to criminal individuals or groups, who may see the currency as an instrument with which to evade tax or to obscure the origin of illicitly obtained funds:

> Criminal groups and individuals may increasingly use digital currencies, as opposed to online trading of real currency, due to the anonymity. These digital currencies present challenges for government agencies in following the money trail.[8]

6.15 The AFP agreed with the premise that the lack of AUSTRAC oversight of Bitcoin means it is an attractive method for money laundering or tax evasion in Australia:

> ...the use of these currencies may circumvent Australian Transaction Reports and Analysis Centre (AUSTRAC) reporting requirements regarding the movement of monies into, and out of, Australia.[9]

6.16 The ABA also noted in its submission the increasing availability of Bitcoin as an alternative currency. The submission noted the US Inland Revenue Service recognised Bitcoin as a currency and that it had been seized as part of their confiscations of the proceeds of crime program.[10]

Darknet

6.17 As outlined above, Darknet is often associated with the use of Bitcoin to enable financial related crime, including the use of stolen or misappropriated funds to purchase illicit goods or services.

6.18 SAPOL noted that with an 'onion router', an internet user could obtain access to the Darknet where they could access a variety of illicit material, including child exploitation sites or online drug markets:

> These darknet sites are predominantly around child exploitation material. There are drug sites. They had identified their own drug sites. It is a bit like Gumtree—you put an order in, say what you want, you give an address and then it will be sent to you. But because of the way the site operates, it uses your IP address because it comes through what is known as the onion

7 AUSTRAC, Submission 10, p. 20.

8 AUSTRAC, Submission 10, p. 20.

9 AFP, *Submission 6*, p. 7.

10 ABA, *Submission 4*, p. 5.

> router. There is no way of identifying who the person is. Because it comes in through that piece of software, the actual identity is stopped.[11]

6.19 While law enforcement agencies can act to some extent against Darknet sites, SAPOL noted that it was difficult for law enforcement to keep track of purchasers and sellers of illicit substances through the internet and Darknet.[12]

6.20 Victoria Police agreed that Darknet was an issue, as it facilitated criminal access to firearms sales, drugs and child exploitation materials.[13]

Committee view

6.21 The committee shares the concerns of Commonwealth, state and territory law enforcement agencies about the use of Bitcoin to procure illicit products and services on the Darknet.

6.22 The committee believes it is critical to ensure that Australian federal law enforcement agencies have adequate strategies and tools for the detection and disruption of technologically enabled financial crime.

6.23 However, at the time of writing the committee notes the Senate Economics References Committee is currently undertaking an inquiry into digital currency. This inquiry, which is focussed in detail on the implications of the emergence of virtual currencies, was extended on 2 March 2015 to report on 10 August 2015.[14] Accordingly, the committee has decided not to make any specific recommendations in this regard, but will await the conclusion of that inquiry process.

Identity crime

6.24 The committee heard from numerous submitters about increasing incidents of identity crime in Australia. Identity crime takes many forms, including using a fabricated or stolen identity to commit offences.[15]

6.25 The AFP noted that identity crime is often linked to other forms of criminality, including illicit commodity movements, money laundering, fraud against the Commonwealth, people smuggling and human trafficking.[16] Additionally, the AFP submitted that the organised theft and sale of stolen identity information was usually for the purposes of manufacturing fraudulent identity documents, including credit

---

11 Mr Paul Dickson, Assistant Commissioner, South Australian Police, *Committee Hansard*, 9 September 2014, p. 10.

12 Mr Paul Dickson, Assistant Commissioner, South Australian Police, *Committee Hansard*, 9 September 2014, p. 10.

13 Mr Stephen Fontana, Assistant Commissioner, Victoria Police, *Committee Hansard*, 9 September 2014, p. 57.

14 *Journals of the Senate*, No. 79—2 March 2015, p. 2203. Information about the Senate Economics References Committee inquiry into digital currency can be found here: www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency.

15 AFP, *Submission 6*, p. 1.

16 AFP, *Submission 6*, p. 5.

cards, driver licences and Medicare cards. All of these documents can be subsequently used for criminal purposes.[17]

6.26 In relation to the level of identity crime in Australia, the AFP noted:

> The extent and impact of identity crime in Australia remains difficult to establish definitively. The Australian Bureau of Statistics Personal Fraud Survey for 2010-11 estimated over 700 000 Australians were victims of identity fraud and over 44 000 Australians were the victims of identity theft.[18]

6.27 The AGD elaborated on this point noting that surveys by the Australian Institute of Criminology (AIC) and Australian Bureau of Statistics (ABS) indicate that around 4 to 5 per cent of Australians report being a victim of identity crime each year, and have suffered subsequent financial loss. The AGD quantified the financial losses experienced by victims of identity crimes:

> The AIC survey indicated that victims reported an out-of-pocket loss of between $1 and $310,000, at an average of $4,101 per incident. However, just over half of respondents (55%) who reported losing money managed to recover or be reimbursed for some of their losses, at an average of $2,481 per incident, while the remaining 45 per cent did not receive any reimbursement or recover any losses. Overall, losses were relatively small, with 50 per cent of victims losing less [than] $250 and 75 per cent losing less than $1000.[19]

National Identity Security Strategy

6.28 The National Identity Security Strategy (NISS) was developed in 2005, following a Council of Australian Governments (CoAG) agreement to recognise that preservation and protection personal identity information 'is a key concern and a right of all Australians.'[20]

6.29 In 2012, the NISS was revised to 'support the development and implementation of the identity crime measurements framework.'[21] The AFP submitted that the NISS aims to develop conditions where Australians feel confident they enjoy the benefits of a 'secure and protected identity':

> The scope of the NISS is shaped by the need to strengthen national security, prevent crime and enable the benefits of the digital economy. Commonwealth, state and territory Governments are working together to enhance national consistency, interoperability and opportunities (including for government service delivery) through nationally consistent processes for

---

17 AFP, *Submission 6*, p. 5.

18 AFP, *Submission 6*, p. 5.

19 AGD, *Submission 9*, p. 14.

20 Attorney-General's Department, *National Identity Security Strategy*, www.ag.gov.au/rightsandprotections/identitysecurity/pages/nationalidentitysecuritystrategy.aspx, (accessed 26 June 2015).

21 AFP, *Submission 6*, p. 13.

> enrolling, securing, verifying and authenticating identities and identity credentials.[22]

6.30 The AGD submitted that the DVS was a key element of the NISS.[23]

Document Verification Service

6.31 The committee heard evidence from numerous witnesses, including the AGD, ABA and remittance industry participants regarding the DVS, which is used by financial service providers to validate the identity of customers. The feedback on the DVS was largely positive, however some witnesses, including the ABA, criticised the cost of access and the limited information available to financial service providers.

Background

6.32 The DVS is a secure, online system that 'provides for automated checks of the accuracy and validity of information on the key government documents commonly presented as evidence of identity.'[24] The AGD submitted that the DVS allows user organisations, like banks and other financial services providers, to check the information on identity credentials against the records of issuing agencies.

6.33 The DVS has been available to government agencies since 2009. Certain private sector organisations, which have requirements to verify identities under Commonwealth legislation, gained access in early 2014.[25] The AGD noted:

> There has been strong private sector interest in the DVS, particularly from providers of financial services. As at 29 April 2014, 160 private sector applications had been approved and the service had 23 active private sector users. On 5 May 2014, the Attorney-General, Senator the Hon George Brandis QC, launched the DVS commercial service.[26]

6.34 The AGD was emphatic in its view that the DVS helps businesses protect themselves against identity crime while making identity verification mandated by legislation easier. Further, the AGD submitted that the DVS was not a database in that it did not retain personal information, and that all checks must be carried out with the informed consent of the individual. Finally, the AGD noted it was working with State and Territories (as joint owners of the DVS) to further expand the range of private sector organisations that have access to the service.[27]

---

22 AFP, *Submission 6*, p. 13.

23 Attorney-General's Department, *National Identity Security Strategy*, www.ag.gov.au/rightsandprotections/identitysecurity/pages/nationalidentitysecuritystrategy.aspx, (accessed 26 June 2015).

24 AGD, *Submission 9*, p. 16.

25 AGD, *Submission 9*, p. 16.

26 AGD, *Submission 9*, p. 16.

27 AGD, *Submission 9*, p. 16.

Responses from private sector DVS users

6.35 The ABA argued that while the DVS was a step in the right direction in enabling private sector operators to access verified identity data, it suggested that government and industry should work together to create a 'secure digital identity' for Australians.[28]

6.36 Independent remittance industry representatives noted that there are costs to private sector users of the DVS, including being charged 67 cents to check identities (per successful check) and paying a $5000 set up fee.[29] The independent remittance industry association, subsequently known as the Australian Remittance and Currency Providers Association, submitted that the $5000 set up fee ought to be waived. The association argued that the removal of the fee would allow remittance providers of varying sizes access to the DVS.[30]

6.37 Similarly, representatives from Veda, a data analytics company with a background in identity security and fraud prevention, argued for easier access to the DVS. Veda representatives contended that the VDS did not include enough data and was not accessible to numerous stakeholders who require identity verification technology.[31]

6.38 Veda submitted that the DVS, while verifying the authenticity of government issued identification, is only available to organisations with a requirement under Commonwealth legislation to verify identities.[32] Veda submitted that 'the restriction on access must end,'[33] and was also critical of the fees charged for access, arguing that the high fees had resulted in low numbers of subscribers:

> Fifteen months after opening, only 200 entities have applied. Consider the real estate agent letting a property or the utility providing energy. As the South Australian police submission points out, organised criminal syndicates are involved in cannabis-growing houses with rentals under false names. We ask that the committee recommend that the DVS should be open to any entity with a reasonable requirement to verify identity and have subscriber requirements similar to those used to subscribe to other government registers, such as ASIC's Personal Property Securities Register. We also note, reflecting the varying unreadiness of state registers, that the

28 Mr Guy Boyd, Global Head of Financial Crime, Australia and New Zealand Banking Group Ltd, *Committee Hansard*, 9 September 2014, p. 3.

29 Ms Dianne Nguyen, Director, Head of Compliance, Eastern & Allied Pty Ltd, *Committee Hansard*, 9 September 2014, p. 27.

30 Australian Remittance and Currency Providers Association, *Supplementary Submission No. 2*, p. 2.

31 Mr Matthew Strassberg, Senior Advisor, External Relations, Veda, *Committee Hansard*, 9 September 2014, p. 36.

32 Mr Matthew Strassberg, Senior Advisor, External Relations, Veda, *Committee Hansard*, 9 September 2014, p. 36.

33 Mr Matthew Strassberg, Senior Advisor, External Relations, Veda, *Committee Hansard*, 9 September 2014, p. 36.

> DVS cannot verify birth, death and marriage certificates online and in real time. This in the digital age needs remedying.[34]

6.39 Veda argued that a more widely available and cheaper DVS, together with changes to the restriction on access to electoral roll and credit reporting data would 'add integrity to the first layer of identity checking'.[35]

Response from AGD

6.40 In answers to *Questions on Notice*, the AGD detailed its proposal to the Law Crime and Community Safety Council (a council of COAG) that the DVS should be open to any organisation that has a reasonable requirement to identify a person to conduct their business and obtains that person's consent. According to the AGD, this would be consistent with the *Privacy Act 1988*, including the revisions that came into effect in March 2014.[36]

6.41 The AGD advised that it expected to implement the new access policy for all jurisdictions that have agreed to the arrangements, in March 2015.[37] The AGD has also reviewed the process to access to the DVS:

> The Department will implement a substantially simplified application process in March 2015. The per user access fee will be significantly reduced as a result.[38]

6.42 Expanded access to the DVS became effective on 31 March 2015. The DVS website notes that 'businesses with a reasonable need to use a Commonwealth identifier to verify their client's identity may now be eligible to access the DVS.'[39] The changes made to DVS access include:

- a reduction in access (or 'set up') fee from $5000 to $250;[40] and
- a change to fee structure so that fees are charged per identity check. Details of these fees are outlined in Table 1 below.

---

34 Mr Matthew Strassberg, Senior Advisor, External Relations, Veda, *Committee Hansard*, 9 September 2014, p. 36.

35 Mr Matthew Strassberg, Senior Advisor, External Relations, Veda, *Committee Hansard*, 9 September 2014, p. 36.

36 AGD, *Answers to Questions on Notice*, p. 4.

37 AGD, *Answers to Questions on Notice*, p. 4.

38 AGD, *Answers to Questions on Notice*, p. 4.

39 Attorney-General's Department, *The Document Verification Service—fast, secure, trusted*, www.dvs.gov.au/Pages/default.aspx (accessed 10 June 2015).

40 Attorney-General's Department, *The Document Verification Service—fast, secure, trusted*, www.dvs.gov.au/Pages/default.aspx (accessed 10 June 2015).

Table 1—DVS fees schedule, as at 10 June 2015[41]

Annual Volume	Per calendar month	Per query charge
< 400 000	<33 000	$1.40
>400 000 <600 000	>33 000 <50 000	$1.20
>600 000 <800 000	>50 000 <65 000	$1.00
>800 000 <1 million	>65 000 <85 000	$0.80
> 1 million	>85 000	$0.65

Committee view

6.43 The committee acknowledges the ongoing threat of identity crimes.

6.44 The committee welcomes the major reduction in the DVS registration fees and is satisfied with the efforts of the AGD to broaden access to the system. The committee is confident that over time this will lead to many more private sector organisations accessing the DVS facility, and in turn improve personal identity security in Australia. In the committee's view the DVS will become a keystone for government agencies and private companies who require verification of a client's identity.

Support for victims of identity crime

6.45 In 2014, the Minister for Justice launched iDcare, a national support centre for victims of identity crimes.[42] iDcare argued that since 2003, financial crime in Australia has evolved rapidly and mirrors developments in commerce, government services and mobile communications.[43]

6.46 iDcare argued that the previous ten years has also seen the advent of technology-based identity crime, where motives have expanded from traditional financial gain and theft of personal or financial information, to political or ideological statements, known as *Hacktevism*. iDcare submitted that it viewed *Hacktevism* crimes as more personalised than 'traditional' identity theft, and that it had responded to over 800 individual clients since September 2013, some of whom had been victimised by *Hacktevism*, 'the consequences of which can have quite different impacts to individuals.'[44]

41 *The Document Verification Service—fast, secure, trusted*, www.dvs.gov.au/Pages/default.aspx (accessed 10 June 2015).

42 iDcare, *Submission 23*, p. 1.

43 iDcare, *Submission 23*, p. 1.

44 iDcare, *Submission 23*, p. 2.

6.47 Critically, iDcare estimated that 1.1 million Australians and New Zealanders are impacted by identity theft and misuse of information every twelve months.[45]

6.48 iDcare raised specific issues relating to Commonwealth victim certificates, which are designed to support claims for victims of Commonwealth identity crime. iDcare noted that under the current scheme individuals must satisfy three criteria:

- a person makes, supplies or uses identification information (yours, or a third party's);
- they do this intending that either they or someone else will pretend to be you or another person (who is living, dead, real or fictitious); and
- the act of pretending would be done to commit or help commit a Commonwealth indictable offence.[46]

6.49 iDcare argued that these criteria were difficult to fulfil given that less than six per cent of identity crime perpetrators are arrested or prosecuted successfully.[47] iDcare contended that the certifications are not working to support victims of identity crime:

> iDcare is not aware of any successful issuance of a victim certificate for identity crime, within either relevant State equivalent measures or the Commonwealth. This is not from a lack of interest. iDcare receives a number of calls from individuals that express interest in obtaining such certificates, but in all instances fall at the first hurdle of the essential element – someone has been successfully convicted of an identity crime offence.[48]

Committee view

6.50 The committee is concerned with the evidence from iDcare about the prevalence of identity crime in Australia.

6.51 The committee is also greatly concerned with the evidence that Commonwealth victim certificates appear to be difficult to obtain due to evidence that an arrest and successful prosecution being required to satisfy the first eligibility criterion. Given the seriousness of the problem, the significant personal impacts suffered by the victims of identity theft, and the likelihood of increasing incidences of identity crime, the committee believes there is further work to be done to both deter identity crime and to assist its victims.

6.52 The committee commends iDcare for its work in assisting the victims of identity crime, and is persuaded by its advocacy that the scheme for issuing Commonwealth victim certificates needs to be examined.

---

45 iDcare, *Submission 23*, p. 1.

46 iDcare, *Submission 23*, p. 4.

47 iDcare, *Submission 23*, p. 4.

48 iDcare, *Submission 23*, p. 4.

Recommendation 11

6.53 The committee recommends the Attorney-General's Department review the arrangements for victims of identity crime to obtain a Commonwealth victim certificate.

Contactless payment technology

6.54 As outlined above, the DVS is an effective tool for both law enforcement and financial service providers for checking and verifying the identities of customers accessing financial services. Critically, the related issue of technology-enabled credit card fraud was raised by numerous submitters, including law enforcement agencies, who argued that new technology had effectively expanded the scope for credit card fraud from more traditional credit card fraud, to multiple low value purchases to evade detection. This, they argued, was largely due to the rollout of contactless payment technology.[49] This section addresses some of that commentary in detail.

6.55 Contactless payment technology enables customers to pay for products and services under $100, by 'waving' or 'tapping' their card to payment terminals. Benefits for customers include faster transactions and in some cases, the ability to pay through the use of 'near field communication' technology in mobile phones.[50]

6.56 Victoria Police raised as an area of concern a 'significant increase' in deception offences in Victoria, arguing that new technology had enabled offenders to commit multiple low value transactions with stolen credit cards.'[51]

6.57 Victoria Police argued that increased technology, lack of guardianship and the perception that credit card fraud is a victimless crime, is 'driving [deception] offences'.[52] Victoria Police also argued that 'tap and go' technology, provides motivation for the physical theft of credit cards, with little risk of capture by police or of physical identification. Further, Victoria Police noted:

> The major banks provide a Zero Liability Policy to customers who are victims of fraudulent transactions. This policy is clearly advertised in conjunction with ‘Tap and Go’ technology. Widespread promotion of the Zero Liability Policy is expected to motivate offenders who are likely to see that the victim will not be at a personal loss. Anecdotal information from the Victoria Police Fraud & Extortion Squad and Victoria Police E-Crime Squad suggests that financial institutions factor fraudulent activity into their profit and loss margins and currently the loss associated with ‘Tap and Go’

---

49 Contactless payment refers to technology that allows individuals to pay for products and services by 'tapping' their credit or debit card against a payment terminal. The committee recognises numerous iterations of this technology exist and are referred to, in some cases interchangeably as 'tap and go', 'paywave' and 'paypass'.

50 Visa, Mobile Visa payWave, http://www.visa.com.au/personal/features/include/Visa_mobile_payWave_factsheet_approvedApril2014.pdf (accessed 30 June 2016)

51 Victoria Police, *Submission 13*, p. 2.

52 Victoria Police, *Submission 13*, p. 2.

> is far [outweighed] by the profits generated. If losses are budgeted for, Victoria Police are likely to find it difficult to develop strategies in partnership with financial institutions to improve guardianship. As part of a recent intelligence gathering exercise, National Australia Bank, Commonwealth Bank, ANZ, Westpac and Visa were all contacted via email and/or phone for consultation during recent analysis of this issue by Victoria Police. No responses were received prior to the finalisation of a recent intelligence product. Without engagement by financial institutions it is difficult to understand the full extent of fraudulent activity and the impact new technology and policies have on the criminal environment.[53]

6.58 Broadly, Victoria Police were highly critical of the lack consultation between financial institutions and the police, especially as it relates to the introduction of new, higher risk technologies, such as contactless payment systems:

> Engagement with police prior to such initiatives would greatly assist in having standard practises across industry. Simplicity of structures and processes is essential and "bureaucracy" is often a barrier to effective joint action.[54]

6.59 The committee is aware of the commentary regarding the roll out of contactless payment technology, including media articles detailing police concerns about the security of the systems. Victoria Police have also raised this issue publicly, arguing that it was likely to be behind the rise in 100 extra credit card deceptions per week.[55]

6.60 Representatives of the banking industry disagreed that contactless payment technology poses a significant fraud threat. Mr Boyd argued:

> But the PayWave mechanism itself is not a large driver of fraud losses for consumers or the banks. It is actually very popular with consumers too, because it is very convenient, and it is popular with merchants because it is fast. And at the moment with the low thresholds on that mechanism I do not think it is a realistic large threat to fraud losses. I think some of the other issues we have been discussing are much bigger threats in terms of financial loss and customer inconvenience.[56]

Committee view

6.61 The committee shares the concerns of law enforcement agencies that the rollout of new technology without consultation with law enforcement agencies has the potential to become a driver of financial related crime. The committee believes that banks and other financial service providers ought to consider law enforcement issues

---

53 Victoria Police, *Submission 13*, pp 2–3.

54 Victoria Police, *Submission 13*, p. 5.

55 9news, *Credit card crime increase could see tap-and-go gone*, www.9news.com.au/technology/2015/01/17/07/50/credit-card-crime-increase-could-see-tap-and-go-gone, (accessed 20 April 2015).

56 Mr Guy Boyd, Global Head of Financial Crime, Australian and New Zealand Banking Group Ltd, *Committee Hansard*, 9 September 2014, p. 7.

more carefully, and to facilitate discussions with law enforcement about new technologies prior to rollout.

6.62 As discussed in Chapter 5, the committee is persuaded of the advantages of close private and public sector collaboration in addressing financial related crime.

6.63 While banks have argued the fraud risk of new technologies is accounted for in their banking systems, the committee believes that consumers should have the option of disabling contactless payment features.

Recommendation 12

6.64 The committee recommends that financial institutions which issue debit and credit cards create an 'opt in' function that requires customers to consent to contactless payment technology features being activated on their cards.

Chapter 7

Financial crime against Indigenous communities

7.1 During the inquiry the committee heard evidence from numerous submitters and witnesses regarding the targeting of Indigenous communities by criminal organisations. For instance the Northern Territory Police (NT Police) submission highlighted these concerns:

> The types of financial related crimes that affect the Northern Territory (NT) are consistent with those which occur nationally. The NTP [Northern Territory Police] have identified anecdotal increases in financial crimes exploiting vulnerabilities associated with Indigenous Entities.[1]

7.2 Supporting the submission from the NT Police was evidence from legal and education service providers who argued that Indigenous communities were particularly vulnerable to financial crime.[2] The Northern Australian Aboriginal Justice Agency (NAAJA) for instance submitted that without assistance and education in financial literacy, Indigenous communities were without the resources to fight against financial crime such as phishing scams.[3]

7.3 Officers of the former ACC National Indigenous Intelligence Task Force (NIITF) told the committee that without adequate governance capabilities of Indigenous organisations, including auditing and accounting practices, the government funding provided to Indigenous communities was at risk.[4] This view was supported by evidence from Indigenous legal and education service providers who highlighted the lack of investment in auditing, accounting and financial management education in Indigenous organisations and communities.

7.4 This chapter discusses the evidence received in relation to financial related crime targeting Indigenous communities and organisations, beginning with a scam at Nhulunbuy as an example of the issues faced by many Indigenous communities. The chapter then discusses the main concerns raised by submitters:

- education, financial literacy and language barriers; and
- regulatory environment and governance capabilities of Indigenous organisations (auditing, accounting practices).

---

1 NT Police, *Submission 2*, p. 2.

2 Mr Mark Payne, Assistant Commissioner, Crime and Specialist Services, Northern Territory Police Force, *Committee Hansard*, 8 September 2014, p. 2.

3 Ms Pip Martin, Managing Solicitor–Civil, Northern Australian Aboriginal Justice Agency, *Committee Hansard*, 8 September 2014, p. 20.

4 Ms Judy Lind, Executive Director, Strategy and Specialist Capabilities, Australian Crime Commission, *Committee Hansard*, 8 September 2014, p. 14.

Nhulunbuy community scam

7.5 A scam targeting the Indigenous community in Nhulunbuy, in remote north-east Arnhem Land, provides a clear example of the types of scam perpetrated against Indigenous communities, and the substantive regulatory and educational issues facing Indigenous communities and law enforcement agencies.

7.6 The NT Police explained that international crime groups had specifically targeted vulnerable groups in Indigenous communities. The scam was described by the NT Police as a 'traditional advance fee inheritance scam'. In January 2014, the NT Police received information that between 10 and 20 individuals in the community had made payments to the scammers via the Western Union bank.[5]

7.7 The NT Police estimated the total losses from the community at $70 000, with the funds being paid to locations overseas. The NT Police described the scammers' methodology as including:

> …a combination of open source analysis, using internet search engines as well as targeted calls to identify Indigenous groups in regional outstations.[6]

7.8 Mr Mark Payne, Assistant Commissioner, Crime and Specialist Services, NT Police, told the committee that the Nhulunbuy case had an added layer of complexity because a 'money mule' had been used in the transfers of money through the Western Union bank.[7]

7.9 Commander Richard Bryson, Crime and Specialist Support Command, NT Police, told the committee that the trend towards sophisticated, targeted financial crime against Indigenous communities was very concerning, particularly the speed with which such crimes could be perpetrated:

> …around that Nhulunbuy incident, we see that the method of operation was one where it was a very sophisticated scam to the extent that it involved a lot of subjectivity on behalf of the targets and knowledge around the sorts of conversations and approaches that could be made in order to facilitate that scam. You can see how quickly that that was able to be perpetrated.[8]

7.10 Commander Bryson noted that the level of sophistication in the Nhulunbuy scam showed an evolution in criminal methodology:

> …the most concerning thing is that traditionally a lot of those types of fraudulent scams are done with no subjective understanding, or a very poor subjective understanding, of the victim. As some of those crime types evolve—as we all know, criminals evolve in their method of operation—

5 NT Police, *Submission 2*, p. 2.

6 NT Police, *Submission 2*, p. 2.

7 Mr Mark Payne, Assistant Commissioner, Crime and Specialist Services, Northern Territory Police Force, *Committee Hansard*, 8 September 2014, p. 2.

8 Commander Richard Bryson, Northern Territory Police Force, *Committee Hansard*, 8 September 2014 p. 2.

> what is concerning is that they have had that subjective understanding of the target group and have been able to exploit it.[9]

7.11 Although the NT Police submission states that international crime organisations were responsible for the scams in Nhulunbuy, Assistant Commissioner Payne told the committee that financial crime threats to Indigenous communities could also originate within Australia.[10]

7.12 The Nhulunbuy scam is but one example of the threats faced by Indigenous communities from financial crime organisations. Assistant Commissioner Payne advised that with the combination of funding, lack of governance, and poor financial literacy, the threats to Indigenous communities from financial crime are widespread:

> Essentially, in the Northern Territory we find we are not immune—and in fact we have certain entities within our community who are more susceptible to financial crime. In many instances, these are people who form part of the community who may be less likely to receive advice because of the areas where they live and in some instances, a lower level of education but higher access to moneys, either through royalties or other payments. We also see some targets in the Northern Territory today and ongoing into the future related to large amounts of government funding and grants that sit in accounts that, with some of the governance arrangements that stand around these entities and these associations, make them very vulnerable to financial fraud.[11]

Intelligence gathering

7.13 NT Police representatives explained that they had put a lot of faith into the Australian Cybercrime Online Reporting Network (ACORN), arguing that it would result in higher detection and awareness of scams earlier, and facilitate a speedier response to financial related crime.[12]

7.14 Further, NT Police detailed their expectation that ACORN would provide a much better picture of criminality for law enforcement agencies, as well as provide information to victims of crime due to its business rules. This would encourage more accurate capture and retention of information, without giving unrealistic hopes or expectations to victims of fraud:

---

9 Commander Richard Bryson, Northern Territory Police Force, *Committee Hansard*, 8 September 2014 p. 3.

10 Mr Mark Payne, Assistant Commissioner, Crime and Specialist Services, Northern Territory Police Force, *Committee Hansard*, 8 September 2014, p. 1.

11 Mr Mark Payne, Assistant Commissioner, Crime and Specialist Services, Northern Territory Police Force, *Committee Hansard*, 8 September 2014, p. 2.

12 Mr Mark Payne, Assistant Commissioner, Crime and Specialist Services, Northern Territory Police Force, *Committee Hansard*, 8 September 2014, p. 4.

> The ACORN initiative will automate a large body of that work and be much better for the wider community and the victims of this type of offending.[13]

7.15 NT Police also raised the role of the NIITF in detecting not only child related sex offences, but also the existence of a substantial connection to financial related crime, in that facilitators of either crime were often interchangeable:

> ...for the facilitators of some crimes against children or, vice versa, the facilitators of some financial fraud, there is a relationship between the two, that is, compromising people, or having people compromised over offences that they may have committed and then making them the subject of fraud activity in terms of duress, basically.[14]

National Indigenous Intelligence Task Force

7.16 The committee received evidence relating to the establishment (and eventual completion) of the NIITF. Established as part of the Commonwealth Government's Building Stronger Communities in the Northern Territory initiative, 'the NIITF was announced in July 2006 as part of a whole‑of‑government response to violence and child abuse in remote, rural and urban Indigenous communities.'[15] The committee understands that the NIITF ceased operation on 30 June 2014.

7.17 Former officers of the NIITF told the committee:

> The NIITF's aim was to build a national understanding of the nature and extent of violence and child abuse in Australia's remote, regional and urban Indigenous communities. The ACC was well placed to run the NIITF as it is the only criminal intelligence agency with a national footprint and access to a range of capabilities required to collect, analyse and provide information regarding the extent of child abuse and violence in Indigenous communities.[16]

7.18 The NIITF representatives also noted the significant threats to Commonwealth funding of Indigenous programs, largely due to the sophistication of schemes targeting Indigenous Australians:

> In terms of the drivers of financial crime and exploitation within Indigenous communities, there are a number of factors at play, including socioeconomic disadvantage, problem gambling, poor governance and

---

13 Commander Richard Bryson, Northern Territory Police Force, *Committee Hansard*, 8 September 2014 p. 6.

14 Mr Mark Payne, Assistant Commissioner, Crime and Specialist Services, Northern Territory Police Force, *Committee Hansard*, 8 September 2014, p. 5.

15 National Indigenous Intelligence Task Force (NIITF), Factsheet, Australian Crime Commission, p. 1.

16 Ms Judy Lind, Executive Director, Australian Crime Commission, *Committee Hansard*, 8 September 2014, p. 9.

> accountability, and the absence of probity check of staff and board members within some Indigenous communities.[17]

7.19 The NIITF representatives explained that while financial related crime and exploitation within Indigenous organisations is difficult to detect, investigate and prosecute, its prevalence is largely due to a number of factors, including:

> …the significant under-reporting due to fear of retribution, the fear of self-incrimination, shame, unawareness that it has actually taken place, and, where government funding is concerned, a concern that making a complaint might risk future funding into those organisations.[18]

7.20 The committee received a confidential copy of the NIITF report to assist with its analysis of the work of the NIITF. The committee has decided not to release this information publicly. The committee notes that aspects of that report were released under FOI by the ACC on 13 March 2015.[19]

7.21 While the report focusses mainly on issues associated with violence and child abuse in Indigenous communities, the NIITF developed numerous intelligence products relating to illicit substances and financial crimes.[20]

7.22 The report notes that, in relation to financial crime, exploitation of Indigenous organisations occurs in every jurisdiction and is likely to increase, with remote communities assessed as being particularly vulnerable.[21]

7.23 The NIITF report notes:

> Indigenous program funding is significant and is vulnerable to financial crime and exploitation. When funding is diverted by criminal acts, there can be significant reductions in program delivery, loss of community trust and confidence, normalisation of criminal activity, and community disadvantage.[22]

7.24 These issues are examined in greater detail below in the context of financial services awareness (education), financial literacy and governance.

---

17 Ms Judy Lind, Executive Director, Australian Crime Commission, *Committee Hansard*, 8 September 2014, p. 9.

18 Ms Judy Lind, Executive Director, Australian Crime Commission, *Committee Hansard*, 8 September 2014, p. 10.

19 www.crimecommission.gov.au/publications/freedom-information/disclosure-log

20 ACC, *The Final Report of the National Indigenous Intelligence Task Force*, (released under FOI), 2006–2014, p. 5.

21 ACC, *The Final Report of the National Indigenous Intelligence Task Force*, (released under FOI), 2006–2014, p. 17.

22 ACC, *The Final Report of the National Indigenous Intelligence Task Force*, (released under FOI), 2006–2014, p. 17.

Risk factors and prevention

7.25 The factors which place Indigenous communities and organisations at risk should be, in the opinion of witnesses and submitters, the key targets for preventative action. This section examines each risk factor in turn, noting the current and suggested actions for prevention and safeguarding of Indigenous communities and organisations:

- education (organisations and individuals);
- financial literacy and language barriers; and
- governance capabilities of indigenous organisations (auditing, accounting practices).

Education – organisations and individuals

7.26 Many witnesses, like the NT Police[23] and NAAJA[24] agreed that education, and particularly financial literacy, was the best means of protecting individuals and organisations in Indigenous communities from financial crime. Commander Bryson told the committee that while there were good mechanisms in place to deal with crime once reported, education was essential:

> …from a law enforcement perspective there are already some fairly robust mechanisms in place so that once there is any vision over that type of scam or offending then the appropriate things take place in relation to the money transfers and in relation to the accounts the moneys are being transferred to in order to basically put a stop to that crime series. But I think the better way to approach things is in relation to the education space I spoke about before, for the target group here in the Northern Territory that does not have access to the normal types of communication strategies that the government would engage in.[25]

7.27 Assistant Commissioner Payne agreed that educated and aware individuals were those best protected against financial crime. He noted the role of the ACCC in educating the public regarding financial crime and scams:

> I would also like to raise just briefly some of the advancements, particularly we think the role of the Australian Competition and Consumer Commission in terms of getting information out to the public and the strategies that are enforced through the Australasian Consumer Fraud Taskforce, which detect, disrupt and disable, are very sound strategies. We tend to feel, as

23 Commander Richard Bryson, Northern Territory Police Force, *Committee Hansard*, 8 September 2014 p. 3.

24 Ms Pip Martin, Managing Solicitor-Civil, Northern Australian Aboriginal Justice Agency, *Committee Hansard*, 8 September 2014, p. 21.

25 Commander Richard Bryson, Northern Territory Police Force, *Committee Hansard*, 8 September 2014 p. 4.

> law enforcement agencies, that our best attack is the defence that we gain by advising victims and trying to make them more savvy and aware.[26]

7.28 Commander Bryson argued that the best way to educate those who needed it most was to have 'boots on the ground':

> From the educational perspective, the large Indigenous population that we have here in the Northern Territory are extremely disparate in some of the remote communities where they live, and, notwithstanding some of our efforts where we have worked with the other stakeholders in that education space, it is problematic to actually reach that target audience and have them be aware. The traditional way that you might go about that in other parts of Australia will not get the traction that you would expect or hope to get in those circumstances. Unfortunately it involves a lot of face-to-face contact and a lot of actually having relationships with relevant people on the ground. For lack of a better expression, it involves 'boots on the ground' in these remote communities to make sure that people are aware of these things.[27]

7.29 Commander Bryson also emphasised the need for education and proper management, particularly in an environment such as the Northern Territory, which has a large investment of Commonwealth grant funding going to community-based organisations:

> Certainly from the Northern Territory Police perspective, we really feel that a greater investment from some of the Commonwealth bodies in that education space before it gets to the stage of offending and some more robust accounting and auditing processes going forward would be of assistance. Also, we are a small jurisdiction but have a disproportionate amount of Commonwealth grants and Commonwealth funding coming into the jurisdiction. We have done some work in the last 18 to 24 months where, going forward, we would like to think that in the medium term we may be able to move ourselves into a position where we have our own joint task force here in the Territory and we can get some of the Commonwealth bodies to come on board and cohabitate with us here in the Territory so that we can case manage some of these matters in a much better fashion.[28]

7.30 The committee heard from Mr Richard Trudgen, an advocate on Indigenous matters who appeared in a private capacity, of his experiences providing education to those in communities who had been the victims of scams. Mr Trudgen is a community

---

26 Mr Mark Payne, Assistant Commissioner, Crime and Specialist Services, Northern Territory Police Force, *Committee Hansard*, 8 September 2014, p. 2.

27 Commander Richard Bryson, Northern Territory Police Force, *Committee Hansard*, 8 September 2014 p. 3.

28 Commander Richard Bryson, Northern Territory Police Force, *Committee Hansard*, 8 September 2014 p. 3.

educator and author, and has worked with the Yolngu people in north-east Arnhem Land for about 40 years.[29]

7.31 Mr Trudgen told the committee that 'knowledge gap' research has revealed the true extent of the lack of education and awareness about financial management and financial crime in Indigenous communities.[30] Mr Trudgen had the opposite view to the NT Police of the utility of the ACCC's scam awareness work:

> It is no good if the [ACCC] or any of those other organisations come along and say, 'We'll put some posters out.' Well, wonderful! They will sit in a corner somewhere. They are all in English and they will just become fire fodder. They do not deal with the real needs that people have.[31]

Financial literacy and language barriers

7.32 Mr Trudgen highlighted two key problems with the financial literacy levels in Indigenous communities, and the consequent vulnerability to financial crime: lack of financial understanding and language barriers.[32]

7.33 Understanding the financial system, including modern innovations of electronic banking, is vital for individuals to identify ways to protect themselves from financial crime. Mr Trudgen explained that this basic understanding, and financial literacy was lacking from the communities with which he engaged:

> We introduce all these technologies to Indigenous people and we do nothing about preparing them. We have opened up now to electronic banking et cetera. People are basically economically illiterate, which they were not years ago when they were trading with Makassar [a major Indonesian port]. The older people I knew 40 years ago had very good economic literacy and understanding of those things. But today there is little economic literacy, especially since the Northern Territory intervention, with the mystification about government having all this money and government printing all this money.[33]

7.34 Mr Trudgen used the example of the concept of banking passwords to explain the point further:

> Plus, we introduce all these technologies to people, like bank cards and SIM cards and the things we develop programs around, like passwords and security codes… When we did the work around passwords, people had no understanding of what that word meant, as you would not if English was your second language, as it was for these people—or fifth or sixth language. When you asked them, 'What does that word mean,' they said, 'That's the

29 Mr Richard Trudgen, private capacity, *Committee Hansard*, 8 September 2014, p. 16.

30 Mr Richard Trudgen, private capacity, *Committee Hansard*, 8 September 2014, p. 16.

31 Mr Richard Trudgen, private capacity, *Committee Hansard*, 8 September 2014, p. 18.

32 Mr Richard Trudgen, private capacity, *Committee Hansard*, 8 September 2014, p. 17.

33 Mr Richard Trudgen, private capacity, *Committee Hansard*, 8 September 2014, p. 17.

> word you pass on to people,' because they had no history of Europe and where that word came from… So we told that story, and even the Yolngu lady who was helping me said, 'I've been doing credit union training forever, for the last 10, 20 years, and this is the first time I've actually heard the background meaning to the word "password".' I see people give out their security codes like they are nothing. They will give a card to a kid and give them the security code, and off they go to get money out.[34]

7.35 Language barriers are also considerable obstacles in people's financial understanding, and in the communication of awareness of financial crimes. Mr Trudgen argued passionately for the need for communication materials designed for Indigenous communities to be in the language of those communities:

> …we need the Australian government to roll out something, for Aboriginal people right across the country, even where Aboriginal people are speaking Aboriginal English, not through culturally incompetent mainstream services, but through organisations like ours and so on, who have the language skills, who know their people and who know what the gaps are... We could turn this stuff around if we just spent a fraction of the dollars that have been wasted in the Aboriginal industry at the moment.[35]

7.36 Ms Pip Martin, a managing solicitor of NAAJA, supported Mr Trudgen's evidence, noting that 'at the same time as we have this increase in technology, there is a lack of education and basic knowledge to be able to deal with those technologies.'[36]

7.37 Both Mr Trudgen and Ms Martin insisted on the need for any education or awareness raising to be done in an individual's first language. Mr Trudgen reported the benefits from the use of radio as opposed to written communication.[37] Ms Martin made the point that whenever the community legal education team visits communities they always use interpreters. Ms Martin believed that very few, if any, national campaigns on financial literacy were available in translated form. Further, Ms Martin noted that written information is not as suitable for communication in Indigenous communities. She described the approach taken by the community legal education team as 'not PowerPoint presentations; it is sitting down discussing and role playing – using interactive adult education techniques – to overcome those literacy and language issues.'[38]

7.38 In contrast to the work being done by Australian Government agencies to raise awareness of financial crimes, Mr Trudgen observed that sadly it was the

---

34 Mr Richard Trudgen, private capacity, *Committee Hansard*, 8 September 2014, p. 17.

35 Mr Richard Trudgen, private capacity, *Committee Hansard*, 8 September 2014, p. 19.

36 Ms Pip Martin, Managing Solicitor-Civil, Northern Australian Aboriginal Justice Agency, *Committee Hansard*, 8 September 2014, p. 21.

37 Mr Richard Trudgen, private capacity, *Committee Hansard*, 8 September 2014, p. 18.

38 Ms Pip Martin, Managing Solicitor-Civil, Northern Australian Aboriginal Justice Agency, *Committee Hansard*, 8 September 2014, p. 22.

criminals themselves who, by working patiently with individuals, were providing more education:

> These crooks are providing better education than what the mainstream system is doing. They actually educate them on how to fill out the forms, to go to the post office. They take them through it step by step. The impact is significant. It is still out there and I think it is right across. The methods and practices are, basically, the same at the moment of mining information as fast as possible.[39]

7.39 Mr Trudgen warned that the need for appropriate language services in awareness raising was not just an issue in north-east Arnhem Land but was likely to be a problem across Australia:

> I am convinced that it is not just East Arnhem Land. Because of my language ability and from being here for a long time, people talk to me and open up to me. I reckon it will be right across North Australia and Central Australia. It is in what we call the 'silent culture zone', which just does not get out into mainstream. It is not heard on the media. It is not there because people are operating in that other language.[40]

7.40 Mr Trudgen's final comments to the committee noted that through empowering Indigenous Australians to have control in safeguarding their own financial assets, many problems may be solved, including the mental health issues related to lack of confidence and falling victim to financial crime.[41]

7.41 Education as a means of preventing crime was also supported by Ms Judy Lind, Executive Director, Strategy and Specialist Capability at the ACC, who stated:

> It is our belief that any further strategy should be focused on prevention and not just focused on the investigation of referrals alone, including raising awareness of the nature of the threats, educating communities and strengthening the environment for which financial crime and exploitation can occur.[42]

7.42 Ms Lind proposed that in addition to education, more could be done with structural mechanisms for increasing accountability and transparency in Indigenous organisations:

> There are measures in place under the [Public Governance, Performance and Accountability Act 2013]. There are measures in terms of independence and requirements for auditing of agencies. We know that some of the funding agreements being entered into in Indigenous communities require

39 Mr Richard Trudgen, private capacity, *Committee Hansard*, 8 September 2014, p. 19.

40 Mr Richard Trudgen, private capacity, *Committee Hansard*, 8 September 2014, p. 18.

41 Mr Richard Trudgen, private capacity, *Committee Hansard*, 8 September 2014, p. 19.

42 Ms Judy Lind, Executive Director, Australian Crime Commission, *Committee Hansard*, 8 September 2014, p. 10.

> quite high levels of checks and balances in relation to those funding agreements.
>
> Some additional preventative measures that could be considered in this environment could include the need for probity checking of directors, secretaries and employees of Indigenous organisations, as well as appointing independent board members to Indigenous organisations; the continued provisioning of targeted governance training to Indigenous organisations, and support to those organisations to try to build governance capabilities and financial literacy; the potential to increase the transparency of royalty payments and land-use agreements so that law enforcement and other regulators can assist communities to attempt to detect and avoid potential areas of exploitation of the huge amounts of money that is flowing into Indigenous communities under those agreements; and the potential need to more systematically identify problem gamblers within those organisations that hold or attempt to hold office, and some mitigating strategies wrapped around those individuals.[43]

Committee view

7.43 The evidence received by the committee indicates that Indigenous communities would benefit from culturally appropriate and targeted financial literacy programs. As witnesses with significant first-hand experience in Indigenous communities explained, there are two major issues regarding the provision of culturally appropriate financial literacy material. The first is that many Indigenous communities access information verbally as opposed to via written form. Secondly, because English is not the primary language in many remote Indigenous communities, mainstream financial literacy materials are likely to be ineffective. To reduce the risk of these communities being targeted by organised criminal groups and fraudsters, financial literacy materials need to be provided in local Indigenous languages, and targeted in an appropriate medium and format.

7.44 Without appropriately translated materials that are delivered in a culturally accessible manner, Indigenous communities across Australia are likely to remain particularly vulnerable to financial related crimes. This in turn puts at risk the wellbeing of Indigenous Australians, and also the government funding across a range of portfolios which is provided to support these communities and organisations.

7.45 The committee agrees with the evidence presented that Indigenous communities require support to develop financial literacy and education, including in local Indigenous languages. These actions would do much to build financial management skills and confidence, as well as assisting Indigenous communities build resilience against the perpetrators of financial related crime.

---

43 Ms Judy Lind, Executive Director, Australian Crime Commission, *Committee Hansard*, 8 September 2014, pp 10-11.

Recommendation 13

7.46 The committee recommends the government fund targeted financial literacy education programs for Indigenous communities. These programs must be translated into local Indigenous languages, be specific to the local community circumstances and be delivered in a culturally appropriate manner.

Governance capabilities of Indigenous organisations

7.47 The lack of financial understanding in individuals becomes a larger problem when financial crimes are transferred to a community controlled organisation. Without basic organisational proficiencies, it is difficult to account for funds and maintain accurate records. Without good governance systems in place, an organisation is susceptible to be the target of organised financial crime from external groups as well as being vulnerable to fraud and other financial crimes from within the organisation itself.

7.48 The committee heard that there is a lack of education and awareness in community-based organisations in Indigenous communities. Ms Martin told the committee that:

> We have been approached by individual directors from Indigenous corporations for advice. From their perspective when they approach us—and it is only a few people—they are not aware of their responsibilities as a director. They are aware of power plays going on but they are not aware of the fact that they can stand up to it in terms of voting and being involved in the decision making of an organisation. So governance is a very important issue.[44]

7.49 Regarding the effect of financial crime on Indigenous organisations, Ms Lind echoed the sentiments expressed by Mr Trudgen[45] about the effect of financial crime on individuals:

> Our broad conclusion is that the impact of financial crime in Indigenous communities cannot be understated, and in some cases can be linked to a decline in living conditions where those frauds have resulted in the removal of funding destined for particular programs that try to address Indigenous disadvantage. Funding by government to Indigenous organisations is often for programs aimed at tackling child abuse, neglect, violence, substance abuse and improving overall Indigenous health and wellbeing. Misappropriations within those organisations can result in failure to deliver these services and a consequent failure to deal with these problems.[46]

---

44 Ms Pip Martin, Managing Solicitor-Civil, Northern Australian Aboriginal Justice Agency, *Committee Hansard*, 8 September 2014, p. 22.

45 See also: Paragraph 7.38

46 Ms Judy Lind, Executive Director, Australian Crime Commission, *Committee Hansard*, 8 September 2014, p. 11.

7.50 Lack of governance creates opportunities for fraud, but can also impede a police investigation which may prevent further losses. Commander Bryson told the committee of the difficulties faced by police in making an investigation into fraud in an organisation with poor governance practices:

> When we have a report of a financial related crime here in the Territory, time and time again we find that a lot of the entities, whether they be incorporated bodies or associations, have extremely poor governance and poor records. That makes it very problematic to conduct a successful investigation and move the matter into the prosecution phase.

7.51 Assistant Commissioner Payne told the committee that oversight of organisations is made by the Department of Business, Northern Territory, which:

> …oversees the [Associations Act] of the Northern Territory. In fact, it has regulatory powers, but, in a general sense, as I understand it, it is a case of ensuring that, on a yearly basis, it provides its end-of-year financials, it is solvent and it is operating as a business.[47]

7.52 Assistant Commissioner Payne went on to explain that it is up to each organisation or association itself to have in place appropriate processes:

> The [Associations Act] requires each association to have a constitution, and the constitution has, essentially, the business rules of the organisation. This is one of our problems. Sorry, generally speaking, when we become involved we have discovered that the organisation was incompetent and made very bad decisions, or there has been criminal activity that has caused the organisation to fail financially.[48]

7.53 Although witnesses differed in their perspectives, all agreed that good governance practices are central to efforts to mitigate the threat faced by organisations from financial crime. From a policing perspective, Commander Bryson told the committee that:

> …there needs to be early intervention and regular auditing and inquisition. The record keeping is extremely poor. Quite often when we go behind and start to look at large sums of money and how they have been acquitted, it is clear that there has been a lack of governance for an extended period of time and that nobody has been in that space for an extended period of time to see exactly how the funds are being dispersed versus what they were granted for and the objective that is sought to be achieved.
>
> From a policing perspective, as I said, normally there is an extended time line between when the conduct was engaged in and when we actually get the report, which is unhelpful. We really need to be in a space, from a

47 Mr Mark Payne, Assistant Commissioner, Crime and Specialist Services, Northern Territory Police Force, *Committee Hansard*, 8 September 2014, p. 7.

48 Mr Mark Payne, Assistant Commissioner, Crime and Specialist Services, Northern Territory Police Force, *Committee Hansard*, 8 September 2014, p. 7.

> community perspective, where we are looking at these things much more regularly and much earlier...[49]

7.54 Ms Martin stressed the importance of governance, education, and mentoring being provided to Indigenous communities to help people build capacity to support themselves:

> NAAJA is one of the organisations involved in a peak organisation called Aboriginal Peak Organisations of the Northern Territory—that is the medical services, the legal services and the land councils. They were given significant funding to set up a governance program to support Aboriginal organisations and train up the directors and provide mentoring. That is a great approach in terms of building up the capacity of Aboriginal corporations so that they can manage the funds to support their people in the range of services that are required.[50]

7.55 However, Ms Martin expressed concern over the fact that once the current funding concludes, NAAJA would have to reapply:

> That funding is finishing, if not in June 2015, in June 2016, and we are, at the moment, having to apply for more funding under the Indigenous Advancement Strategy.[51]

7.56 Mr Trudgen too argued for the need for education, and particularly education in the appropriate language, to help individuals and organisations manage better. But Mr Trudgen, like Ms Martin, observed that without funding, there was no way to deliver education in a meaningful way:

> Unfortunately nobody does this training for Indigenous people, especially remote Indigenous people, except organisations like us that take it on. We have organisations that apparently should be doing it, but they are all English first language and therefore they cannot do it and they do not do it. Our company struggles to survive because we do not get income and we do all these things for nothing. We have to decide what we are going to do, for the sake of closing it down.[52]

7.57 The NIITF report released under FOI notes that Indigenous corporations would likely continue to be exploited by individuals, including board members, who wish to advance personal, family or group interests at the expense of the community.

---

49 Commander Richard Bryson, Northern Territory Police Force, *Committee Hansard*, 8 September 2014 p. 3.

50 Ms Pip Martin, Managing Solicitor-Civil, Northern Australian Aboriginal Justice Agency, *Committee Hansard*, 8 September 2014, p. 21.

51 Ms Pip Martin, Managing Solicitor-Civil, Northern Australian Aboriginal Justice Agency, *Committee Hansard*, 8 September 2014, p. 22.

52 Mr Richard Trudgen, private capacity, *Committee Hansard*, 8 September 2014, p. 17.

The report suggests that members would pressure office holders to approve programs or policies that are not in the best interests of the community.[53]

Committee view

7.58 The committee is greatly concerned by the evidence that Indigenous communities are likely to continue to be victims of financial related crime. This is due to a combination of factors, including the lack of support for, and oversight of, adequate governance arrangements for Indigenous corporations and organisations.

7.59 The committee agrees that it is problematic that Indigenous communities do not feel empowered, have the requisite skills, or have adequate resources to comply with financial accounting requirements.

7.60 The committee commends the NIITF for its detailed work regarding financial related crimes in Indigenous communities. The committee supports the NIITF's recommended remedial actions regarding financial crime in Indigenous communities including recommendations: for ongoing funding for law enforcement agencies to prevent, detect and investigate suspected financial crimes in Indigenous organisations; and to provide targeted governance training to Indigenous organisations.

7.61 The committee believes that the implementation of the NIITF's recommendations regarding financial related crime would require the ongoing involvement of the ACC in collaboration with state and territory law enforcement agencies.

7.62 The recently announced Serious Financial Crime Taskforce could have an alternative role in continuing the financial crime aspects of the NIITF's work, should it be impractical for the ACC to have an ongoing role in this space.

Recommendation 14

7.63 The committee recommends the government implement the recommendations from the National Indigenous Intelligence Task Force report relating to the prevention of financial crime and improved governance in Indigenous organisations.

Mr Craig Kelly MP

Chair

53 ACC, *The Final Report of the National Indigenous Intelligence Task Force*, (released under FOI), 2006–2014, p. 17.

APPENDIX 1

Submissions, additional information and answers to questions on notice[1]

Submissions

Submission Number	Submitter
1	CrimTrac
2	Northern Territory Police
3	National Financial Services Federation
4	Australian Bankers' Association Inc
5	Australian Crime Commission
6	Australian Federal Police
7	Australian Taxation Office
8	Australian Customs and Border Protection Service
9	Attorney-General's Department
10	Australian Transaction Reports and Analysis Centre
11	Customer Owned Banking Association
12	South Australia Police
13	Victoria Police
14	Mr Adrian Cox
15	Remittance Industry Association
16	Veda
17	Reserve Bank of Australia
18	Uniting Church in Australia
19	Office of the Australian Information Commissioner
20	AML Master
21	ASIC

1 www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/Financial_related_crime/Submissions

22 Mr Gregg Smith

23 iDcare

Answers to Question on Notice[2]

1 Answer to Question on Notice from the Australian Customs and Border Protection Service (ACBPS) at a public hearing on 10 September 2014

2 Answer to Question on Notice from the Australian Customs and Border Protection Service (ACBPS) at a public hearing on 10 September 2014

3 Answer to Question on Notice from the Attorney-General's Department at a public hearing on 10 September 2014

4 Answers to Questions on Notice from Australian Transaction Reports and Analysis Centre (AUSTRAC) at a public hearing on 9 September 2014.

5 Answer to Question on Notice from the Attorney-General's Department (received 20 February 2015)

6 Answer to Question on Notice from the Australian Crime Commission (received 18 February 2015)

7 Answer to Questions on Notice from AUSTRAC (received 25 February 2015)

8 Answers to Questions on Notice from ASIC (received 24 March 2015)

Additional Information[3]

1 Tabled document from public hearing in Canberra, ACT on 10 September 2014 from the Australian Taxation Office

2 Annotated Bibliography provided by the Parliamentary Library for the inquiry into Financial related crime

3 Chronology includes major events concerning serious and organised crime relating to the financial sector in Australia - provided by the Parliamentary Library

4 Additional information - Australian Financial Services Federation

---

2 www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/Financial_related_crime/Additional_Documents

3 www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/Financial_related_crime/Additional_Documents

Correspondence[4]

1 Correspondence received from Westpac Relating to financial related crime and the remittance industry

2 Correspondence from the ACCC Chairman Mr Rod Sims re: financial related crime inquiry

4 www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/Financial_related_crime/Additional_Documents

APPENDIX 2

Witnesses who appeared before the committee

Monday, 8 September 2014 – Darwin

Northern Territory Police Force

Mr Mark Payne, Assistant Commissioner, Crime and Specialist Services

Commander Richard Bryson, Crime and Specialist Support Command

Australian Crime Commission

Ms Judy Lind, Executive Director, Strategy and Specialist Capabilities

Mr Stephen Pitkin, Acting Queensland State Manager and former Head of Determination, National Indigenous Intelligence Task Force

Mr Richard Trudgen, Private capacity (via teleconference)

Northern Australian Aboriginal Justice Agency

Ms Pip Martin, Managing Solicitor-Civil

AML Master (via teleconference)

Ms Joy Greary, Director

Tuesday, 9 September 2014 – Sydney

Australian Bankers' Association Inc

Mr Paul Stacey, Policy Director

Mr Guy Boyd, Global Head of Financial Crime, Australian and New Zealand Banking Group Ltd

Mr Damian McMeekin, Head of Group Security, Australian and New Zealand Banking Group Ltd

Mr Steven York, Head of Groups Security and business Resilience, Bank of Queensland

South Australia Police

Mr Paul Dickson, Assistant Commissioner

Reserve Bank of Australia

Mrs Michele Bullock, Assistant Governor (Currency)

Mr Keith Drayton, Deputy Head, Note Issue Department

National Financial Services Federation

Mr Philip Johns, Chief Executive Officer

Ria Financial Services Australia Pty Ltd

Mr Crispin, Head of Compliance, Australia and New Zealand

Mr Eduardo Bieytes Corro, Managing Director

Ms Dianne Nguyen, Director, Head of Compliance, Eastern and Allied Pty Ltd

Veda

Ms Imelda Newton, General Manager, Fraud and Identity Solutions

Ms Tanya Stoianoff, General Manager, External Relations

Mr Matthew Strassberg, Senior Advisor, External Relations

Uniting Church in Australia

Dr Mark Zirnsak, Director, Justice and International Mission Unit, Synod of Victoria and Tasmania

Mrs Gillian Donnelly, Consultant

Australian Transaction Reports and Analysis Centre

Mr John Schmidt, Chief Executive Officer

Ms Liz Atkins, Executive General Manager, Corporate

Mr Peter Clark, Executive General Manager, Operations

Mr John Visser, General Manager, Intelligence

Victoria Police

Mr Steve Fontana, Assistant Commissioner

Wednesday, 10 September 2014 – Canberra

Australian Crime Commission

Mr Chris Dawson, Chief Executive Officer

Mr John Moss, Acting Executive Director, Operations

Mr Richard Grant, National Manager, Investigations

Australian Federal Police

Mr Michael Phelan, Deputy Commissioner Operations

Mr Ian McCartney, Acting Assistant Commissioner, Acting National Manager Crime Operations

Commander Linda Champion, Manager Fraud and Anti-Corruption

Australian Taxation Office

Mr John Ford, Assistant Commissioner, Private Groups and High Wealth Individuals, Tax Crime

Mr Brett Martin, Assistant Commissioner, Indirect Tax, Compliance Strategy and Government Relations

Australian Customs and Border Protection Service

Mr Anthony Seebach, National Manager, Special Investigations and Programs

Mr Bjorn Roberts, Director, Trade Enforcement Unit

Attorney-General's Department

Mr Iain Anderson, First Assistant Secretary, Criminal Justice Division

Mr Andrew Rice, Assistant Secretary, Cyber and Identity Security Policy Branch

Mr Daniel Mossop, Director, Financial Crimes Section, Criminal Law and Law Enforcement Branch