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.