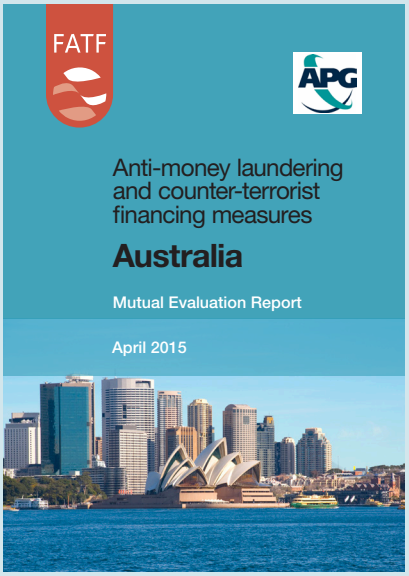
Anti-money laundering and counter-terrorist financing measures - Australia



5. Preventive measures

Effectiveness and technical compliance

Citing reference:

FATF and APG (2015), "Preventive measures" in *Anti-money laundering and counter-terrorist financing measures - Australia,* Fourth Round Mutual Evaluation Report, FATF, Paris and APG, Sydney
www.fatf-gafi.org/topics/mutualevaluations/documents/mer-australia-2015.html

For more information about the FATF, please visit the website: **www.fatf-gafi.org**

5. PREVENTIVE MEASURES

Key Findings

Reporting entities' understanding of their ML/TF risks and the effective implementation of preventive measures varies across and within sectors. The major reporting entities – including the big four domestic banks which dominate the financial sector – have a good understanding of their Australian AML/CTF risks and obligations, which do not all comply with FATF Standards.

Australia's requirements on CDD, beneficial ownership, and the requirements for PEPs were enhanced on 1 June 2014. Most of the reporting entities interviewed by the assessment team advised that they are not yet able to apply the improved requirements; they have a transition period until 31 December 2015. Therefore, those reporting entities that are applying the pre-June 1 measures are not adequately identifying beneficial owners or applying CDD to PEPs.

DNFBP sectors, other than casinos and bullion dealers, including those assessed as high risk in the NTA, are not subject to AML/CTF regulation, and have demonstrated a poor understanding of their ML/TF risks. Australia should establish comprehensive AML/CTF obligations for all DNFBPs as a matter of priority.

5.1 Background and Context

(a) Financial Sector and DNFBPs

5.1. Australia's financial sector is the 12th largest in the world, and is dominated by banks. Total banking sector assets amount to over 200% of GDP (over AUD 321.1 billion). Australia's banking sector is the third largest in the Asia-Pacific region, following Japan and China, and is highly concentrated, with the four largest banks accounting for 78% of the total banking assets. The Australian banking system comprises a mix of domestic and foreign players, with 48 of the 68 licensed banks being subsidiaries or branches of foreign banks.

Table 5.1. Type of Financial Institutions Authorised to Conduct Financial Activities and Operations

Type of financial institution	No. of entities
Banks Australian owned banks Foreign Subsidiary Banks Branches of Foreign Banks	68 20 8 40
Building Societies	9
Credit Unions	85
Specialised credit card institutions	2
Other authorised deposit-taking institutions	4
Finance companies – Australian Credit Licensees	5 856
Authorised Credit Representatives	28 201
Lease Finance Companies – Credit Licensees Providing Consumer Leases	4 102 With 19 330 authorised representatives
Money Remittance Companies	6 230
Australia Financial Securities Licensees	5 093
Financial Markets	18
Clearing and Settlement Facilities	6
Market Dealers	136 market participants
Securities Dealers	800
Friendly Societies	12
Superannuation Funds and Trustees	200 superannuation fund trustees 53 Pooled Superannuation trusts 2 979 small APRA funds 62 Single-member authorised deposit funds 528 701 self-managed superannuation funds
Funds Managers	
Managed Investment Schemes (trustees)	784 494 responsible entities for MIS
Registered Managed Investment Schemes	4 152
Foreign Financial Service Providers	614

Table 5.1. Type of Financial Institutions Authorised to Conduct Financial Activities and Operations (continued)

Type of financial institution	No. of entities
Custodial Service Providers	718
Investment Banks	26
Hedge Fund Managers	250
Retail Over-the-Counter (OTC) Derivative Providers	43
Life insurers / Life Insurance Brokers/ Life Insurance Agents	28
Foreign exchange contracts – Australian Financial Services License holders	1 079
AFS Authorised Representatives	7 853
Money and currency exchange providers – bureaux de change	108

5.2. Australia is one of the major centres of capital market activity in the Asia Pacific region. Annual turnover across Australia's financial markets was AUD 135 trillion in the year to June 2013. Australia's total stock market capitalisation is more than USD 1.3 trillion, making it the 10th largest market in the world and the 4th largest in the Asia Pacific region. Australia's foreign exchange market is ranked 8th in the world by turnover, with the AUD/USD the fourth most actively traded currency pair in the world by turnover.

5.3. Australia has a large number of remittance providers which provide an important service to Australia's significant multicultural society. MVTS are offered by remitters, which fall into three types: remittance network providers (RNPs); agents or affiliates of the RNP; and independent remittance providers. Over 6 000 reporting entities registered with AUSTRAC operate in the remittance sector in one of these three categories. More than 5 500 of these entities are agents or affiliates of RNPs and the value of transactions flowing through the remittance sector is relatively concentrated. The top five networks account for 90% of all MVTS. The top 14 remitters account for 83% of the value of funds transferred in and out of Australia through the remittance channel. Outside of these networks, there are approximately 650 independent remitters registered with AUSTRAC. In terms of value, international funds transfers through remitters accounted for 1.7% or AUD 66 billion of over AUD 3.9 trillion aggregate international funds transfers in 2013. The banking sector accounts for more than 95% of the total cross-border funds transfers.

5.4. The NTA highlights banks, the gaming sector, and remitters as the main channels for ML (and also for TF through the remitters). Specifically, the NTA appears to have been a substantial driver for the creation of the Eligo National Task Force in December 2012. As noted earlier, the four largest banks are domestic banks and account for 78% of total banking assets and 66% of the international funds transfers by value. AUSTRAC has a dedicated team called Major Reporters, which regulates the 19 most significant reporting entity groups (REGs) comprising mainly the major Australian and foreign banks. In considering the risk and context of the financial sector, assessors gave greater material importance to the domestic banks and remitters.

5.5. Most of the DNFBPs operate in Australia. As highlighted under IO.1, the real estate sector has been identified by authorities as a high ML/TF risk, and professional facilitators (lawyers, accountants, trust and company service providers – especially from lower tier firms) were almost universally considered a major risk for ML. The real estate sector in Australia was also identified as an attractive avenue for investments, including by organised crime groups looking to launder illicit monies. As a result, the assessors viewed these sectors as materially important in determining effectiveness.

Table 5.2. DNFBPs: Type and number of entities

Type of Entity	Number of entities
Casinos	12
Lawyers	The Law Council acts on behalf of approx. 56 000 legal practitioners
Notaries	Approx. 260
Accountants	Institute of Public Accountants – over 25 000 members in 50 countries Certified Practicing Accountants Australia – over 150 000 in 121 countries Institute of Chartered Accountants Australia – over 73 000 members globally
Precious Metals & Stones Dealers	82 Bullion Dealers Jewellers Association of Australia - 1 100 outlets
Trust and Company Service Providers	Approx. 300 company formation agents.
Real Estate Agents	35 019

(b) Preventive Measures

5.6. Australia's AML/CTF regime has undergone significant reform since the last assessment in 2005. The most important reform was the enactment of the AML/CTF Act in 2006, which expanded the scope and coverage of Australia's AML/CTF regime. Businesses with AML/CTF obligations increased from approximately 3 000 under the previous AML/CTF regime to about 15 000 under the AML/CTF Act. The AML/CTF Act focuses on the services to be regulated – called "designated services" in the Act – rather than the nature of the entity that provides the service. In broad terms, the AML/CTF Act applies to the services provided by financial institutions, gambling service providers, bullion dealers and remittance dealers. Entities that provide these designated services are known as reporting entities and are supervised by AUSTRAC for compliance with the Act. Beyond bullion dealers and gambling services, including casinos, other DNFBPs (i.e. real estate agents, dealers in precious stones, lawyers, notaries, other legal professionals and accountants, and trust and company service providers) are only covered when they provide one of the designated services – i.e. essentially acting in the capacity of a financial institution under the FATF Recommendations. None of the services designated relates to real estate agents, dealers in precious stones or trust and company service providers activities.

5.7. The AML/CTF Act requires REs to establish an AML/CTF programme, which is divided into two parts – Part A and Part B. The primary purpose of Part A of the standard AML/CTF programme is to identify, mitigate and manage ML/TF risks that a reporting entity faces and includes AML/CTF risk awareness training for employees, employee due diligence program, oversight by boards and senior management, and procedures for independent review of programme. The primary purpose of Part B is to set out the reporting entity's applicable customer identification procedures (ACIP), including beneficial ownership, ongoing customer due diligence and enhanced due diligence. A standard programme applies to a particular RE; joint programmes apply to each reporting entity that belongs to a particular DBG .

5.8. The AML/CTF Act is supplemented by the *AML/CTF Rules Instrument 2007* (AML/CTF Rules), issued by AUSTRAC's CEO pursuant to section 229 of the AML/CTF Act. The AML/CTF Rules expand on the requirements and provide greater specificity with respect to some of the obligations in the AML/CTF Act. For example, the AML/CTF Rules set out the requirements on reporting entities' risk assessments, and include provisions on their adoption of a risk-based approach.

5.9. The AML/CTF Rules were updated on 15 May 2014 via the *AML/CTF Rules Amendment Instrument 2014 (No.3)* (Rules Amendment). The Rules Amendment updated a number of the preventive measure requirements, including those related to customer identification, beneficial ownership, and the provisions of Part A of the AML/CTF program. The Rules Amendment commenced on 1 June 2014 but REs have until 1 January 2016 to fully implement the requirements before certain sanctions will be applied.

(c) Risk-Based Exemptions or extensions of preventive measures

5.10. Casinos and bullion dealers are the only categories of DNFBPs subjected to AML/CTF requirements, including the requirement to establish AML/CTF programmes to mitigate ML/TF risks. Other DNFBP sectors such as lawyers, accountants, real estate agents, and trust and company service providers are not subject to such obligations, which is in direct contrast to their assessment as a high threat in the NTA and the risk-based approach. On the regulated sectors, Australia sets the threshold for CDD requirements to be applied to customers of casinos at AUD 10 000 (USD 9 300 / EUR 6 900), which exceeds the USD / EUR 3 000 threshold in the FATF Recommendations. Persons licensed to operate gaming machines are also not subject to most of the AML/CTF obligations under the Australian regime if they operate no more than 15 such machines, although there are State and Territory-level restrictions on winnings paid in cash.

5.11. AUSTRAC has the powers to grant exemptions to specified persons from all or parts of the AML/CTF Act. In practice, it has granted full or unconditional exemptions to various applicants, including those operating in private banking, prepaid cards or investment funds. According to the AUSTRAC Exemption Policy, exemptions are considered based on a number of factors, including – but not limited to – the risk profile of the applicant, the designated service, issues of competitive neutrality, and the level of regulatory burden to which the applicant is being subjected. While AUSTRAC considers these exemptions on a case-by-case basis, the assessment team was not convinced that the exemptions were sufficiently justified as low risk.

5.2 Technical Compliance (R.9-23)

5.12. See for the full narrative the technical compliance annex:

- **Recommendation 9 (financial institution secrecy laws) is rated compliant.**
- **Recommendation 10 (customer due diligence) is rated partially compliant.**
- **Recommendation 11 (record-keeping) is rated largely compliant.**
- **Recommendation 12 (politically exposed persons) is rated largely compliant.**
- **Recommendation 13 (correspondent banking) is rated non-compliant.**
- **Recommendation 14 (money or value transfer services) is rated largely compliant.**
- **Recommendation 15 (new technologies) is rated largely compliant.**
- **Recommendation 16 (wire transfers) is rated partially compliant.**
- **Recommendation 17 (reliance on third parties) is rated partially compliant.**
- **Recommendation 18 (internal controls and foreign branches and subsidiaries) is rated partially compliant.**
- **Recommendation 19 (higher risk countries) is rated partially compliant.**
- **Recommendation 20 (reporting of suspicious transactions) is rated compliant.**
- **Recommendation 21 (tipping-off and confidentiality) is rated compliant.**
- **Recommendation 22 (DNFBPs – customer due diligence) is rated non-compliant.**
- **Recommendation 23 (DNFBPs – other measures) is rated non-compliant.**

5.3 Effectiveness: Immediate Outcome 4 (Preventive Measures)

5.13. The AML/CTF Act requires reporting entities to perform regular risk assessments. This entails assessing the risk of the reporting entity being involved in or facilitating ML or TF, and determining what the reporting entity will need to do to identify, mitigate, and manage those risks. The AML/CTF Rules specify that in its risk assessment a reporting entity must consider its customer types, the types of designated services it provides, the methods by which it delivers designated services and the foreign jurisdictions with which it deals.

5.14. **Financial institutions' and DNFBPs' understanding of ML/TF risks and measures to mitigate them varies across sectors.** Financial sector representatives demonstrated a better understanding of their ML/TF risks and were better at identifying steps to mitigate and manage those risks. Most DNFBPs that are not subject to prudential or AML/CTF regulation or supervision did not demonstrate an adequate understanding of their ML/TF risks.

5.15. **The understanding of risks and measures also vary across reporting entities within the respective sectors, depending on the scale and complexity of their operations.** Across the board, larger reporting entities demonstrated a better understanding and ability to mitigate their identified ML/TF risks.

5.16. **Across sectors it was reported to the assessment team that smaller reporting entities found it challenging to understand and meet all the AML/CTF requirements.** AUSTRAC has undertaken a large number of outreach strategies to communicate with small to medium reporting entities, including compliance guides for small bookmakers, independent remitters and clubs and hotels and outreach to industry associations. Nevertheless, the small to medium reporting entities have a lower level of understanding of their obligations and risks. To a large extent this is as a result of the inherent characteristics of smaller entities that do not have the capacity to maintain the wide range of compliance resources and capabilities employed by larger entities. Both large and small reporting entities interviewed suggested that insufficient regulatory and enforcement presence was a contributing factor. The larger reporting entities enjoy close working relationships with AUSTRAC and the law enforcement agencies, which enhances their ability to understand the authorities' views on risk. The same opportunity is not as available to the smaller reporting entities, which rely on the NTA and the published AUSTRAC guidance and typologies for insight into how the authorities assess risk. While reporting entities indicated that the guidance and typologies were generally useful, they all noted that these materials could be clearer and more up-to-date.

5.17. **DNFBP sectors that are not subject to the AML/CTF regime generally demonstrate a poor understanding of ML/TF risks.** Most were unaware of the NTA or its findings that many of the unregulated DNFBPs are a high risk for ML. Those that were aware of the NTA disagreed with its conclusions, citing the lack of clear evidence in typologies reports or criminal prosecutions to justify the assessment. Nearly all of these sectors asserted that the ML/TF risks in their respective sectors are low, as they handle no or minimal cash transactions. They also claimed that the current professional standards for their sectors sufficiently protect the sector from abuse by criminals.

5.18. *Banks* – **Banks operating in Australia generally have a sufficient understanding of the ML/FT risks of their clients, and have a framework in place to mitigate them**. In addition, large banks demonstrated a better understanding of their AML/CTF obligations and had the resources to effectively implement them. This was significantly more challenging for small to medium sized banks due to more limited resources and capacity, as well as the complexity of the requirements laid out in the AML/CTF Act and the AML/CTF Rules.

5.19. **Domestic banks did not have measures that fully meet FATF Standards on CDD, beneficial owners and politically-exposed persons**. This appeared to be due to Australian-based banks limiting the scope of their ML/TF assessment to the scope of the requirements as outlined in AML/CTF Act and Rules. International banks whose home jurisdictions comply with these relevant Standards generally considered a wider array of factors when reviewing the ML/TF risks of their bank and its business lines.

5.20. *Money and Value Transfer Services* – **Within the remittance sector, the ability to adequately assess risk varies widely.** Large RNPs with global operations seem to adequately identify and mitigate the

risk associated with their product lines and their customers (the five largest RNPs in Australia account for 90% of affiliates). For example, large RNPs will have varying thresholds for enhanced due diligence based on transaction corridor, or customer type based on internally determined risk profiles. Such approaches are less likely in smaller RNPs and independent remitters, but they make up only a limited part of the sector.

5.21. In 2011, regulatory changes were implemented to strengthen the remittance registration process. The criteria applied to registration changed and the AUSTRAC CEO was given the capacity to refuse, cancel, suspend or impose conditions on registration. RNPs were included in the registration process and the compliance obligations of agents/affiliates shifted to the RNP. This included requiring RNPs to undertake due diligence on their affiliate (including requiring RNPs to obtain criminal records checks of all key personnel within their affiliates), providing the agent/affiliate with a compliance program, monitoring agent compliance, training agents, and conducting transaction monitoring of their entire network.

5.22. The 2011 regulatory changes improved the ability of AUSTRAC to monitor the remittance sector and improved implementation of obligations. However, representatives from the sector reported to the assessment team that **implementation of obligations in line with the FATF Standards continues to vary greatly within the sector.** A number of larger remitters and RNPs implement obligations in line with the FATF Standards. Smaller remitters – which account for a small part of the sector – lack capacity to implement Australia's complex regulatory requirements and do not implement preventive measures in line with the FATF Standards.

5.23. In line with Australia's AML/CTF Rules, money remitters are implementing the Australian obligations for wire transfers and the filing of IFTIs, but the existing Rules are not in line with the requirements of Recommendation 16. Smaller remitters were universally identified by the authorities and the private sector as less compliant with Australian AML/CTF obligations and highly vulnerable to ML.

5.24. To improve compliance throughout the remittance sector, sector participants are considering the creation of a professional association of remitters. In addition to furthering compliance, an association would further establish professional standards and would act as an advocate for the sector.[1]

5.25. *Casinos* – The casino sector has been identified by the NTA and AUSTRAC as high risk and is therefore supervised more intensively, especially over the last two years. One of the **larger casinos in Australia demonstrated a good understanding of its AML/CTF obligations** and reported having more stringent AML/CTF measures than what the law required in some aspects. For instance, they set lower cash thresholds for CDD triggers, or have wider scope of due diligence. This is driven in part by their desire to better manage business and reputation risks in their activities, and/or to ensure the chances of success in renewing or holding on to their licences. Given the relatively small number of casino operators and AUSTRAC's supervisory focus on this sector, the discrepancy among casino operators in implementing AML/CTF measures that are commensurate with their scale and ML/TF risks is unlikely to be as large as in some other sectors.

5.26. *Bullion dealers* – Bullion dealers are regulated by AUSTRAC and are required to comply with AML/CTF obligations. Consistent with feedback from most private sector representatives, the larger bullion dealers attract regular scrutiny from AUSTRAC, and are likely to demonstrate better understanding of their AML/CTF obligations and have adequate AML/CTF safeguards as a result. Insufficient information was provided for the assessors to establish whether smaller bullion dealers implement AML/CTF measures commensurate with their activities and ML/TF risks. The characteristics of small bullion dealers are consistent with other small reporting entities – the understanding of obligations and compliance levels are expected to be lower than it is for the larger players.

5.27. *Other DNFBPs* (lawyers, accountants, real estate agents, trust and company service providers, dealers in precious stones) – These DNFBPs are not subject to AML/CTF requirements or supervision and, with limited exceptions, demonstrated a low understanding of their respective ML/TF risks.

1 In October 2014, the Australian Remittance and Currency Providers Association Limited was established with 50 members from RNPs and independent remitters.

5.28. Some sectors, such as the legal and accounting profession, are of the view that they are subject to stringent professional standards that are sufficient to manage any potential ML/TF risks and/or allow them to adequately know their customers. However, the sector representatives were unable to demonstrate to or convince the assessors how existing professional standards were sufficient to mitigate ML/TF risks over and above their personal business interests, or had enabled them to be an effective contributor in combating system-wide ML/TF risks. These sectors do not see themselves as having a gatekeeping role to prevent ML/TF, and felt this is the responsibility of the financial sector, on the basis that most funds are expected to flow through the financial system.

5.29. Other sectors like the business incorporators (i.e. trust and company service providers) reported having a fairly good understanding of their customers, given the nature and simplicity of the services that they provide.

5.30. On the whole, however, there is no conclusive evidence that these non-regulated DNFBPs are rejecting customers due to suspected ML/TF activities. They also do not have obligations to report suspicious matters to AUSTRAC, and do not do so in practice.

Requirements on CDD and PEPs

5.31. **Financial institutions' and DNFBPs' existing measures on customer due diligence and identification of beneficial owners and PEPs are not in line with FATF Standards.** As mentioned above, the Rules Amendment commenced on 1 June 2014. The implementation period is outlined on the AUSTRAC website and is accompanied by policy principles issued by the Minister for Justice. The policy principles indicate that certain enforcement action – being an application for a civil penalty order or an injunction, the issuing of a remedial direction, or the imposition of a requirement to undertake an external compliance audit – will not be taken by the AUSTRAC CEO during the period of the policy principles for breaches of the additional CDD requirements, provided the reporting entities demonstrate that they have taken "reasonable steps" to comply by 1 January 2016. What constitutes "reasonable steps" is also set out in the policy principles and includes requiring reporting entities to have adopted a board approved transition plan to comply setting out how it will reach compliance with the new obligations. The transition plan was required to have been adopted by 1 November 2014. Also, where reporting entities are able to comply with the provisions through their existing operations, they must do so to demonstrate that they have taken reasonable steps. In addition, high-risk customers on-boarded by a reporting entity after 1 June 2014, but prior to the full implementation of the new obligations, are required to be retrospectively identified at the level required by the new obligations.

5.32. Based on interviews with reporting entities, assessors determined that at the time of the onsite a majority of reporting entities were not able to fully implement the requirements in the Rules Amendment; most continue to operate under the pre-June 1, 2014 requirements. While all the reporting entities endeavour to be in compliance as soon as possible, Australia-based reporting entities generally responded that they were unlikely to be able to comply with the new requirements ahead of 1 January 2016. Most sector representatives indicated that enforcement action would be taken against them if they took until that time to implement them. See also the preamble to Section 5 of the TC Annex. A number of international reporting entities noted that they were already implementing a number of the requirements based on their foreign obligations, and expected to be in compliance with the Rules relatively quickly.

5.33. The Rules Amendment expands on the CDD requirements with respect to the identification of the beneficial owner and the PEPs requirements, which are more in line with the FATF standard on Recommendations 10 and 12. However, even under the updated rules, several deficiencies remain as outlined in Recommendation 10.

Record Keeping

5.34. **The larger reporting entities appear to have adequate record keeping measures in place, while some smaller entities have weaker record keeping procedures.** In demonstrating that reporting entities in general had effective record keeping measures in place, AUSTRAC provided information on a range of sectors. Of 68 on-site and off-site assessments conducted on major reporters since 2009, record-keeping deficiencies did not seem to be a key weakness across the major reporters. Only 16 requirements

were issued relating to record keeping requirements. The number of recommendations issued by AUSTRAC to reporting entities to remediate record-keeping requirements in 2013/14 is also relatively low compared to other obligations, such as identification procedures and reporting obligations. These suggest that the major reporters do not have major difficulties with meeting record keeping requirements. Private sector representatives reported anecdotal feedback on limited capacity of smaller players to cope with obligations in the AML/CTF Act in general. Law enforcement's experience was that, with the exception of many smaller remitters, most reporting entities kept fairly good records.

5.35. On average across all industry sectors, 90% of reporting entities that lodged compliance reports to AUSTRAC to report their compliance with AML/CTF obligations in 2012 reported that they retain records of all customer identification information. While this proportion has improved over time, this suggests that some reporting entities (most likely the smaller ones) may not be meeting basic record keeping obligations fully.

Other Measures

Correspondent banking

5.36. Financial institution representatives did not highlight any major challenges or difficulties in instituting measures for correspondent banking under the AML/CTF Act and AML/CTF Rules. AUSTRAC identified very few breaches of correspondent banking obligations in 2013/14. Based on AUSTRAC's understanding, financial institutions would adopt a risk-based approach to determine the extent of due diligence that is required with respect to correspondent banking. Interviews with the sector indicate that Australian rules on correspondent banking are being implemented. It should however be noted that the AML/CTF Act correspondent banking requirements are not in line with the FATF Standard; as a result the measures implemented by reporting entities may not meet the FATF standard, even if they meet Australia's requirements.

New technologies

5.37. Sector representatives whom the assessors interviewed did not report particular difficulties in applying AML/CTF measures for new technologies. Before introducing a new designated service, delivery method or technology, larger reporting entities would typically conduct a product risk assessment that included ML/TF risk, and determine the controls needed to mitigate these risks.

Wire transfer rules

5.38. Sector representatives indicated that the information accompanying cross-border wire transfers seems to comply with Australian requirements. However, the Australian requirements are not in line with the FATF Standard. In some cases, especially with respect to large, international financial institutions, the information accompanying a wire transfer exceeds the Australian requirements and may be in line with the FATF Standards. Representatives for banks and remitters were aware of the Australian requirements regarding the filing of international funds transfer instructions (IFTI) reports with AUSTRAC.

Targeted financial sanctions (TFS)

5.39. As noted under IO.10, reporting entities were generally aware of their obligations with respect to the DFAT sanctions lists. Under section 41 of the *Charter of the United Nations (Dealing with Assets) Regulation 2008* using a process agreed to by DFAT, the AFP, the Australian Bankers' Association and major banks, reporting entities should contact AFP if there was a question about whether they had a match with the Consolidated List. Only a few reporting entities were aware that the AFP is the point of contact. However, it was universally reported by both the public and private sector that DFAT is responsible for enforcement of TFS and that reporting entities were not being monitored for compliance with TFS obligations.

5.40. AUSTRAC's role in relation to TFS is limited to its FIU activities – DFAT is a partner agency of AUSTRAC for these purposes. From a regulatory perspective, AUSTRAC would only have a role in monitoring the compliance with TFS obligations to the extent that an entity failed to lodge an SMR where it has formed a suspicion relevant to a breach of the laws related to TFS. In some limited instances during its regulatory

engagements, AUSTRAC has identified possible breaches of sanctions during its compliance assessments. In two instances, reporting entities were involved in sending transactions to sanctioned Iranian banks. Warning letters were issued by AUSTRAC in relation to these matters. Of the two instances, one entity ceased trading and closed accounts, and the second entity ceased the relationship with the Iranian bank. No further action was taken (by AUSTRAC). AUSTRAC has also taken sanctions matters into account in determining registration decisions related to particular remitters.

Higher risk countries

5.41. Larger reporting entities that employ risk models usually use multiple data sources to assess jurisdiction risks, to a large extent based on their experience with foreign regulators. Based on AUSTRAC's understanding, the FATF International Cooperation Review Group list of jurisdictions carries a significant weighting in such assessments. The outcomes of these risk assessments are used to guide their business and customer on-boarding decisions. Smaller entities with less sophisticated measures are likely to rely only on DFAT's list and guidance to identify higher risk countries.

Suspicious Transaction Reporting Obligations and Tipping Off

5.42. **Reporting obligations are generally well understood by FIs and DNFBPs and they are filing SMRs.** As AUSTRAC is both the FIU and the AML/CTF regulator, reporting of SMRs and other reporting obligations such as IFTIs and TTRs (i.e. quality of the reporting) is often the focus of its engagement with financial institutions and DNFBPs. In this regard, the quality and volume appears to meet AUSTRAC's expectations. Overall, the assessors felt that reporting entities were effectively implementing the SMR requirements.

5.43. **On the other hand, the number of recommendations that AUSTRAC issued to reporting entities to remediate reporting obligations is the second highest among all obligations in 2013-14.** This may be a result of AUSTRAC's focus on reporting obligations and the IFTI obligation. Based on feedback gathered, the timeliness of SMR reporting varies according to reporting entities. It is also influenced by the complexity of the transactions and when a suspicion is formed. Some reporting entities, particularly the major financial institutions, will contact AUSTRAC and provide notice of an impending SMR that they consider a priority. Some financial institutions and remitters will reportedly contact law enforcement agencies before submitting an SMR to ensure that they are capturing and reporting adequate information. Private sector representatives also reported having good communication channels with AUSTRAC and other law enforcement agencies, and sharing of transaction details or records on an ad hoc basis to facilitate their investigations.

5.44. Universally, the private sector highlighted the need for information and more timely feedback from AUSTRAC and law enforcement agencies to improve their transaction monitoring systems for detecting ML and TF. Reporting entities specifically noted challenges in detecting TF in the absence of specific information, and putting in place effective measures to prevent them.

5.45. With respect to the quality of reporting, AUSTRAC considers that most medium to large reporting entities provide sufficient information and context for the SMRs submitted. Missing information usually relates to insufficient detail on the subject of the report, but does not appear to have significant adverse impact on the relevance or value of the SMRs. Overall, the reports received by AUSTRAC – including SMRs, TTRs and IFTIs – form a fundamental pillar of financial intelligence (see also IO.6).

5.46. Reporting entities are aware of the prohibitions against tipping off and have included the provisions in their internal policies, controls and trainings. A number of the large, international REs noted that the scope of the tipping off provisions have required them to have exemptions from the global AML/CTF programmes, as notifying the parent or home office of the institutions about SMRs would violate the provisions.

Internal AML/CTF Controls

5.47. Reporting entities are aware of their requirement to have AML/CTF programmes – as outlined earlier under this IO – to ensure compliance with their obligations under the AML/CTF Act. They are also

aware of their obligation to submit compliance reports to AUSTRAC annually. REs reported having screening procedures when hiring new employees, ongoing training programmes and independent audit functions.

5.48. Reporting entities that are headquartered outside Australia and subject to AML/CTF regulation and supervision elsewhere generally reported having benefitted from comparing and contrasting guidance and requirements imposed by their home or other host jurisdictions, and adapting sound or best practices and applying them to their Australian operations. As a result, a number of these entities are implementing internal controls in line with FATF Standards, even when the Australian requirements do not meet the standard.

5.49. Reporting entities headquartered in Australia with cross-border operations include their overseas branches in their AML/CTF programmes. However, they reported that they have not extended their internal controls to their foreign subsidiaries, on the basis that they are separate legal entities from the Australian parent and because it is not a requirement under the Australian regulatory regime. It also appears that they have not adopted the more stringent of Australian or host jurisdiction rules in their group-wide AML/CTF framework on areas where host country requirements are stricter or more in line with FATF Standards.

5.50. Due to confidentiality provisions in Australia laws, reporting entities are not permitted to share their SMR information and details with their overseas operations unless they are branch operations. This relates to both Australian headquartered as well as foreign entities operating in Australia. Private sector representatives reported to the assessors that this restriction has impeded the efficiency and effectiveness of their group-wide AML/CTF controls. However, assessors noted that Australia's tipping off provision is in line with the FATF Standard. Authorities also note that reporting entities often share information with other parts of the REG about matters triggering alerts without sharing specific information that an SMR has been filed.

Overall conclusions on Immediate Outcome 4

5.51. Australia exhibits some characteristics of an effective system for applying preventive measures in financial institutions and DNFBPs. In general, the major reporting entities and other high risk reporting entities subject to more regular supervisory engagement appear to have a reasonable understanding of ML/TF risks and preventive measures that comply with the Australian AML/CTF regime. Reporting entities have demonstrated that they are aware of their requirement to have AML/CTF programmes and reported having implemented the necessary internal AML/CTF controls. However, a number of aspects of the AML/CTF regime – including those that relate to internal controls, wire transfers, correspondent banking, etc. – do not meet FATF Standards. As a result, reporting entities' implementation of AML/CTF measures will not meet the FATF Standards if its internal controls are developed solely to meet the Australian requirements. In addition, while the requirements have been revised with respect to CDD and PEPs, none of the reporting entities reported they were able to fully implement these requirements at the time of the onsite. As a result, at the time of the onsite visit, reporting entities were working to transition from the pre-June 1 AML/CTF Rules, which were not in line with the FATF Standards. At the same time, a lot of reliance is placed on the banking and financial sector as gatekeepers due to the absence of AML/CTF regulation and requirement on key high-risk DNFBPs such as lawyers, accountants, real estate agents and trust and company service providers. As a result of these factors, the effectiveness of the preventive measures in the financial system as a whole and DNFBPs is called into question to some extent.

5.52. **The overall rating is therefore a moderate level of effectiveness for Immediate Outcome 4.**

5.4 Recommendations on Preventive Measures

5.53. The following recommendations are made on preventive measures (IO.4):

- Ensure that lawyers, accountants, real estate agents, precious stones dealers, and trust and company service providers understand their ML/TF risks, and implement effective AML/CTF obligations and risk mitigating measures in line with the FATF Standards. Among others, persons and entities in these sectors should be able to demonstrate that they are effectively refusing businesses on ML/TF grounds or when CDD is incomplete, in addition to their own business or reputation considerations.

In addition, they should be required to report suspected proceeds of crime and funds in support of terrorism to competent authorities in a swift manner. Last but not least, the effectiveness of the controls and measures that they put in place should be subject to sufficient monitoring and supervision to ensure compliance.

- Ensure that reporting entities implement preventive measures in line with the FATF Standards.
- Ensure that reporting entities implement as early as possible before 1 January 2016 the obligations on enhanced CDD, beneficial owner, and politically exposed persons introduced on 1 June 2014.
- Monitor and ensure that reporting entities headquartered in Australia with cross-border operations to ensure that their overseas branches and subsidiaries have effective AML/CTF programs and risk mitigation measures in place as required under the AML/CTF Act.
- Improve the feedback and guidance to reporting entities on reporting quality and volumes of SMRs and reinforce this feedback loop into their ML/TF risk identification and the effectiveness of their AML/CTF programmes.

5. PREVENTIVE MEASURES

Preamble

a5.1. **Scope of financial institutions –** The chart below sets out the types of entities and persons who carry out the financial activities listed in the Glossary to the Methodology, as well as the licensing authority. Australia advised that debit and credit card schemes (see item 5 below) are licensed by ASIC and supervised for ML/TF purposes by AUSTRAC; however, representatives of such institutions met during the visit to Australia informed the team that they are not regulated or supervised by Australian authorities. AUSTRAC is the supervisory authority for AML/CTF.

Table A5.1. Types of entities and persons who carry out financial activities

Activities and operations according to the FATF definition of financial institutions		Financial institutions authorised to conduct these activities and operations	Licensing authority
1.	Acceptance of deposits and other repayable funds from the public	Banks [1] (or authorised deposit-taking institutions (ADIs)): 20 Australian-owned Banks 8 Foreign Subsidiary Banks 40 Branches of Foreign Banks	APRA
		9 Building Societies (ADIs)	APRA
		85 Credit Unions (ADIs)	APRA
		4 Other ADIs	APRA
2.	Lending	Banks (or ADIs) see item 1 above	APRA
		9 Building Societies (ADIs)	APRA
		85 Credit Unions (ADIs)	APRA
		2 Specialist credit card institutions (ADIs)	APRA
		Finance companies [Total of 5 856 Australian Credit Licensees and 28 201 authorised credit representatives, including ADIs, of which 4 102 licensee provide consumer leases]	ASIC
3.	Financial leasing	Lease finance companies	ASIC
4.	Money or value transfer services	6 287 Money remittance companies, including hawala ADIs	AUSTRAC
5.	Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money)	ADIs, including specialist credit card institutions	APRA
		Debit and credit card schemes (e.g. Visa, Mastercard, Bankcard) Electronic payment systems providers (e.g. BPAY, Paypal) 641 Ancillary non-cash payment facility providers e.g. phone companies (paying for meter parking or vending machine purchases by SMS), providers of prepaid phone card, providers of gift vouchers etc.	ASIC

1. The size of the activity (assets) is as follows: banks - AUD 3214.1 billion; Building Societies - AUD 23.2 billion; Credit Unions - AUD 41.0 billion; Other ADIs and Specialised Credit Card institutions - AUD 7.7 billion; life insurance - AUD 273.9 billion

Table A5.1. Types of entities and persons who carry out financial activities (continued)

Activities and operations according to the FATF definition of financial institutions		Financial institutions authorised to conduct these activities and operations	Licensing authority
6.	Financial guarantees and commitments	Banks	APRA
7.	Trading in: money market instruments (cheques, bills, certificates of deposit, derivatives etc.); foreign exchange; exchange, interest rate and index instruments; transferable securities; commodity futures trading	ADIs Investment banks/firms (securities/derivatives dealers/ market makers) Money market firms (foreign exchange derivatives dealers/market makers) - 26 investment banks, 250 hedge fund investment managers/ responsible entities, 43 retail (over-the-counter) OTC derivative providers 1 079 AFSL holders are authorised to provide financial product advice or deal in foreign exchange contracts. These licensees have 7 853 authorised representatives.	ASIC
8.	Participation in securities issues and the provision of financial services related to such issues	18 financial markets 6 clearing and settlement facilities 136 market participants 800 securities dealers	ASIC
9.	Individual and collective portfolio management	12 Friendly societies	APRA
		28 Life insurers	APRA
		Superannuation funds and trustees: 53 Pooled superannuation trusts 2 979 Small APRA funds 62 Single-members ADFs	APRA
		528 701 Self-managed superannuation funds 200 superannuation fund trustees	ATO
		4 789 Investment advisors (3,394 AFSL holders licensed to provide personal advice and 1,395 AFSL holders licensed to provide general advice)	ASIC
		Funds managers	ASIC
		784 Managed investment schemes (trustees) 4 152 registered managed investment schemes, 494 responsible entities for MIS (as of July 2013), 614 foreign financial service providers, 718 custodial service providers, 26 investment banks, 250 hedge fund managers, and 43 retail OTC derivative providers	ASIC
10.	Safekeeping and administration of cash or liquid securities on behalf of other persons	Licensed financial service providers including: 718 custodial service providers 483 Managed investment operators (responsible entities)	ASIC

Table A5.1. Types of entities and persons who carry out financial activities (continued)

Activities and operations according to the FATF definition of financial institutions		Financial institutions authorised to conduct these activities and operations	Licensing authority
11.	Otherwise investing, administering or managing funds or money on behalf of other persons	Licensed financial service providers– see item 10 above	ASIC
12.	Underwriting and placement of life insurance and other investment related insurance	28 Life insurers 207 Reinsurers	APRA
		Life insurance brokers/ life insurance agents (see 9 for list of investment and general financial advisors) Financial advisors (if holder of an AFS licence)	ASIC
13.	Money and currency changing	Bureaux de change / currency exchange providers – 108 bureaux de change enrolled with AUSTRAC ADIs and other businesses performing bureaux de change functions	None

Information as of 31 December 2013.

a5.2. **Exemptions from the AML/CTF Act granted by AUSTRAC under section 248 of the AML/CTF Act –** Section 248 of the AML/CTF Act authorises AUSTRAC to exempt a specified person from one or more provisions of the AML/CTF Act, or to amend the applicable provisions of the AML/CTF Act in relation to a specified person. Pursuant to its internal policy, AUSTRAC considers a number of factors while deciding on granting an exemption or not, including the 'the level of any potential or existing money laundering and/or terrorism financing risk'. AUSTRAC advised that a number of exemption requests were declined, including because of the ML/TF risk such an exemption would incur. All exemptions granted are publically available on AUSTRAC's website. However, a sample of exemption decisions reviewed shows that AUSTRAC has granted full exemptions from their AML/CTF obligations to applicants and unconditional exemptions. Australia advised that unconditional exemptions have not been granted since 2010. Exemptions were also granted to businesses operating in the area of private banking, prepaid cards or investment funds. The first two sectors have been identified as a high ML threat in the NTA, while investment funds were rated as presenting medium threat. Moreover, a director from an exempted private bank has been banned by ASIC from the financial service industry for dishonest conduct, including for hiding where investment money would ultimately be placed. APRA also took enforceable undertakings against this company. Neither the exemptions nor AUSTRAC's policy on exemptions provide for a regular review and the potential revocation of the exemptions granted.

a5.3. **Nature of some requirements applicable to reporting entities** – The AML/CTF Act and Rules contain obligations and prohibitions applicable on reporting entities - financial institutions or other persons, including some DNFPBs - when providing designated services. It should be noted that some of the FATF requirements are translated into the Act as prohibitions accompanied by sanctions (e.g. section 32 prohibits the commencement of the provision of designated service if the reporting entity has not carried out the applicable customer identification procedure; and section 81 prohibits reporting entities from providing designated services if it has not adopted an AML/CTF program or does not maintain such a program). The Rules are issued pursuant to section 229 of the AML/CTF Act and specify the obligations of the Act, in particular with respect to customer identification. The Rules, however, do not impose direct obligation on reporting entities to identify their customer, but require that their AML/CTF programme includes procedures to identify and verify the identity of their customers. Consequently, there is no explicit requirement on reporting entities to apply CDD as specified in the Standard – what they do in each case is determined by their own procedure for how they meet the requirements. Pursuant to the provisions under Part 7 of the AML/CTF Act (section 80 et seq.) reporting entities are required to adopt, maintain and apply an AML/CTF programme that complies with the AML/CTF Rules. AUSTRAC supervises reporting entities' respect of this obligation and applies sanctions as necessary, see also Recommendations 26 and 35. As a result, from a technical point

of view, the evaluation team is satisfied with the original structure of the AML/CTF obligations for reporting entities opted for by Australia.

a5.4. **Enforceability of the 2014 AML/CTF Rules.** Amendments to the 2007 Rules were adopted in May 2014 and entered into force on 1 June 2014. The 2014 amendments introduced and amended a few, though essential, obligations, most importantly with respect to beneficial ownership, ongoing due diligence and politically exposed persons. In addition to the adoption of the Rules, the *Policy (Additional Customer Due Diligence Requirements) Principles 2014* was issued by the Minister of Justice on 15 May 2014. Provision 213 of the AML/CTF Act allows the Minister to give written policy with which AUSTRAC must comply. According to the policy, for 18 months after the entry into force of the Rules (1 January 2016), a civil penalty or an injunction, the issuing of a remedial direction, or the imposition of a requirement to undertake an external compliance audit, may be applied only if the reporting entity 'has failed to take reasonable steps to comply with the relevant provision'. The policy specifies the matters to consider in determining whether a reporting entity has failed to take reasonable measures or not; they include the adoption of a transition plan and require that the Rules be applied as soon as practical in case of high ML/TF risk, and as soon as reasonable to existing customers. Notions such as 'as soon as practical' or 'as soon as reasonable' are not specified. Transition plans are to be established by 1 November 2014; they should include the necessary action and timeframes to ensure full compliance with the 2014 Rules from 1 January 2016. AUSTRAC advised that the policy reflects how AUSTRAC would have implemented and enforced the Rules in the absence of a formal policy issued by the Minister of Justice. The assessment team took the 2014 Rules into account for the purpose of the TC ratings.

Recommendation 9 – Financial institution secrecy laws

a5.5. Australia was rated compliant in its 3rd round Mutual Evaluation Report. Since the adoption of the 3rd round assessment, the AML/CTF Act was adopted in 2006.

a5.6. **Criterion 9.1 –** The AML/CTF Act imposes on reporting entities a number of reporting obligations (Parts 3 and 4), in particular a suspicious matter report (SMR). The *Privacy Act 1988* (Privacy Act) exempts from the non-disclosure prohibition where the disclosure is required or authorised by or under an Australian law or a court/tribunal order. As a result, the Privacy Act does not hinder the implementation of the AML/CTF Act.

a5.7. No obstacle that would inhibit the implementation of the FATF Recommendations was identified in the regime for correspondent banking, wire transfers, and reliance on third parties.

Weighting and Conclusion

a5.8. **Recommendation 9 is rated compliant**.

Customer due diligence and record-keeping

Recommendation 10 – Customer due diligence

a5.9. In its 3rd assessment, Australia was rated non-compliant on Recommendation 5. Deficiencies had been identified under most aspects of the Recommendation, as well as in the scope of the financial institutions covered. In subsequent follow-up reports, progress was made through the adoption of the AML/CTF Act in 2006 and the AML/CTF Rules in 2007. The AML/CTF Rules were amended in 2014.

a5.10. **Criterion 10.1 –** Sections 139 and 140 of the AML/CTF Act prohibit the provision and the reception of a "designated service", including opening and operating an account as defined under section 6 of the AML/CTF Act, using a false customer name or customer anonymity. The penalty is two years imprisonment and/or 120 penalty units.

a5.11. **Criterion 10.2 –** Section 32 of the AML/CTF Act requires that the applicable customer identification procedures (hereinafter ACIPs) be applied prior to the provision of a designated service, including operating an account or carrying out an occasional transaction, including wire transfers. Section 39 of the AML/CTF Act provides for general exemptions to the identification requirements. These exemptions can be found in the AML/CTF Rules and apply to:

- Partial or full transfer of business from one reporting entity to another (Chapter 28). This situation is not in contradiction with the requirement of Recommendation 10.
- The identification of signatories of financial institutions with whom the RE has a correspondent banking relationship (Chapter 35).
- The sale of shares up to AUD 500 for charitable purposes (Chapter 38). This case is not in contradiction with the requirement of Recommendation 10. See also Recommendation 8.
- Premium funding loans for a general insurance policy (Chapter 39). This case does not seem to be in contradiction with the requirement of Recommendation 10.
- Superannuation funds, when the total amount of interest to be cashed out does not exceed AUD 1 000, or when the total amount of interest to be cashed out does not exceed AUD 5 000 (Chapter 41). These cases do not seem to be in contradiction with the requirement of Recommendation 10.

a5.12. Section 38 of the AML/CTF Act provides that the ACIP is deemed to be carried out if the customer has already been subject to ACIP consistent with the AML/CTF Act and Rules by another reporting entity. See Recommendation 17 below.

a5.13. With respect to occasional transaction above the USD/EUR 15 000 threshold and structuring: section 6 of the AML/CTF Act sets the scope of the Act and therefore of the application of the CDD obligation. Among them, the issuance of stored value cards is covered by the AML/CTF Act if the value stored on the card is more than AUD 1 000 (if whole or part of the monetary value stored on the card may be withdrawn in cash) or AUD 5 000 (if the monetary value stored cannot be withdrawn in cash) and the increase of the value of a card with the same threshold. The latter case (reloadable cards) is not an occasional transaction and should therefore require that CDD be applied regardless of any threshold, which is not the case under the current Australian legislation. Stored value cards are identified in Australia's NTA as presenting potentially high ML threats. Australia advised that a risk-based approach is applied to these means of payment and that, pursuant to items 21-24 in Table 1 in subsection 6(2) of the AML/CTF Act, the thresholds can be adjusted by regulation if necessary.

a5.14. Section 6 of the AML/CTF Act is completed by Paragraphs 14.2 to 3 of the AML/CTF Rules which sets thresholds for the application of the provisions of Part 4.2 of the AML/CTF Rules (i.e. customer identification). Pursuant to these provisions, cheques drawn on a customer for less than AUD 5 000 or AUD 1 000 for cheques funded by cash; transactions below AUD 1 000 relating to traveller's cheques (i.e. issuing, cashing or redeeming); and currency exchange below AUD 1 000 are exempted from customer identification. These transactions do not exceed the USD/EUR 15 000 threshold set by the standard; however this raises an issue in the absence of a requirement to perform CDD for occasional transactions below the threshold that appear to be linked (i.e. structuring). Australia advised that reporting entities are required to detect structuring, as section 142 of the Act makes it an offence to structure transactions to avoid the reporting threshold (AUD 10 000). This argument is only relevant in the scope of the reporting obligation of section 43 (and its exemptions in section 44).

a5.15. Occasional transactions using wire transfers: there is no threshold for the identification and verification of the identity of the originator of wire transfers, regardless of the nature of the transfer. See Recommendation 16, below.

a5.16. In case of suspicion of ML/TF, reporting entities are required under Paragraph 15.9 of the AML/CTF Rules to apply enhanced due diligence. Paragraph 15.10 specifies that measures taken in the context of

enhanced CDD must be 'appropriate to [the] circumstances'. The measures listed include the clarification or update of KYC information already collected on the customer, etc.

a5.17. There is no explicit obligation for reporting entities to conduct CDD when they have doubts about the veracity or adequacy of the previously obtained customer identification data. However, Australia advised that pursuant to the provisions of Paragraph 15.10 of the AML/CTF Rules, reporting entities are required to apply enhanced CDD (see criterion 10.17 below) when a suspicion has arisen, including in situations where there are doubts about the veracity or adequacy of previously obtained customer identification data.

a5.18. **Criterion 10.3 –** As mentioned in the preamble to the section, there are no direct requirements to identify and verify the identity of the customer in the Act or in the Rules. Reporting entities are required to have AML/CTF programmes that include procedures to identify/verify the identity of the customer and enable them 'to be reasonably satisfied' that the customer is who/what he claims to be. Chapter 4 of the AML/CTF Rules requires reporting entities[1] to identify their customer and verify the information received. For each type of customer (i.e. natural persons, legal persons, trusts, etc.) the identification and verification requirements are specified. When the customer is a natural person, including a sole trader (Part 4.2 of the AML/CTF Rules): his/her name, date of birth and address must at a minimum be collected. The name must be verified as well as either the date of birth or the address. Verification is made through 'reliable and independent documentation' or electronic data or a combination of documents and electronic data. Parts 4.9 and 4.10 of the AML/CTF Rules specify the verification requirement, either from documentation or from electronic data.

a5.19. Similarly, Parts 4.3 to 4.8 provide for customer identification, and verification of the identification information when the customer is a company, a trust, a partnership, an association, a registered co-operative or a government body.

a5.20. Reliable and independent documentation is defined by the Rules as including but not limited to photographic and non-photographic identification documents, such as birth/citizenship certificates issued by a State/Territory/Commonwealth or foreign government, and secondary identification documents. Secondary identification documents – which can only be used to supplement primary documents to help establish identity, rather than prove identity – may include notices issued by utilities providers or schools; assessors are of the view that these documents cannot per se be seen as reliable documentation. Australia advised that in practice, reporting entities rely on multiple primary and secondary identification documents to verify the identity of their customers.

a5.21. **Criterion 10.4 –** Section 89 of the AML/CTF Act specifies that Part B of financial institutions' AML/CTF programmes must apply to agents purporting to act on behalf of a customer. Part 4.11 of the AML/CTF Rules contains different obligations considering the nature of the customer. Where the customer is a natural person, reporting entities are required under Paragraph 4.11.2 to identify the agent and collect evidence of their authorisation to act on behalf of the customer. There is no obligation to verify the identity of the agent of a customer, as Paragraphs 4.11.3 and 4 leave it to the reporting entities to determine whether and to what extent the identity of the agent must be verified. Where the customer is a 'non-natural' person, the name of the agent, his/her position or role with the customer, a copy of his/her signature and evidence of the authorisation to act on behalf of the customer must be verified (Paragraph 4.11.13).

a5.22. **Criterion 10.5 –** The beneficial owner is defined (Paragraph 1.2.1 of the Rules) as an individual who ultimately owns or controls (directly or indirectly) the customer. It is specified that *control* includes control

A5

1 The AML/CTF Act requires reporting entities to establish an AML/CTF programme, which is divided into two parts – Part A and Part B. The primary purpose of Part A of the standard AML/CTF programme is to identify, mitigate and manage ML/TF risks that a reporting entity faces and includes AML/CTF risk awareness training for employees, employee due diligence programme, oversight by boards and senior management, and procedures for independent review of programme. The primary purpose of Part B is to set out the reporting entity's ACIPs including beneficial ownership, ongoing CDD and enhanced due diligence. The AML/CTF Rules – including Chapter 4 – lays out items that the reporting entity are required to include in their AML/CTF programme.

as a result of, or by means of, trusts, agreements, etc. and includes exercising control through the capacity to determine decisions about financial and operating policies. *Owns* means ownership (either directly or indirectly) of 25% or more of a person.

a5.23. Pursuant to Part 4.12 of the AML/CTF Rules, reporting entities are required to collect information on the name, and either date of birth or address of each beneficial owner, and to take reasonable measures to verify it before the provision of a designated service, or as soon as practicable after the service has been provided. Pursuant to Paragraph 4.12.2 of the AML/CTF Rules, the obligation may be modified when the customer is a natural person, as the reporting entity may assume that the customer and the beneficial owner are one and the same person, unless there are reasonable grounds to consider otherwise. The obligation does not need to apply when the customer is a company or trust subject to simplified verification (i.e. Australian public listed companies and their majority owned subsidiaries, as well as companies licensed and subject to the regulatory oversight of a Commonwealth, State or Territory statutory regulator), an Australian Government Entity or a foreign listed public company subject to disclosure requirements concerning beneficial ownership comparable to those applicable in Australia. When the information is to be verified, verification must use reliable and independent documentation and/or electronic data (see above). The definition and obligations are largely in line with the FATF Recommendation; however, the exception concerning natural persons, trusts that are registered and subject to regulatory oversight, and companies that are licensed and supervised, is not authorised by the Standard, as it is not completely clear who this applies to and the level and type of supervision that is applied. Australia advised that the decisions with regard to trusts that are registered and subject to regulatory oversight and to companies that are licensed and regulated were made considering the existing high-level regulatory oversight and that both categories of legal entities are low risk.

a5.24. **Criterion 10.6 –** Paragraph 8.1.5 of the AML/CTF Rules only provides that an AML/CTF programme 'enable' the reporting entity to understand the nature and purpose of the business relationship with its customer types (i.e. natural or legal persons), including, as appropriate, the collection of information relevant to that understanding. The use of 'enable' does not require a reporting entity to understand the nature and purpose of the business relationship. However, the AML/CTF Rules were accompanied by an Explanatory Statement issued by the AUSTRAC CEO. Explanatory Statements are admissible as evidence under the *Acts Interpretation Act 1901* as to the intention of the Rules. Item 2 of the Explanatory Statement that accompanied the AML/CTF Rules states that the amended text of Paragraph 8.1.5 requires reporting entities to understand the nature and purpose of their business relationships with their customers. Moreover, the reference to 'customer types' used in this provision seems to deal with customers in general and does not contain the specific obligation to understand the nature and purpose of the relationship with every single customer. On the contrary, Australia advised that 'customer types' is used in Paragraph 8.1.5 to make it clear to reporting entities that all customers are included in this requirement.

a5.25. **Criterion 10.7 –** Section 36 of the AML/CTF Act requires financial institutions to monitor their customers with a view to identifying, mitigating and managing ML/TF risks. Chapter 15 of the AML/CTF Rules further details the ongoing due diligence obligation. The transaction monitoring programme is risk-based and must allow a reporting entity to identify suspicious transactions and have regard to complex, unusual large transactions and patterns of transactions, which have no apparent economic or lawful purpose. Little information or guidance is given on how to implement the obligation; for example, there is no express reference to the KYC information and customers' profile. Paragraph 15.3 of the AML/CTF Rules requires reporting entities to undertake reasonable measures to keep, update and review the documents, data or information collected under the ACIP (particularly in relation to high risk customers) and relating to the beneficial owner. The wording 'reasonable measures' is weaker than that of the criterion, which requires that CDD documents, data or information be kept up-to-date and relevant.

a5.26. **Criterion 10.8 –** Paragraph 8.1.5(2) of the AML/CTF Rules requires reporting entities to understand the control structure of non-individual customers. There is no explicit requirement to understand the nature of their business and their ownership structure.

a5.27. **Criterion 10.9 –** The AML/CTF Rules specifies for each category of legal persons what information is to be collected and/or verified (see below). There is also a general provision, providing in each case that the financial institution should be reasonably satisfied that the legal person exists. The specified information for categories of legal persons and arrangements are as follows:

- Companies: The AML/CTF Rules, Part 4.3, specify the information that financial institutions are required to collect, including: the full name of the company, its addresses of registration and principal place of business, its registration number (either the Australian Company Number or Australian Registered Body Number), the nature of the company and the names of the directors. Only the name, legal form and registration number must be verified. Reporting entities determine on the basis of risk if other information should be verified.

- Trusts: Part 4.4 of the AML/CTF Rules requires financial institutions to collect information on the name of the trust, its type, country of establishment and information on the trustees, beneficiaries and, under specific circumstances, the settlor. Verification only applies to the name of the trust and its beneficiaries and is done using a trust deed, certified copy or certified extract of the trust deed. Reporting entities determine on the basis of risk if other information should be verified.

- Partnership: Part 4.5 of the AML/CTF Rules requires financial institutions to collect information on the name of the partnership, country of establishment, identity and address of each partner. Only the name of the partnership and information about one partner must be verified. Reporting entities determine on the basis of risk if other information should be verified. Verification is done using the partnership agreement, or a certified copy or extract of the partnership agreement.

- Associations: Part 4.6 of the AML/CTF Rules requires financial institutions to collect information on the name of the association, its address or that of its chairman, secretary or treasurer, name of the chairman, secretary and treasurer and unique identification number. Only the name and identification number are to be verified. In case of unincorporated associations, information on the name and address of the association, on the name of the chairman, secretary and treasurer and on the identity of the members must be collected. Only information on the name of the association and information on the members is to be verified. Reporting entities determine on the basis of risk if other information should be verified. Verification is done using the constitution or rules of the association, or a certified copy or extract.

- Registered co-operatives: Part 4.7 of the AML/CTF Rules requires financial institutions to collect information on the name of the co-operative, its full address, unique identification number and the name of the chairman, secretary and treasurer. Only information on the name of the co-operative and unique identification number must be verified. Reporting entities determine on the basis of risk if other information should be verified. Verification is done through any register maintained by the cooperative, or a certified copy or extract.

- Government bodies: Part 4.8 of the AML/CTF Rules requires financial institutions to collect and verify information on the name, principal place of operations and whether the government body is an entity or an emanation of the Commonwealth, a State, Territory or a foreign country or is established under the legislation of the Commonwealth, a State, Territory or a foreign country.

a5.28. The identification of companies seems to be overall in line with the criterion. For customers that are legal persons, not all required elements must be verified, in particular the powers to bind the legal person and, for companies, the names of senior management (i.e. apart from the directors and those who appear on the legal person's statutes). The obligation to verify the information gathered does not cover the entire information that is required to be collected by the AML/CTF Rules and is therefore not in compliance with the Standard. However, the AML/CTF programmes must include risk-based systems and controls to determine if the information collected other than that for which the verification is mandatory should be verified.

a5.29. **Criterion 10.10 –** Part 4.12 of the AML/CTF Rules provide for the identification and verification of the identity of the beneficial owner, see criterion 10.5, above. Paragraph 4.12.9 of the AML/CTF Rules provides for the measures to be undertaken if the reporting entity has not been able to determine who the beneficial owner is. In this case, the reporting entity must identify and take reasonable measures to verify the identity of any individual exercising more than 25% of the voting rights or holding a position of senior managing official. This is in line with the Standard, though there is no gradation between the two measures of Paragraph 4.12.9.

a5.30. **Criterion 10.11 –** Part 4.4 of the AML/CTF Rules deals with the identification of trusts. As already described under criterion 10.9 above, the identification of the trust as a customer requires the identification of the trustees (pursuant to the rules applicable to the nature of the trustee) and beneficiaries. Information on the name and address of each trustee is required to be collected, as well as either information on the full name of each beneficiary or collection information on the class of beneficiaries. Amendments introduced in May 2014 now also require reporting entities to identify and verify the name of the settlor, unless the settlor's contribution to the trust is less than AUD 10 000 at the time of its creation, or if the settlor is deceased, or if trust is subject to the simplified trustee verification procedure. Verification on the identity of the trustees and beneficiaries is not required by the Rules. Paragraph 4.4.11 leaves it to the reporting entities to determine whether and to what extent the identity of the agent must be verified. Paragraph 4.12.9 of the AML/CTF Rules requires reporting entities unable to determine who the beneficial owner of a trust is, to identify and take reasonable measures to verify the identity of any individual who holds the power to appoint or remove the trustees of the trust.

a5.31. **Criterion 10.12 –** Pursuant to item 39 of Table 1 under section 6 of the AML/CTF Act, the person(s) to whom a payment is made under a life insurance policy is considered as being the customer of the paying financial institution. CDD measures of Chapter 4 of the AML/CTF Rules described above apply to the customer at the time of the payment. No obligation applies in relation to the identity of the beneficiary of a life insurance policy as soon as the beneficiary is identified or designated.

a5.32. **Criterion 10.13 –** The beneficiary of a life insurance policy is considered as being the customer of the paying reporting entity, which is required to apply enhanced due diligence to the customer in certain circumstances, see criterion 10.17 below.

a5.33. **Criteria 10.14 and 10.15 –** Section 32 of the AML/CTF Act prohibits the provision of financial services if the financial institution has not carried out the ACIP. This prohibition does not apply to existing customers (section 28), in case of 'low risk designated services' (section 30) and in the circumstances of Chapter 46 of the AML/CTF Act dealing with the acquisition or disposition of a security or a derivative or a foreign exchange contract (section 33). The AML/CTF Rules do not list any low-risk designated service and no designated services have been listed as 'low-risk' since the enactment of the AML/CTF Act in 2006. Concerning the special circumstances of Chapter 46, a list of eight conditions is provided, including the impossibility for the customer to transfer the amount of the contract and the prohibition for the financial institution to accept cash. It is specified among the conditions of Chapter 46 that it is practically impossible to conduct the ACIP before the transaction, which must be performed rapidly due to the market conditions, and that the financial institution put 'in place appropriate risk-based systems and controls to determine whether and in what circumstances to provide the designated service to a customer before the applicable customer identification procedure is carried out, including in relation to the number, types and/or amount of transactions'. The financial institution is required to carry out the ACIP within five business days (section 34 of the AML/CTF Act and Chapter 46 of the AML/CTF Rules); otherwise, it must not continue to provide any transaction or service or to perform another transaction or service.

a5.34. **Criterion 10.16 –** Division 2 of Part 2 of the AML/CTF Act explicitly applies to existing customers. Obligations with respect to existing customers apply when a suspicion arises (section 29); the obligations are set forth in Part 6.3 of the AML/CTF Rules: financial institutions are required within 14 days after the suspicion arose to take at least one of the following actions: (i) perform ACIP; (ii) collect any KYC information; or (iii) verify certain KYC information. As a result, the financial institution should be satisfied that the customer is the person he or she claims to be. This mechanism does not seem to take account of the risk presented by the customer and its objective focuses on the identity of the customer (i.e. it does not cover beneficial owner or the functioning of the account). Moreover, it does not seem to be fully consistent as the trigger event would most likely be a transaction (that raises suspicion), while the objective and measures to take rather deal with the identification of the customer. Though this is not explicit in section 36 of the AML/CTF Act and in Chapter 15 of the AML/CTF Rules, Australia advised that the requirement to monitor customers and the obligation to apply enhanced due diligence also applies to existing customers.

a5.35. **Criterion 10.17 –** Paragraph 15.8 *et seq.* of the AML/CTF Rules provides for the enhanced CDD programme and measures to implement in this context. Such a programme must be implemented when the reporting entity determines that the ML/TF risk is high; when the customer is a foreign PEP; when a suspicion

has arisen; or, when the customer is located in a prescribed foreign country (i.e. Iran). The enhanced CDD measures to be taken must be appropriate to the circumstances. Examples of a range of measures are listed in Paragraph 15.10; some of the measures included in the range seem to address normal due diligence (e.g. clarification and update KYC information, including its activity or business, identification of the beneficial owner, etc.). Other measures, such as identification of the sources of funds and wealth, and seeking senior management approval, are more suited to enhanced due diligence.

a5.36. **Criterion 10.18 –** Paragraph 4.3.8 allows financial institutions to apply simplified verification procedures when the customer is a domestic listed company, a majority owned subsidiary of a domestic listed public company or a company licensed and subject to the regulatory oversight of a Commonwealth, State or Territory statutory regulator. The verification measures are considered to be satisfied provided that the reporting entity at least obtains a search of the relevant domestic stock exchange, of the relevant ASIC database or of the license or other records of the relevant regulator or a public document issued by the relevant company. The application of simplified measures to companies that are licensed and supervised is not justified nor authorised under the FATF Standards. Pursuant to Paragraph 4.4.8, simplified verification procedures may apply to trusts that are managed investment schemes registered by ASIC, managed investment schemes that are not registered by ASIC under specific conditions, trusts registered and subject to the regulatory oversight of a Commonwealth statutory regulator, or a government superannuation fund established by legislation. Australia has not established that these cases have been identified through risk analysis.

a5.37. In Chapter 4 there are a number of provisions allowing financial institutions to apply CDD on the basis of risk. In most cases, it relates to measures other than those that are mandatory according to the Rules, e.g. collection of additional KYC information or verification of information other than in cases required by the Rules. In a few instances, the drafting of the provisions may lead to a complete exemption from CDD measures, in particular the verification obligation but also the obligation to collect information (see for example Paragraph 4.4.11 concerning the verification of the name of any or each trustee or beneficiary or class of beneficiaries or any other KYC information collected; Paragraph 4.11.3 on the verification of the identity of the agents of a customer, etc.) as the Rules leave it to the financial institutions 'to determine whether [and in what manner] to collect and/or verify' information.

a5.38. **Criterion 10.19 –** Where a financial institution is unable to comply with the relevant CDD measures, there is no requirement to not open the account/terminate the business relationship, or consider filing an SMR. If a reporting entity suspects on reasonable grounds that a customer is not the person who he/she/it claims to be, including because the reporting entity is not able to comply with the CDD measures, the reporting entity must file an SMR pursuant to subsections 41(1)(d) and (e) of the AML/CTF Act.

a5.39. **Criterion 10.20 –** There is no provision permitting financial institutions to not pursue the CDD process where there is a risk of tipping off, or requiring them to file an SMR in those cases (apart from the regular SMR obligation).

Weighting and Conclusion

a5.40. Several deficiencies have been identified under Recommendation 10 including:

- exemptions provided by the AML/CTF Act and Rules diminish the application of CDD in every situation envisaged by the standard (e.g. signatories of financial institutions in domestic correspondent banking relationships, reloadable stored value cards operating at a threshold, occasional transactions below a threshold which appear linked);
- shortcomings regarding verification requirements in relation to agents;
- exemptions and simplified due diligence do not appear based on proven low risk;
- shortcomings in relation to identification requirements and verification (powers to bind the legal entity and its senior managers) across all legal persons and legal arrangements including ownership structure;

- no requirement to identify the beneficiary of a life insurance policy until payout; limitations in enhanced customer due diligence which may be satisfied by updating identification which is considered normal due diligence; and

- no requirements relating to not proceeding or terminating the business relationship when CDD is unable to complied with or to stop performing CDD if there is a risk of tipping off.

a5.41. **Recommendation 10 is rated partially compliant.**

Recommendation 11 – Record-keeping

a5.42. In the 3rd assessment, Australia was rated partially compliant for Recommendation10. The main deficiencies were that the FTR Act did not cover transaction record-keeping for all types of financial institutions, and there were no specific requirements for account files and business correspondence to be retained. Record-keeping requirements were substantially amended respectively in 2006 and 2007 by the AML/CTF Act (Part 10) and AML/CTF Rules, lastly amended in 2014. AUSTRAC has published guidance note 08/04 on record-keeping requirements to assist reporting entities to comply with their record-keeping obligations.

a5.43. **Criterion 11.1 –** Sections 106 to 110 of the AML/CTF Act applies to transaction records, and these requirements are comprehensive. Section 106 identifies designated services where a transaction record must be made and retained. If a reporting entity makes a record of information relating to the provision of a designated service, that reporting entity must also keep records for seven years in relation to transaction records, or a copy of transaction records for seven years following the closing of the customer relationship (section 107). A document or a copy of the document provided by a customer relating to the provision of a designated service must also be retained for seven years after the provision of the document (section 108). These are supplemented by broad requirements to keep transaction records in corporate legislation. Under section 286 of the *Corporations Act 2001* (Corporations Act), all companies, registered schemes and other disclosing entities (whether or not they are financial institutions) must keep for seven years financial records that correctly record and explain their transactions and financial position and performance and would enable true and fair financial statements to be prepared and audited.

a5.44. **Criterion 11.2 –** Reporting entities must make and keep records of the ACIP, which must include the information obtained in the course of carrying out the procedure (sections 112 – 113 of the AML/CTF Act). These records seem to cover all CCD information collected and must be kept for seven years following the conclusion of the customer relationship. The following must also be kept for seven years: electronic funds transfer instructions, an AML/CTF programme made under Part 7 of the AML/CTF Act, and due diligence assessments of correspondent banking relationships (sections 115 – 117).

a5.45. Pursuant to a designating provision in section 107 of the AML/CTF Act, the AML/CTF Rules (Chapter 29) exempt certain documents in particular customer-specific documents, such as account statements and documents routinely prepared by the reporting entity, correspondence, and records of customer enquiries from the record-keeping requirements. These exemptions mean that not all account files and business correspondence, and results of any analysis undertaken, needs to be kept.

a5.46. **Criterion 11.3 –** There is no clear obligation in the AML/CTF Act that transaction records should be sufficient to permit reconstruction of individual transactions. AUSTRAC guidance note 08/04 (section 7.3) indicates that AUSTRAC considers it preferable that transaction records be sufficient to permit the reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for the potential prosecution of criminal activity. However, this is not a legally enforceable requirement. There are additional recordkeeping obligations laid out in the Corporations Act (section 988E) and the *National Consumer Credit Act 2009* (section 92), that require – among other things – that financial records must be kept in sufficient detail to show particular details related to all money received or paid by the licensee. This may be sufficient to permit reconstruction of individual transactions into/out of some financial institutions, but there are gaps in the scope of financial institutions covered by these provisions and it is unclear whether this would capture all types of transactions. In the case of international

wire transfers and for transactions reported to AUSTRAC (either SMR or TTR), more detailed information may be available as it is required in the context of the reporting obligations.

a5.47. **Criterion 11.4 –** There is no requirement upon financial institutions to ensure that all CDD information and transaction records are available swiftly to domestic competent authorities upon appropriate authority. There are provisions relating to AUSTRAC's monitoring and enforcement authorities (Parts 13-15 of the AML/CTF Act), including the power to give a written notice requiring the person to provide information or produce documents or copies of documents in the manner and within the time specified in the notice. AUSTRAC guidance note 08/04 (section 7.9) does indicate that, pursuant to AUSTRAC's monitoring powers under Part 13 of the Act, records should be stored in a retrievable and auditable manner. However, the actions available under the monitoring and enforcement powers of AUSTRAC do match the swift availability of the records and are limited to AUSTRAC. The guidance note is not enforceable. There are additional provisions in section 49 of the AML/CTF Act for the heads of selected government authorities to request information directly from reporting entities; this authority is limited to information related to reports (SMRs, IFTIs or TTRs) filed by reporting entities.

Weighting and Conclusion

a5.48. Reporting entities are required to keep records of the transactions with their customers and of their identification information for seven years. However, certain customer-specific documents are exempt from record-keeping requirements. There is also no requirement that the records kept be sufficient to permit the reconstruction of the transactions although Australia's reporting framework provides a complementary backstop. Finally reporting entities are not legally required to ensure that the records are available to all competent authorities. **Recommendation 11 is rated largely compliant.**

Additional Measures for specific customers and activities

Recommendation 12 – Politically exposed persons

a5.49. In its 3rd assessment, Australia was rated non-compliant on Recommendation 6 as PEPs were not dealt with under the AML/CTF regime in place at that time. In subsequent follow-up reports, some progress was made through the adoption respectively in 2006 and 2007 of the AML/CTF Act and AML/CTF Rules, as amended in 2014.

a5.50. Scope – Part 1.2 of the AML/CTF Rules provides the definition of PEP which is broadly in line with that of the FATF. However, it seems that the status of the PEP ceases with the position or function, as the definition refers to an individual who holds a prominent public position or function. Important political party officials are not explicitly covered by the Rules. Australia advised that they are covered by other categories, such as senior government officials or senior politicians. This may be true in Australia, but may not be adequate to cover important political party officials in foreign countries. Immediate family members are covered while the standard refers more broadly to 'family members'. The notion of 'close associates' requires beneficial ownership of a legal person or arrangement. Australia advised that the definition of PEPs is inclusive.

a5.51. **Criterion 12.1 –** Part 4.13 of the AML/CTF Rules deals with PEPs. Pursuant to Paragraph 4.13.1, reporting entities are required to determine whether a customer or the beneficial owner is a PEP. This determination should occur before the provision of a designated service to the customer or as soon as practicable after the provision of a designated service. Paragraph 4.13.3 provides for the measures to be taken in case of foreign PEPs. If the PEP is the beneficial owner of the customer, the ACIP applicable to the customer should apply to the PEP. In all cases, the reporting entity should (i) obtain senior management approval before establishing or continuing the business relationship; (ii) take reasonable measures to establish the PEP's source of wealth and source of funds; and, (iii) comply with the obligations in Chapter 15 on 'Ongoing customer due diligence'.

a5.52. **Criterion 12.2 –** In addition to the common measures applicable to all PEPs, measures specific to domestic PEPs and PEPs of international organisations are set out in Paragraph 4.13.2 of the AML/CTF Rules. If the PEP is the beneficial owner of the customer, the ACIP applicable to the customer should apply to the PEP. If the PEP is considered as presenting high ML/TF risk, then the reporting entity should (i) obtain senior management approval before establishing or continuing the business relationship; (ii) take reasonable measures to establish the PEP's source of wealth and source of funds; and, (iii) comply with the obligations in Chapter 15 on 'Ongoing customer due diligence'.

a5.53. **Criterion 12.3 –** The obligations described above apply to PEPs. The definition of which includes 'immediate family members' and 'close associates of PEPs'.

a5.54. **Criterion 12.4 –** As described under criterion 10.12, CDD measures only apply to the beneficiary of a life insurance policy at the time of the payout. There is no further obligation in case of higher risk situation.

Weighting and Conclusion

a5.55. The AML/CTF Rules Amendment set comprehensive obligations for PEPs.. The notions of close associate, which requires beneficial ownership of a legal person or arrangement, and of family members, which only apply to the spouse, parents and children, are too restrictive. Important officials of political parties are not covered and there is no specific requirement for life insurance. **Recommendation 12 is rated largely compliant**.

Recommendation 13 – Correspondent banking

a5.56. In its 3rd assessment, Australia was rated non-compliant on Recommendation 7 as correspondent banking relationships were not regulated under the AML/CTF regime in place at that time. In subsequent follow-up reports, some progress was made through the adoption respectively in 2006 and 2007 of the AML/CTF Act and AML/CTF Rules, lastly amended in 2014.

a5.57. **Criterion 13.1 –** Pursuant to sections 97 to 99 of the AML/CTF Act and Part 3.1 of the AML/CTF Rules, financial institutions are required, in relation to the provision of correspondent banking services, to:

- Conduct a preliminary assessment (section 97(1) of the AML/CTF Act) of the risk the financial institution may reasonably face that the correspondent banking relationship might involve or facilitate ML/TF. This assessment is to be carried out before the establishment of the correspondent banking relationship and is to be carried out on a regular basis. No further indication is provided on how such an assessment should be conducted, using what information, etc. Based on the outcomes of the preliminary assessment, financial institutions may be required under section 97(2) of the AML/CTF Act to conduct a 'due diligence assessment'. Pursuant to Paragraph 3.1.2 of the AML/CTF Rules, undertaking a 'due diligence assessment' is not compulsory; a reporting entity determines whether it is warranted based upon the preliminary assessment. This assessment of the ML/TF risk presented by the correspondent financial institutions covers among other things the existence and the quality of the AML/CTF regulation in the country of the correspondent institution; the adequacy of the AML/CTF internal control and compliance of the correspondent institution; information on the ownership, control and management, the reputation of the correspondent institution; information on whether the correspondent institution has been subject to ML/TF related investigations or prosecution, etc. This assessment must be conducted prior to the establishment of the correspondent banking relationship and must be updated on a regular basis. There is however no reference to the ML/TF supervision conducted in the country of the correspondent institution;
- Obtain prior approval from a senior officer of the financial institution;
- Document the respective responsibilities. There is no specification of the AML/CTF responsibilities, which therefore are deemed to be covered (section 99(2) of the AML/CTF Act).

a5.58. However, as noted above, Part 3.1 of the AML/CTF Rules specifies that 'due diligence assessment' is implemented on the basis of risk, which is not permitted under the standard.

a5.59. **Criterion 13.2 –** There is no requirement with respect to payable-through accounts. However, in July 2007 AUSTRAC issued a guidance note to assist financial institutions in implementing their obligations in relation to correspondent banking relationships, which provides an example of a payable-through account.

a5.60. **Criterion 13.3 –** Section 95 of the AML/CTF Act prohibits financial institutions from entering into a correspondent banking relationship with a shell bank, or with another financial institution that has a correspondent banking relationship with a shell bank. It is unclear whether the prohibition extends to entering into a correspondent banking relationship with a financial institution that does not currently have a correspondent banking relationship with a shell bank, but would theoretically be permitted to engage in such a relationship in the future. Financial institutions are also required to terminate such business relationships within 20 days after becoming aware that the correspondent institution is a shell bank or within the period of time determined by AUSTRAC.

Weighting and Conclusion

a5.61. The information reporting entities are required to gather and verify in the context of a correspondent banking relationship is insufficient as information on the AML/CTF regulation applicable to the correspondent bank; the adequacy of its internal controls; information on the ownership, etc. is gathered in the due diligence assessment, which a financial institution can conduct or not based upon the risk. There are no specific obligations for payable through accounts. **Recommendation 13 is rated non-compliant**.

Recommendation 14 – Money or value transfer services

a5.62. In its 3rd assessment, Australia was rated partially compliant on Special Recommendation VI as a number of deficiencies had been identified, in particular with respect to the licensing/registration of MVTS and limitations of the FTR Act. In subsequent follow-up reports, progress was made through the adoption respectively in 2006 and 2007 of the AML/CTF Act and AML/CTF Rules, lastly amended in 2014.

a5.63. **Criterion 14.1 –** Part 6 of the AML/CTF Act relates to the Remittance Sector Register. Section 74 provides that a person must not provide a registrable remittance network service or a designated remittance service unless they are registered as a remittance network provider, a remittance affiliate of a registered remittance network provider, or an independent remittance dealer. Sanctions are two-year's imprisonment or 500 penalty units, or both. Pursuant to section 75, AUSTRAC is required to maintain the Remittance Sector Register. The Register indicates the name of the person; the category in which s/he is registered (remittance network provider, or an affiliate of a registered remittance network providers, or independent remittance dealer); as necessary, the name of the network to which the affiliate is affiliated; any conditions to which the registration of the person is subject; the date of effect of the registration; and the registrable details in relation to the person. AUSTRAC's decision to register a person is made according to section 75C after having considered whether the person would involve a significant ML/TF or people smuggling risk that would potentially arise, should registration be granted. Registration is valid for three years; after that period, it must be renewed. AUSTRAC has large powers in the registration process. For example, further conditions to the registration can be imposed; further information can be requested; registration can be cancelled or suspended, in particular in case of significant ML/TF or people smuggling risk, etc. Pursuant to section 75M, any change that could materially affect the person's registration must be notified by the registered person. Civil penalties apply in case of failure to notify substantial change on a registered person.

a5.64. **Criterion 14.2 –** Australia advised that a series of measures has been implemented since the commencement of the AML/CTF Act in 2006 in order to identify unregistered MVTS. These measures include advertisements using radio and press in several languages, awareness raising and training sessions and material, the reliance on large money transfer networks to identify unlicensed remitters, etc. As mentioned above there are sanctions applicable to those persons: two years imprisonment and/or 500 penalty units.

a5.65. **Criterion 14.3 –** MVTS providers are subject to the monitoring of AUSTRAC for AML/CTF compliance. Australia advised that within AUSTRAC a team is dedicated to MVTS. This team is in charge of maintaining the Remittance Sector Register; dealing with the registration requests; and monitoring MVTS' AML/CTF compliance.

a5.66. **Criterion 14.4 –** As described above under criterion 14.1, agents (or affiliates in Australia's AML/CTF Act) are required under section 74 to register with AUSTRAC.

a5.67. **Criterion 14.5 –** Pursuant to section 84(5A) of the AML/CTF Act, a registered remittance network provider is required to make a standard AML/CTF programme available to its affiliates. This however does not prevent a remittance affiliate from adopting an individual specific AML/CTF program. Paragraph 54.2 of the AML/CTF Rules specifies that a remittance network provider assumes the TTR and IFTI reporting obligations of its agents. However, this does not entail that a remittance network provider monitors all activities of its agents. Australian authorities believe that there is an implicit requirement for a registered remittance network provider to monitor the compliance of its affiliates with the AML/CTF programme as part of the ongoing customer due diligence and transaction monitoring of the registered remittance network provider conducted on the affiliate, as the AML/CTF Act notes that the affiliates are the customer of the registered remittance network provider. However, the assessors believe that this was not sufficient in requiring the registered remittance network provider to monitor compliance of its affiliates with the AML/CTF programme and would recommend that this be made an explicit requirement.

Weighting and Conclusion

a5.68. MVTS are registered and supervised by AUSTRAC, which has taken a number of initiatives to ensure that all providers are registered. Agents of an MVTS provider can be included the provider's AML/CTF programme, but this is not an obligation. Their compliance with the AML/CTF programmes is not monitored by the MVTS provider. **Recommendation 14 is rated largely compliant**.

Recommendation 15 – New technologies

a5.69. In its 3rd assessment, Australia was rated non-compliant on Recommendation 8 in the absence of an AML/CTF regime applicable to new technologies. In subsequent follow-up reports, some progress was made through the adoption respectively in 2006 and 2007 of the AML/CTF Act and AML/CTF Rules, lastly amended in 2014.

a5.70. **Criterion 15.1 –** Australia has identified and assessed in its 2011 NTA the ML risks associated with 'electronic payment systems and new payment methods' which cover ATMs, credit/debit cards and stored value cards, online payment systems, online remittance and digital currencies. It seems to the assessors that among these items, not all can be considered as new technologies. Moreover, the NTA does not cover new business practices nor is it up to date. See also Recommendation 1. However, AUSTRAC also has conducted research on virtual currencies/Bitcoin and issued a policy.

a5.71. Reporting entities are required under section 81 of the AML/CTF Rules to adopt and maintain an AML/CTF programme whose objective, consistently with section 84(2), is to identify; mitigate and manage ML/TF risk. The AML/CTF Rules further specify under Parts 8.1 and 9.1 the factors to be considered for the identification of ML/TF risk, in particular the types of services provided and the methods by which services are delivered. The same provisions also state that the AML/CTF programme must enable reporting entities to assess the ML/TF risk posed by all new designated services prior to introducing them to the market; all new methods of designated service delivery prior to adopting them; and all new or developing technologies used for the provision of a designated service prior to adopting them.

a5.72. **Criterion 15.2 –** As described above, reporting entities are required to assess new services, methods of delivery and technologies prior to their adoption or use. However, other than the general obligation to assess the ML/TF risk (section 80 et seq. of the AML/CTF Act and Paragraphs 8.1.5 and 9.1.5 of the AML/CTF Rules), there is no specific explicit requirement for reporting entities to take appropriate measures to manage and mitigate the identified risks in the area of new technologies.

Weighting and Conclusion

a5.73. Australia demonstrated it had assessed ML/TF risks associated with some new products and technologies. Reporting entities are required to identify, mitigate and manage their ML/TF risks, but there is no specific obligation for new technologies. **Recommendation 15 is rated largely compliant**.

Recommendation 16 – Wire transfers

a5.74. Australia was rated non-compliant for Special Recommendation VII (wire transfers). There was no system to implement the requirements, only a reporting obligation for international wire transfers (a requirement which was deemed not-relevant in the context of and for the assessment of the compliance with SRVII, which required, as the current standard still does, that certain information flow to other financial institutions dealing with each wire). Since 2009, Australia has implemented measures intended to solve the shortcomings related to SR.VII. These have not been re-assessed as part of follow-up, but were extensively discussed with the authorities as part of this assessment and seem to address the earlier deficiencies. The requirements for Recommendation 16 have been extensively updated compared to SR.VII.

a5.75. **For all criteria –** Australia meets the requirements regarding the originator information (name, account number or unique transaction reference, address or identity/customer number or date and place of birth). Australia also meets the requirement that originator information is retained with a transfer. However, the legislation does not yet require the new elements of Recommendation 16: verification of the accuracy of the information, beneficiary information, intermediary financial institutions, record keeping (for the information that is not required). There is no threshold in Australia, thus criterion 16.3 does not apply. The current legal framework applies to MVTS but only covers the requirements related to SR.VII. However, in practice, Australia already requires MVTS to report information on originator and beneficiary MVTS transfers when filing an SMR (not in law, but through the relevant report forms). With respect to the freezing obligations, Australia does not ensure that freezing action is undertaken in the context of Recommendation 16.

Weighting and Conclusion

a5.76. Australia has the elements in place to comply with the originator information requirements contained in the old SR.VII; however, the intermediary, beneficiary, verification, MSB and targeted financial sanctions elements have not yet been updated in line with the new Recommendation 16. **Recommendation 16 is rated partially compliant**.

Reliance, Controls and Financial Groups

Recommendation 17 – Reliance on third parties

a5.77. In its 3rd assessment, Australia was rated non-compliant on Recommendation 9 in the absence of most of the requirements necessary to mitigate the risk posed by reliance on third parties. In subsequent follow-up reports, some progress was made through the adoption respectively in 2006 and 2007 of the AML/CTF Act and AML/CTF Rules, lastly amended in 2014.

a5.78. Section 38 of the AML/CTF Act sets out the conditions in which a reporting entity may rely on the CDD measures performed by a third party. The third party must be a reporting entity and have performed CDD consistent with the AML/CTF Act and Rules. Section 38(d) further provides that other conditions set out in the AML/CTF Rules must be satisfied. Chapter 7 of the AML/CTF Rules sets conditions in relation to financial advisers (i.e. holder of an AFSL) and for reporting entities that belong to the same designated group. Australia advised that only financial advisers and designated groups have expressed interest in the mechanism of section 38. Therefore, in other situations, the sole provisions of section 38 of the AML/CTF Act apply. In practice, reporting entities can only rely on a reporting entity located in Australia. The Explanatory Note of the Declaration, made on 16 March 2009 by the CEO of AUSTRAC, widens the range of third parties

on whom a reporting entity can rely to those that are a subsidiary of an Australian company located in a foreign country and that have customer identification procedures comparable to those prescribed under the AML/CTF regime in Australia. The objective of the declaration is to cover subsidiaries of Australian financial institutions located abroad, in particular in New Zealand.

a5.79. **Criterion 17.1 –** Section 38 introduces the presumption that the ACIP has been conducted by the reporting entity that relies on the third party. It is not explicitly stated that the reporting entity relying on a third party remains ultimately responsible for CDD measures. When the reporting entity relying on a third party is a financial adviser or reporting entity belonging to the same DBG as the third party, Chapter 7 of the AML/CTF Rules requires that the reporting entity relying on a third party has obtained a copy of the record made by the third party, or has access to it and has determined that it is appropriate to rely on the ACIP carried out by the third party having regard to the ML/TF risk. There is no obligation in relation to the regulation and supervision of the third party located abroad or on the existence of measures in line with Recommendations 10 and 11 for the third parties located abroad and regulated by foreign laws.

a5.80. **Criterion 17.2 –** As mentioned above, it is possible for Australian REs to rely on third parties located in Australia or abroad, in particular in New Zealand. Australia has not demonstrated that the ML/TF risk presented by New Zealand financial institutions was considered when the declaration expanding the scope of third parties to New Zealand financial institutions was issued. More generally, the Declaration of 16 March 2009 makes it the responsibility of the reporting entity "to ascertain that under its risk-based procedure that the relevant ACIP has been carried out under an AML/CTF regime, which is comparable to the Australian AML/CTF Act".

a5.81. **Criterion 17.3 –** Part 7.3 of the AML/CTF Rules sets out similar conditions for relying on a third party within the same DBG to those described above. As demonstrated above, reliance on third parties is limited to those located in Australia and on the subsidiaries of Australian reporting entities located abroad.

Weighting and Conclusion

a5.82. There are several deficiencies in Australia's regulation of third party reliance. It is not explicitly stated that the reporting entity relying on a third party remains ultimately responsible for CDD measures. There is no obligation in relation to the regulation and supervision of the third party located abroad, or on the existence of measures in line with Recommendations 10 and 11 for the third parties located abroad and regulated by foreign laws. The geographic risk regarding New Zealand or any other country has not been taken into account when considering expanding the scope of third parties to financial institutions from this country was issued. **Recommendation 17 is rated partially compliant.**

Recommendation 18 – Internal controls and foreign branches and subsidiaries

a5.83. In its 3rd assessment, Australia was rated non-compliant on Recommendations 15 and 22 in the absence of an obligation for financial institutions to have AML/CTF internal controls, policies and procedures and to ensure that their foreign branches and subsidiaries apply AML/CTF measures consistent with the Australian requirements. In subsequent follow-up reports, progress was made through the adoption respectively in 2006 and 2007 of the AML/CTF Act and AMLM/CTF Rules, lastly amended in 2014.

a5.84. **Criterion 18.1 –** Section 81 of the AML/CTF Act requires financial institutions to adopt, maintain and apply an AML/CTF programme. A standard programme applies to a particular financial institution; joint programmes apply to each financial institution that belongs to a particular DBG. Such programmes, either standard or joint, are divided into two parts. Part A is general; Part B relates to customer identification (sections 84(1)(b) and 85(1)(b)). Pursuant to sections 84.2 and 85.2, the objective of Part A is for the financial institution or entities of the DBG to identify, mitigate, and manage the ML/TF risk it may face. Chapters 8 and 9 of the AML/CTF Rules provide details as to what Part A and the joint AML/CTF programmes must contain.

- Compliance management arrangements, including the appointment of a compliance officer at the management level - Parts 8.4 and 8.5 and 9.4 and 9.5, require that Part A and the joint AML/CTF programme must be approved by the board and senior management of the financial institution or

group and that an AML/CTF compliance officer must be designated at the management level. There is no other compliance mechanism and the role and functions of the compliance officer are not further detailed.

- Screening procedures when hiring employees – Parts 8.3 and 9.3 provide that Part A of an AML/CTF programme (either standard or joint) must include 'an employee due diligence programme', which 'put in place appropriate risk-based systems and controls for the reporting entity to determine whether to, and in what manner to, screen any prospective employee who, if employed, may be in a position to facilitate the commission of a money laundering or financing of terrorism offence'. Screening of potential employees is based on risk and therefore may not be performed. It is limited to ML/TF aspects. However, it should be noted that a new screening may be conducted in case of transfer or promotion of an employee.

- Ongoing employee training programme – Parts 8.2 and 9.2 provide that Part A of an AML/CTF programme (either standard or joint) must include an 'AML/CTF risk awareness training programme' which must be designed so that the reporting entity gives its employees appropriate training at appropriate intervals, having regard to the ML/TF risk it may reasonably face. The objective is to 'enable employees to understand' the AML/CTF obligations set out by the Act or the Rules and applicable to a particular financial institutions, the type of ML/TF risk that the financial institution may face, and the processes and procedures established in the AML/CTF programme. The wording 'enable to understand' is weaker than requiring that the employee understands AML/CTF obligations.

- Independent audit function - Parts 8.6 and 9.6 provide that Part A of an AML/CTF programme (either standard or joint) must be subject to a regular independent review by an internal or external party. The objective is to assess the effectiveness of the Part A programme, its compliance to the AML/CTF Rules, and effective implementation. The result of the review is to be submitted to the board and senior management. The function is limited to the audit of Part A programmes. There are no indications as to the frequency of the "regular" review, or how to guarantee the independence of an internal audit, etc.

a5.85. **Criterion 18.2 –** As mentioned above, section 85 of the AML/CTF Act deals with the AML/CTF programme applicable in DBGs. DBGs are groups of two or more members that have decided to be member of the group. Part A of a programme is to identify, mitigate and manage ML/TF risk that each financial institutions of the DGB may face. The description and conclusions of criterion 18.1 above also apply.

- Sharing information – Part A of a joint programme is not required to contain policies and procedures on the sharing of information. It should be noted that the Act allows any member of a DBG to discharge certain obligations on behalf of other members. Section 123(7) of the AML/CTF Act is an exception to the tipping-off prohibition as it allows a member of a DBG with a joint AML/CTF programme to disclose information about one of its customer to another reporting entity within that DBG, in order to inform the other reporting entity about the risks involved in dealing with the customer.

- Group-level compliance, audit and/or AML/CTF functions – Section 207(3) of the AML/CTF Act allows a member of a DBG to disclose to the other members that an information notice pursuant to section 202 of the Act has been given. There are no further obligations for DBGs.

- Confidentiality and use of information exchanged – As mentioned above, members of a DBG may under certain circumstances disclose information in relation to a SMR to other members of the group. The financial institution to which information has been disclosed is prohibited to disclose it, unless the disclosure is made to another member of the DBG for the purpose of informing about the ML/TF risk. There are no further obligations in relation to confidentiality and use of information exchanged.

a5.86. **Criterion 18.3 –** Section 6(6) of the AML/CTF Act extends the application of the Act to foreign branches and subsidiaries of Australian financial institutions. Part 8.8 and 9.8 deal with permanent

establishments in foreign countries (i.e. foreign branches). Paragraph 8.8.3 sets out without any further detail that where a foreign branch is regulated by AML/CTF laws comparable to Australia, only minimal additional systems and controls need to be considered by the financial institution. Paragraph 8.8.4 provides that Parts 8.1 to 8.3 (i.e. general provision on Part A programme, risk awareness training and employee due diligence programme) do not apply to foreign branches. Chapter 9 of the Rules contains similar provisions for DBGs. Except for section 6(6) of the Act, there are no provisions applicable to subsidiaries located abroad. There is no obligation for financial institutions with respect to the adequacy of the AML/CTF regime of host countries; and no obligation to apply the higher standard or Australia regime to the extent possible. There is no obligation to apply measures to manage ML/TF risks and to inform AUSTRAC when the host country does not permit the proper implementation of AML/CTF measures consistent with Australia's AML/CTF regime.

Weighting and Conclusion

a5.87. There are numerous deficiencies with respect to reporting entities' internal controls: there is no obligation beyond the nomination at management level of a compliance officer, the audit function is limited and there is no indication of the frequency of the audit or guarantee of its independence. This also applies at the group level. There are a number of deficiencies concerning branches and subsidiaries located abroad, in particular the obligation to apply the higher standard. **Recommendation 18 is rated partially compliant**.

Recommendation 19 – Higher-risk countries

a5.88. In the 3rd assessment, Australia was rated partially compliant for Recommendation 21. The deficiencies noted that while AUSTRAC has the authority under section 38(1)(e) of the FTR Act to indicate other countries as higher risk, it had made limited use of this provision. Also, there was no specific requirement for financial institutions to pay special attention to transactions involving countries that do not adequately apply the FATF Recommendations in accordance with Recommendation 21. Since 2005 specific regulatory measures have been implemented to target higher-risk countries.

a5.89. **Criterion 19.1 –** Chapter 15 (On-going Due Diligence) of the AML/CTF Rules requires reporting entities to apply their enhanced CDD programme when they determine the situation to be of higher risk, a ML/TF suspicion has arisen, or when entering, or proposing to enter, into a transaction with a party who is a natural or legal person in a prescribed foreign country. See the analysis in criterion 10.17 regarding what reporting entities must do as part of their enhanced due diligence programmes. Iran has been designated as a prescribed foreign country pursuant to the AML/CTF Regulations (as updated in 2012)—see also criterion 19.2 below. On the other hand, the DPRK has not been designated as a prescribed foreign country via the AML/CTF Regulations. While Australia imposes an autonomous sanctions regime in relation to DPRK, reporting entities are not legally required to apply enhanced due diligence measures to all customers from this country, although Australia notes that reporting entities do so in practice. However, this is not sufficient to meet the Standard.

a5.90. **Criterion 19.2 –** Australia is able to apply counter-measures when called upon to do so by the FATF, or independently of any call by the FATF to do so. Part 9 of the AML/CTF Act allows regulations under the Act to impose countermeasures which regulate or prohibit transactions with legal and natural persons physically present in prescribed foreign countries (which includes situations when the FATF calls upon countries to do so or independently of any FATF call). Regulations made under Part 9 are subject to a two-year sunset effect. The AML/CTF Regulations were amended, with effect from 1 March 2012, to make Iran a prescribed foreign country and prohibit transactions of AUD 20 000 or more unless prior authorisation has been granted by DFAT. Reporting entities must also apply enhanced due diligence on customers and transactions involving Iran, including payments sent or received through third-party countries. AUSTRAC guidance note 12/02 states that AUSTRAC expects all Iran-related transactions be treated as high-risk for the purposes of transaction monitoring.

a5.91. **Criterion 19.3 –** AUSTRAC Information Circulars (AICs) advise reporting parties of concerns about weaknesses in the AML/CTF systems of other countries. The AICs advise or update reporting entities of significant AML/CTF matters such as modified regulatory obligations, federal government listing of terrorist organisations, and UNSC or autonomous Australian sanctions. The circulars also publish the FATF Public

Statements and Improving Global AML/CTF Compliance documents and state that reporting entities should take into account FATF statements when considering whether transactions should be reported to AUSTRAC as suspicious.

Weighting and Conclusion

a5.92. While reporting entities are required to apply enhanced due diligence (and counter-measures) to their relationships and transactions with Iran, they are not required to do so for DPRK, despite the FATF's call to do so. While reporting entities must apply enhanced due diligence when they themselves determine there to be higher-risk, this does not equate to a requirement pursuant to criterion 19.1. And, among the measures for enhanced due diligence listed in the Rules, some address normal due diligence rather than enhanced due diligence. **Recommendation 19 is rated partially compliant.**

Reporting of Suspicious Transactions

Recommendation 20 – Reporting of suspicious transaction

a5.93. In its 3rd assessment, Australia was rated largely compliant for both Recommendation 13 and Special Recommendation IV. Overall, the regime for reporting suspicious transactions within the FTR Act 1988 was comprehensive except that there was a limitation on the scope of "cash dealers" and a concern that the scope of the TF offence could slightly limit the reporting obligation. Provisions of the FTR Act were amended and updated in the AML/CTF Act(section 41).

a5.94. **Criterion 20.1 –** Subsection 41(1) defines a series of "suspicious matter reporting obligation" triggers that then must be reported to AUSTRAC pursuant to subsection 41(2). Civil penalties apply for non-reporting: up to 100 000 penalty units (AUD 17 million) for a body corporate, and up to 20 000 penalty units (AUD 3.4 million) for an individual.

- For ML-related SMRs: these must be reported within 3 business days after the day of forming the suspicion on reasonable grounds that the provision or prospective provision of the service is preparatory to or may be relevant to the investigation or prosecution of ML, a tax offence, or any other offence. "Money Laundering" means any offence against Division 400 of the CC, or any corresponding State, Territory, or foreign offence.

- For TF-related SMRs: these must be reported within 24 hours after forming the suspicion on reasonable grounds that the provision or prospective provision of the service may be preparatory to or may be relevant to the investigation or prosecution of financing of terrorism. "Financing of terrorism" includes: any offence against section 102.6 or Division 103 of the CC; an offence against section 20 or 21 of the CotUNA; or any corresponding State, Territory, or foreign offence. *See the analysis of Recommendation 5 – limitations in the scope of the TF offence may somewhat limit the reporting requirement.*

a5.95. **Criterion 20.2 –** Section 41 includes references to a "prospective" provision of a service when suspicion can be formed (and then must be reported), which incorporates the concept of attempted transactions. The reporting obligations apply regardless of the amount of the transaction involved.

Weighting and Conclusion

a5.96. There are some limitations in the scope of the TF offences given that the reporting requirement is directly tied to the criminalisation in the CC. However, the assessors believe that the limitation is sufficiently minor as to not have a material impact on the reporting requirement. **Recommendation 20 is rated compliant**.

Recommendation 21 – Tipping-off and confidentiality

a5.97. **Criterion 21.1 –** Section 235 of the AML/CTF Act protects a person or an officer, employee or agent of this person from any action, suit or proceeding (whether criminal or civil) in relation to any acts made in good faith in carrying out compliance with any requirement in the AML/CTF Act, Regulations, or Rules.

a5.98. **Criterion 21.2 –** Section 123(1) indicates that if a SMR obligation arises or has arisen for a reporting entity in relation to a person, and the reporting entity has filed an SMR, the reporting entity must not disclose to someone other than the AUSTRAC CEO or a member of the staff of AUSTRAC that information has been communicated to the AUSTRAC CEO.

a5.99. Section 123(2) further provides that if a reporting entity has formed an applicable suspicion (but has not yet filed an SMR), the reporting entity must not disclose to anyone other than the AUSTRAC CEO or an AUSTRAC staff member about the suspicion or about any other information from which the person to whom the information is disclosed could reasonably be expected to infer that the suspicion had been formed. However, subsection 123(4) specifies a number of cases where section 123(2) does not apply, including when the reporting entity is: a legal practitioner; a partnership or company that carries on the business of using legal practitioners to supply professional legal services; a qualified accountant, or a partnership or company that carries on a business of using qualified accountants to supply professional accountancy services; and the information relates to the affairs of a customer of the reporting entity; and the disclosure is made for the purposes of dissuading the customer from engaging in conduct that could constitute an evasion of a taxation law or evasion of a law of a State or Territory that deals with taxation; or an offence against a law of the Commonwealth, State, or Territory. It is unclear to what extent these exemptions weaken the confidentiality requirements before an SMR is filed. The Australian authorities should clarify in what circumstances this could apply to reporting parties that may be lawyers or accountants but also carry out "financial activities" as defined by FATF.

Weighting and Conclusion

a5.100. **Recommendation 21 is rated compliant.**

Designated non-financial businesses and professions

Preamble: Scope of DNFBPs

a5.101. The AML/CTF Act applies to those who provide a service designated in section 6, tables 6.1, 6.2 and 6.3. Tables 6.2 and 6.3 deal with bullion dealers and gambling services, including casinos. Chapter 52 of the AML/CTF Rules exempt persons licensed to operate no more than 15 gaming machines from most of the AML/CTF obligations, in particular CDD, internal control and record keeping obligations. These two categories are the only two DNFBPs explicitly targeted by the AML/CTF Act. Other DNFBPs (i.e. real estate agents, dealers in precious stones, lawyers, notaries, other legal professionals and accountants, and TCSPs) are only covered when they provide one of the designated services – i.e. essentially acting in the capacity of a financial institution under the FATF Recommendations. None of the services designated relates to real estate agents, dealers in precious stones or TCSPs activities. The AML/CTF Act applies to lawyers, notaries and other independent legal professionals when they provide a designated service. Australia specified that lawyers, notaries and other independent legal professionals may provide the designated services listed under Table 6, Items 6, 7 and 54 that relate to money lending and services provided as holder of an AFS licence. These three items are financial activities and dealt with in section 5 of this annex. They are not specific to lawyers, notaries and other independent legal professionals and Recommendation 22. Solicitors are referred to in the FTR Act and require that they report cash transactions exceeding AUD 10 000 (see below).

Recommendation 22 – DNFBPs: Customer due diligence

a5.102. In its 3rd assessment, Australia was rated non-compliant on Recommendation 12 as deficiencies had been identified under most Recommendations referred to in Recommendation 12, in particular Recommendations 5 and 10, and in the scope of the DNFBPs covered. In subsequent follow-up reports, progress was made through the adoption respectively in 2006 and 2007 of the AML/CTF Act and AML/CTF Rules, lastly amended in 2014.

a5.103. **Criterion 22.1** is not met. Pursuant to Chapter 10 of the AML/CTF Rules, gambling services are required to identify their customer when they carry out transactions above AUD 10 000 (approximately USD 9 000 / EUR 6 000) which exceeds the USD/EUR 3 000 threshold for this criterion. Bullion dealers are also obliged to perform CDD measures for transactions of AUD 5 000 or more, which is in line with the standard. When applicable, CDD obligations for casinos and bullion dealers are similar to those applicable by financial institutions and described in Recommendation 10.

a5.104. **Criteria 22.2 to 22.5 –** See Recommendations 11, 12, 15 and 17.

Weighting and Conclusion

a5.105. Only casinos and bullion dealers are subject to AML/CTF obligations. The AML/CTF Act also provides exemptions for casinos and lawyers, though these two sectors have been identified as high ML threat in the NTA. The identification threshold for casinos exceeds that set forth in the Recommendation. See also conclusions under Recommendations 11, 12, 15 and 17. As a result, **Recommendation 22 is rated non-compliant.**

Recommendation 23 – DNFBPs: Other measures

a5.106. In its 3rd assessment, Australia was rated non-compliant on Recommendation 16 as deficiencies had been identified under most Recommendations referred to in Recommendation 16, in particular Recommendations 13, 15 and 21, and in the scope of the DNFBPs covered. In subsequent follow-up reports, progress was made through the adoption respectively in 2006 and 2007 of the AML/CTF Act and AML/CTF Rules, lastly amended in 2014.

a5.107. Criteria 23.1 to 23.4 - See Recommendations 20, 18, 19 and 21.

Weighting and Conclusion

a5.108. Given that most DNFPBs are not subject to AML/CTF requirements on suspicious transaction reporting, instituting internal controls and complying with higher risk countries requirements, and the deficiencies identified under Recommendations 18 and 19 for DNFBPs that are subject to the requirements, **Recommendation 23 is rated non-compliant**.

Table of Acronyms

ABN	Australian business number
ABR	Australian business register
ACA	Australian Central Authority
ACBPS	Australian Customs and Border Protection Service
ACC	Australia's Crime Commission
ACNC	Australian Charities and Not-for-Profits Commission
AFP	Australian Federal Police
AGD	Attorney General's Department
AIC	Australian Intelligence Community
AML	Anti-money laundering
APG	Asia/Pacific Group on Money Laundering
APRA	Australian Prudential Regulation Authority
ARSN	Australian registered scheme number
ASIC	Australian Securities and Investment Commission
ASIO	Australian Security Intelligence Organisation
ATO	Australian Taxation Office
AUSTRAC	Australian Transaction Reports and Analysis Centre
CACT	Criminal Asset Confiscation Taskforce
CDD	Customer due diligence
CDPP	Commonwealth Director of Public Prosecutions
CFT	Countering the financing of terrorism
CotUNA	Charter of the United Nations Act
CT	Combat terrorism
DAR	Dealing with assets regulation
DFAT	Department of Foreign Affairs and Trade
DNFBP	Designated non-financial businesses and professions
FIU	Financial intelligence unit
FTR	Financial transaction report
IDC	Interdepartmental Committee
IFTI	International fund transfer instructions
ILGA	Independent Liquor and Gaming Authority

TABLE OF ACRONYMS

IMP	Information management policy
IOSCO	International Organisation of Securities Commissions
KYC	Know your customer
MACMA	Mutual Assistance in Criminal Matters Act 1987
ML	Money laundering
MLA	Mutual legal assistance
MMOU	Multilateral memoranda of understanding
NOCRP	National organised crime response plan
NPO	Non-profit organisations
NRA	National risk assessment
NTA	National threat assessment
OCTA	Organised crime threat assessment
OSAS	Online sanctions administration system
PEPs	Politically exposed persons
PSPF	Protective security policy framework
REG	Reporting entity group
REs	Reporting entities
RNP	Remittance network provider
SMR	Suspicious matter report
SUSTR	Suspect transactions
TF	Terrorist financing
TFIU	Terrorism financing investigations unit
TFS	Targeted financial sanctions
TTR	Threshold transaction report
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolution