THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING AND OTHER LEGISLATION AMENDMENT BILL 2019

EXPLANATORY MEMORANDUM

(Circulated by authority of the Minister for Home Affairs, the Honourable Peter Dutton MP)
<table>
<thead>
<tr>
<th><strong>Acronym</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>ACIP</td>
<td>Applicable customer identification procedure</td>
</tr>
<tr>
<td>AFP</td>
<td>Australian Federal Police</td>
</tr>
<tr>
<td>AFP Act</td>
<td>Australian Federal Police Act 1979</td>
</tr>
<tr>
<td>AML/CTF</td>
<td>Anti-money laundering and counter-terrorism financing</td>
</tr>
<tr>
<td>AML/CTF Act or the Act</td>
<td>Anti-Money Laundering and Counter-Terrorism Financing Act 2006</td>
</tr>
<tr>
<td>AML/CTF amendment Act</td>
<td>Anti-Money Laundering and Counter Terrorism Financing and Other Legislation Amendment Act 2019</td>
</tr>
<tr>
<td>AML/CTF Rules</td>
<td>Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)</td>
</tr>
<tr>
<td>APP</td>
<td>Australian Privacy Principle</td>
</tr>
<tr>
<td>AUSTRAC</td>
<td>Australian Transaction Reports and Analysis Centre</td>
</tr>
<tr>
<td>AUSTRAC CEO</td>
<td>Chief Executive Officer of the Australian Transaction Reports and Analysis Centre</td>
</tr>
<tr>
<td>BNI</td>
<td>Bearer Negotiable Instrument</td>
</tr>
<tr>
<td>CDPP</td>
<td>Commonwealth Director of Public Prosecutions</td>
</tr>
<tr>
<td>CDD</td>
<td>Customer Due Diligence</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force</td>
</tr>
<tr>
<td>FTR Act</td>
<td>Financial Transaction Reports Act 1988</td>
</tr>
<tr>
<td>MER</td>
<td>Mutual Evaluation Report</td>
</tr>
<tr>
<td>Privacy Act</td>
<td>Privacy Act 1988</td>
</tr>
<tr>
<td>SMR</td>
<td>Suspicious Matter Report</td>
</tr>
</tbody>
</table>
ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING AND OTHER LEGISLATION AMENDMENT BILL 2019

GENERAL OUTLINE


3. Together with the Financial Transaction Reports Act 1988 (the FTR Act), the AML/CTF Act provides the basis for regulation of certain businesses by the Australian Transaction Reports and Analysis Centre (AUSTRAC). AUSTRAC is Australia’s financial intelligence unit and anti-money laundering and counter-terrorism financing (AML/CTF) regulator. The regulatory framework established under the AML/CTF Act and FTR Act provides for the collection of information from the private sector and from inbound and outbound travellers about the movement of money and other assets. AUSTRAC shares this information with Commonwealth, State and Territory agencies, and AUSTRAC’s international counterparts, in order to combat money laundering, terrorism financing and other serious crimes.

4. The Bill contains a range of measures to strengthen Australia’s capabilities to address money laundering and terrorism financing risks, and generate regulatory efficiencies, including amendments to:
   - expand the circumstances in which reporting entities may rely on customer identification and verification procedures undertaken by a third party
   - explicitly prohibit reporting entities from providing a designated service if customer identification procedures cannot be performed
   - strengthen protections on correspondent banking by:
     - prohibiting financial institutions from entering into a correspondent banking relationship with another financial institution that permits its accounts to be used by a shell bank, and
     - requiring banks to conduct due diligence assessments before entering, and during, all correspondent banking relationships
   - expand exceptions to the prohibition on tipping off to permit reporting entities to share suspicious matter reports (SMRs) and related information with external auditors, and foreign members of corporate and designated business groups
   - provide a simplified and flexible framework for the use and disclosure of financial intelligence to better support combatting money laundering, terrorism financing and other serious crimes
   - create a single reporting requirement for the cross-border movement of monetary instruments
   - address barriers to the successful prosecution of money laundering offences by:
     - clarifying that the existence of one Commonwealth constitutional connector is sufficient to establish an instrument of crime offence, and
     - deeming money or property provided by undercover law enforcement as part of a controlled operation to be the proceeds of crime for the purposes of prosecution.

5. The Bill also expands the rule-making powers of the Chief Executive Officer of AUSTRAC (AUSTRAC CEO) across a number of areas. The Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1) (AML/CTF Rules) are legislative instruments within the
meaning of section 8 of the *Legislative Instruments Act 2003*. Accordingly, AML/CTF Rules must be tabled in Parliament and are subject to disallowance by either House.

6. The Bill amends the AFP Act to make it an offence for a person to dishonestly represent that a police award has been conferred on them. The introduction of this offence will preserve the significant honour associated with receiving a police award. These awards recognise the outstanding contribution that individuals make to their community and should be respected accordingly.

7. This measure will also ensure that police awards attract similar protections to service decorations awarded to members of the Australian Defence Force under subsection 80B(1) of the *Defence Act 1903*.

**FINANCIAL IMPACT STATEMENT**

8. The Bill will be implemented within existing resources.

**REGULATION IMPACT STATEMENT**

9. A Regulation Impact Statement has been developed in relation to the Bill. The Regulation Impact Statement is at Annexure A.

10. The AML/CTF Act requires reporting entities to identify and verify their customers through customer due diligence (CDD) procedures, which represents a major component of AML/CTF compliance costs. The Bill will provide reporting entities with further options to rely on CDD procedures undertaken by a third party. These options could reduce the time involved in identifying each customer by 66% and the cost of verifying each customer by 80%. This is expected to deliver significantly reduced compliance costs and an estimated regulatory saving of $3,107,229,243 over ten years.

11. The other measures in the Bill will have either a neutral or low regulatory impact.
STATEMENT OF COMPATIBILITY WITH HUMAN RIGHTS

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Bill 2019

1. The Bill is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the Human Rights (Parliamentary Scrutiny) Act 2011.

Overview of the Bill

2. The Bill amends the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act) and the Criminal Code Act 1995 (Criminal Code) and makes minor consequential amendments to a number of other Acts.


4. The Bill will also address some of the deficiencies identified by the Financial Action Task Force (FATF) in its mutual evaluation report (MER) on Australia’s anti-money laundering and counter-terrorism financing (AML/CTF) regime in 2015. The FATF is an inter-governmental body, which sets the standards for, and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. The MER details the outcomes of the FATF’s assessment of Australia’s compliance with the FATF standards.

5. The AML/CTF Act provides the basis for regulation of certain businesses (reporting entities) by the Australian Transaction Reports and Analysis Centre (AUSTRAC). AUSTRAC is Australia’s financial intelligence unit and AML/CTF regulator. The regulatory framework established under the AML/CTF Act provides for the collection of information from the private sector and from in and outbound travellers about the movement of money and other assets. AUSTRAC shares this information and associated financial intelligence with government agencies in an effort to combat money laundering, terrorism financing and other serious crimes.

6. The Bill contains a range of measures to strengthen Australia’s AML/CTF regime, and generate regulatory efficiencies. It includes amendments to:
   - expand the circumstances in which reporting entities may rely on customer identification and verification procedures undertaken by a third party
   - explicitly prohibit reporting entities from providing a designated service if customer identification procedures cannot be performed
   - strengthen protections around correspondent banking by:
     o prohibiting financial institutions from entering into a correspondent banking relationship with another financial institution that permits its accounts to be used by a shell bank, and
     o requiring banks to conduct due diligence before entering, and during, all correspondent banking relationships
   - expand exceptions to the prohibition on tipping off to permit reporting entities to share suspicious matter reports (SMRs) and related information with external auditors, and foreign members of corporate and designated business groups
• provide a simplified and flexible framework for the use and disclosure of financial intelligence to better align with existing operational practice used to combat money laundering, terrorism financing and other serious crimes
• create a single reporting requirement for the cross-border movement of monetary instruments including physical currency and bearer negotiable instruments (BNIs)
• address barriers to the successful prosecution of money laundering offences by:
  o clarifying that the existence of one Commonwealth constitutional connector is sufficient to establish an instrument of crime offence, and
  o deeming money or property provided by undercover law enforcement as part of a controlled operation to be the proceeds of crime for the purposes of prosecution.

7. The Bill also amends the *Australian Federal Police Act 1979* (AFP Act) to make it an offence for a person to dishonestly represent that a police award has been conferred on them. The introduction of this offence will preserve the significant honour associated with receiving a police award. These awards recognise the outstanding contribution that individuals make to their community and should be respected accordingly.

8. Proposed section 62 of the AFP Act provides that the offence only applies to dishonest representations, which ensures that a balance is struck between punishing individuals who unjustifiably represent themselves as a recipient of a police award while allowing individuals who have not received an award to wear these awards in permissible circumstances without committing an offence.

9. The definition of dishonesty at proposed subsection 62(3) means dishonest according to the standards of ordinary people and known to the defendant to be dishonest according to the standards of ordinary people.

10. Pursuant to this definition, a person would not be considered to have dishonestly represented that a police award has been conferred on them where they wear this award in permissible circumstances, for example:
  i. in a dramatic presentation, such as a film, to convey that a fictional person is the recipient of the award, or
  ii. to honour a deceased family member, close relative or colleague who was the true recipient of the award.

11. However, a representation will be dishonest if a person falsely represents that they received a police award to secure employment or to increase their standing in the community.

**Human rights implications**

12. The Bill engages the following human rights:
• the right to freedom of expression in Article 19(2) of the International Covenant on Civil and Political Rights (ICCPR), and
• the right to privacy in Article 17 of the ICCPR.

**Right to freedom of expression**

13. The Bill engages the right to freedom of expression in Article 19(2) of the ICCPR by amending the existing ‘tipping off’ offence in section 123 of the AML/CTF Act, which prevents a person disclosing SMRs and related information.

14. Article 19(2) of the ICCPR provides that everyone has the right to freedom of expression, including the freedom to impart information and ideas of all kinds, including orally, in writing or through any other media. Article 19(3) provides that the right to freedom of expression may be limited
where it is prescribed by law and necessary to respect the rights or reputations of others, or to protect national security. To the extent that a person is prevented from disclosing that a SMR has been made, and that disclosure would otherwise have been an expression or opinion about the subject of the SMR, the right to freedom of expression in Article 19 may be limited.

15. The ‘tipping off’ offence has been in the AML/CTF Act since it came into force in 2006 and is a requirement for compliance with Recommendation 21 of the FATF standards. The purpose of the offence is to safeguard against a person within a reporting entity ‘tipping off’ a customer that the suspicious activity the customer has engaged in has been or will be reported. The offence addresses concerns that if a customer became aware of such a SMR, they may stop or further disguise their illegal conduct. This would undermine the efforts of law enforcement to detect and disrupt money laundering, terrorism financing, or other serious crimes.

16. Therefore, in addition to ensuring compliance with international standards, prohibiting the sharing of this information is reasonable and necessary to protect national security.

17. There are a number of exceptions to the ‘tipping off’ offence listed in section 123 which ensure the limitation on the right to freedom of expression is proportionate. The exceptions allow disclosure of SMRs and related information for the purposes of:
   - crime prevention
   - obtaining legal advice
   - operation of Part 4 of the Charter of the United Nations Act 1945
   - informing members of a corporate group or designated business group about the risks involved in dealing with a customer
   - disclosing to a registered remittance network provider or its affiliate
   - disclosing to an owner-managed branch of an authorised deposit-taking institution
   - compliance with the law or law enforcement, and
   - giving effect to the AML/CTF Act or the Financial Transaction Reports Act 1988 (FTR Act).

18. The existing prohibition in section 123 will not substantially change but will be simplified to avoid confusion that makes the provision difficult to apply in practice. The amendment limits the right to freedom of expression in a proportionate way to clarify misunderstandings and confusion among reporting entities.

19. The Bill will simplify the ‘tipping off’ offence by clarifying that a reporting entity must not disclose to a person (other than the AUSTRAC CEO or the staff of AUSTRAC) that a SMR has been given or is required to be given to AUSTRAC, or any information from which a person could reasonably infer that a SMR has been or is required to be given. The requirement to report a SMR to AUSTRAC is triggered if any of the conditions specified in section 41 of the AML/CTF Act are satisfied.

20. The existing exceptions will continue to apply. The Bill will add two further exceptions that allow reporting entities to provide SMRs and related information to:
   - auditors for the purposes of an audit or review of the reporting entity’s AML/CTF program, and
   - foreign members of a corporate group or designated business group for the purposes of informing them about the risks involved in dealing with a customer.

21. The disclosure of information in the above circumstances will be subject to certain privacy safeguards.
22. To the extent that the ‘tipping off’ offence limits the rights of a person to impart information orally, in writing, or through any other media, the limitation is reasonable, necessary and proportionate in order to achieve the legitimate objective of protecting public order and national security.

23. The Bill also engages Article 19(2) by amending the offence created at proposed section 62 of the AFP Act to the extent that it criminalises the conduct of a person dishonestly representing himself or herself as a person onto whom a police award has been conferred.

24. The freedom of expression is restricted in order to respect and protect the rights and reputation of legitimate recipients of police awards and the rights of others to wear these awards in permissible circumstances. The restriction is provided by law through the introduction of the offence. The creation of the offence achieves the legitimate objective of criminalising the dishonest representation that a police award has been conferred on the person. This conduct undermines the prestige of being awarded a police award and damages the reputation of persons who have been rightfully conferred such an award.

25. The offence is necessary as there is currently no offence criminalising the dishonest representation of a police award, allowing individuals to dishonestly wear these awards without criminal penalty. It is also proportionate to the legitimate and specific purpose of the offence, as the dishonesty element strikes a balance between punishing individuals who unjustifiably represent themselves as a recipient of a police award while allowing individuals who have not received an award to wear these awards in permissible circumstances without committing an offence.

26. Further, the offence aligns with similar protections for Australian Defence Force service awards under subsection 80B(1) of the Defence Act 1903. Therefore, this offence reflects existing community standards that the improper use of service awards should attract a criminal penalty.

27. To the extent that this offence limits the right to the freedom of expression, it is therefore necessary and proportionate to achieving the legitimate objectives of preserving the integrity of police awards while promoting the rights of persons, both recipients and non-recipients, to use these awards in permissible circumstances.

Right to privacy

28. The Bill engages the right to privacy in Article 17 of the ICCPR by expanding the:

- exceptions to the ‘tipping off’ offence
- circumstances in which reporting entities may rely on customer identification and verification procedures undertaken by a third party, and
- purposes for which AUSTRAC information can be disclosed.

29. Article 17 of the ICCPR provides that no one shall be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence. The use of the term ‘arbitrary’ means that any interference with privacy must be in accordance with the provisions, aims and objectives of the ICCPR and should be reasonable in the particular circumstances. The United Nations Human Rights Committee has interpreted ‘reasonableness’ to imply that any limitation must be proportionate and necessary in the circumstances. The right to privacy can be limited by necessity in a democratic society in the interests of national security or public order.

Tipping off offence

30. The existing ‘tipping off’ offence in section 123 of the AML/CTF Act promotes the protection of privacy and reputation of the person who is the subject of a SMR. The offence recognises that SMRs are inherently subjective given they relate to a suspicion about an individual. This means that reports containing information about a person may be submitted to AUSTRAC even where a customer
has not engaged in any wrongdoing. A person’s privacy and reputation are protected by ensuring that SMRs and related information are prevented from being disclosed in the public domain. The proposed amendments promote the right to privacy by clarifying and simplifying the circumstances in which a SMR can be disclosed. The Bill will also expand the exceptions to the ‘tipping off’ offence to address recommendations from the Statutory Review Report. To the extent that the exceptions limit a person’s right to privacy, the amendments are necessary, reasonable and proportionate to achieving the legitimate objectives of protecting national security and public order.

31. The first additional exception will allow a reporting entity to disclose SMRs and related information to a person appointed or engaged by the reporting entity for the purposes of conducting an audit or review of the reporting entity’s AML/CTF program. An AML/CTF program is a requirement for reporting entities under the AML/CTF Act and ensures that entities identify the money laundering and terrorism financing risks facing their business and document the policies, procedures and controls to mitigate and manage these risks. Under subsection 162(2) of the AML/CTF Act, the CEO of AUSTRAC may direct a reporting entity to appoint an external auditor to conduct an audit of the reporting entity’s compliance with the Act.

32. An effective national AML/CTF regime relies on reporting entities complying with the requirements of the AML/CTF Act. Allowing reporting entities to make disclosures of SMRs and related information to auditors and reviewers assists entities to demonstrate compliance with ongoing customer due diligence and enhanced customer due diligence obligations. Promoting compliance with the AML/CTF Act supports collaboration and cooperation between reporting entities and AUSTRAC in efforts to detect, deter and disrupt money laundering, terrorism financing, and other serious crimes. This additional exception to the ‘tipping off’ offence is therefore reasonable and necessary to protect national security.

33. The Bill also introduces appropriate safeguards and controls to protect the confidentiality of information being disclosed and ensures that the limitation on the right to privacy is proportionate and not arbitrarily applied. The Bill prohibits a person who receives a SMR or related information for the purposes of an audit or review from disclosing to anyone else unless the disclosure is made in connection with the audit or review of the reporting entity’s AML/CTF program.

34. The second additional exception will allow a reporting entity to disclose SMRs and related information to a body corporate within the reporting entity’s corporate group, or another person with the reporting entity’s designated business group, for the purposes of informing them about the risks involved in dealing with a particular customer, subject to certain conditions. This will allow multinational financial institutions to take a global risk management approach to customers who hold accounts in multiple jurisdictions.

35. Sharing information within a corporate group, including to foreign entities, is consistent with the AML/CTF Act’s risk-based approach. It provides an opportunity to share information about potential criminal or terrorism-related activity and therefore promotes the objectives of protecting national security and public order. This addresses a current gap where information cannot be shared with foreign members of a corporate group or designated business group, which is detrimental given the global nature of money laundering and terrorism financing and the multinational nature of many reporting entities. This also assists Australia to fulfill its international obligations to combat money laundering and terrorism financing. This ‘tipping off’ offence exception is therefore reasonable and necessary to protect national security and public order.

36. In order to ensure that the limitation on the right to privacy is proportionate and will not be arbitrarily applied, the Bill also introduces appropriate safeguards and controls to ensure the confidentiality of information being disclosed. The Bill provides that a reporting entity can only share
this type of information with foreign members of a corporate group or designated business group that are regulated in a foreign jurisdiction by laws that give effect to some or all of the FATF recommendations. This safeguard ensures that information can only be shared with a foreign member of a corporate group or designated business group that is subject to similar laws as reporting entities in Australia. The foreign member must also provide the reporting entity with written undertakings about protecting the confidentiality of information, controlling the use of such information, and ensuring that the information is only used for the purpose it was disclosed.

37. The Bill also prohibits a reporting entity who has received information under this exception from disclosing it further unless it is to another reporting entity within the corporate group or designated business group for the purposes of informing them about the risks involved in dealing with the particular customer.

38. To the extent that the right to privacy is limited by the additional exceptions to the ‘tipping off’ offence, the limitations are reasonable, proportionate and necessary to achieve the legitimate objectives of protecting national security and public order.

39. The Bill will also expand the circumstances when a person who has received a section 49 notice can disclose certain information. Under section 49, an entrusted investigating official can request further information from a reporting entity or any other person following a report being submitted under sections 41, 43 or 45. Subsection 123(2) will permit a person to disclose to AUSTRAC, or an entrusted investigating official who has given a section 49 notice, that a notice has been received, that information or a document has been produced under the notice, or any information that could suggest these things have happened. This will avoid duplication of section 49 notices and increase the cooperation between law enforcement and competent authorities when combating money laundering, terrorism financing, or other serious crimes. The limitation on the right to privacy is proportionate as the disclosure of information can only happen to AUSTRAC, or entrusted investigating officials who are officials of Commonwealth agencies. The limitation on the right to privacy is also legitimate as it is authorised by law.

Reliance on customer identification and verification procedures

40. The Bill will insert sections 37A and 37B and replace section 38 of the AML/CTF Act to expand the circumstances in which reporting entities may rely on the applicable customer identification procedures undertaken by a third party. This will include the exchange of personal information including transactional information. These measures address a recommendation from the Statutory Review Report to ensure that Australia is consistent with the FATF Standards.

41. Expanding the circumstances for reliance will facilitate more efficient information sharing between reporting entities and other bodies to ensure the proper identification of customers. This supports cooperation and collaboration to detect, deter and disrupt money laundering, terrorism financing, and other serious crimes.

42. The limitation on the right to privacy is proportionate and not arbitrary as there are appropriate safeguards and controls in the Bill. All reporting entities are subject to the Privacy Act 1988 and subsequently must abide by the Australian Privacy Principles. Other safeguards include requiring an agreement or arrangement to exist between entities before reliance can occur, which must accord with the requirements specified in the Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1) (AML/CTF Rules). The relying reporting entity must also regularly assess the agreement or arrangement and terminate it if, after carrying out an assessment under section 37B, they do not have reasonable grounds to believe that each of the relevant requirements prescribed by the AML/CTF Rules is being met.
43. To the extent that a person’s right to privacy is limited by the sharing of personal information to allow a reporting entity to rely on customer identification undertaken by a third party, the limitations are reasonable, proportionate and necessary to achieve the legitimate objectives of protecting national security and public order.

Disclosure of AUSTRAC information
44. The Bill will significantly simplify and consolidate provisions within existing Part 11 of the AML/CTF Act which deal with secrecy of, and access to AUSTRAC information. The Bill will amend the definition of AUSTRAC information to include information obtained by a person, or generated by a person, in their capacity as an AUSTRAC entrusted person or ‘FTR information’ as defined in the FTR Act. AUSTRAC information includes sensitive personal information, SMRs and related information.

45. The overall amendments introduced by the Bill simplify and consolidate provisions to reduce complexity in Part 11 and address a recommendation from the Statutory Review Report. The substantial changes to the information-sharing framework are to:
   - expand the offence to prohibit an AUSTRAC entrusted person from unlawfully accessing, making a record of, authorising access to or otherwise using AUSTRAC information
   - allow a SMR or related information to be adduced as evidence in criminal proceedings under sections 121, 123, 126, 128, 129, 136, 137, 161, 162, 165 and all civil proceedings under section 175
   - allow the AUSTRAC CEO to authorise specified officials of Commonwealth, State or Territory agencies to access AUSTRAC information rather than specifying each as a ‘designated agency’ in the AML/CTF Act
   - expand the offence for an official of a Commonwealth, State or Territory agency to prohibit the unlawful use of AUSTRAC information
   - expand the ability of government agencies to share AUSTRAC information with a foreign agency
   - introduce an offence prohibiting a person who is disclosed AUSTRAC information unlawfully from making a record of, disclosing or otherwise using that information
   - introduce a power for the AUSTRAC CEO to impose conditions on certain persons who have received AUSTRAC information
   - provide the ability for an AUSTRAC official to disclose AUSTRAC information to a Minister for performance of their responsibilities, and
   - provide the ability for a member of a taskforce that is established by the AUSTRAC CEO to deal with AUSTRAC information in the same way an AUSTRAC official can deal with AUSTRAC information.

46. The proposed amendments engage the right to privacy in Article 17 of the ICCPR. However, they pursue the legitimate objective of protecting national security and public order. The amendments are also proportionate as they are limited to the sharing of information about potentially criminal or terrorism-related activity for law enforcement purposes. They are also limited through the various safeguards provided by the Act such as the AUSTRAC CEO imposing conditions on the use of AUSTRAC information that is disclosed to certain people, and government agencies requiring undertakings from foreign agencies on how they will protect the confidentiality of AUSTRAC information disclosed to them. The measures do not constitute a radical departure from current information-sharing practices under the AML/CTF regime, and are necessary to strengthen the sharing of financial intelligence between competent authorities. This enhanced capacity to share information will help government agencies to better combat money laundering and terrorism financing and assist Australia to fulfil its international obligations. The Bill will enhance the AUSTRAC CEO’s ability to carry out his or her legislative functions to:
   - retain, compile, analyse and disseminate AUSTRAC information
provide access to and share AUSTRAC information to support domestic and international efforts to combat money laundering, terrorism financing and other serious crimes, and

provide advice and assistance to the persons and agencies entitled or authorised to access AUSTRAC information under Part 11.

47. To the extent that a person’s right to privacy is limited by the sharing of AUSTRAC information, the limitations are reasonable, proportionate and necessary to achieve the legitimate objectives of protecting national security and public order.

Conclusion

48. The Bill is compatible with human rights because, to the extent that it may limit human rights, those limitations are reasonable, necessary and proportionate.
NOTES ON CLAUSES

Preliminary

Clause 1 – Short Title

1. This clause provides for the short title of the Act to be the *Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Act 2019* (AML/CTF amendment Act).

Clause 2 – Commencement

2. This clause provides for the commencement of each provision in the AML/CTF amendment Act, as set out in the table.

3. Subclause 2(1) provides that each provision of the AML/CTF amendment Act specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table, and that any other statement in column 2 has effect according to its terms.

4. Item 1 of the table provides that sections 1 to 3 and anything in the AML/CTF amendment Act not elsewhere covered by this table commence on the day this Act receives Royal Assent.

5. Item 2 of the table provides that Parts 1 to 4 of Schedule 1 commence on a day or days to be fixed by Proclamation. However, if any of the provisions do not commence within the period of six months beginning on the day the AML/CTF amendment Act receives Royal Assent, they commence on the day after the end of that period.

6. Item 3 of the table provides that Part 5 of Schedule 1 commences on a day or days to be fixed by Proclamation. However, if any of the provisions do not commence within the period of 18 months beginning on the day the AML/CTF amendment Act receives Royal Assent, they commence on the day after the end of that period.

7. Item 4 of the table provides that Parts 6 and 7 of Schedule 1, commence the day after the AML/CTF amendment Act receives Royal Assent.

8. A note to the table provides that the table relates only to the provisions of this Act as originally enacted. It will not be amended to deal with any later amendments of this Act.

9. Subclause 2(2) provides that any information in column 3 of the table is not part of this Act. Information may be inserted in this column, or information in it may be edited, in any published version of this Act.

Clause 3 – Schedules

10. This clause provides that legislation that is specified in a Schedule to this Act is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this Act has effect according to its terms.

Schedule 1 – Amendments

Part 1 – Identification Procedures

*Anti-Money Laundering and Counter-Terrorism Financing Act 2006*

Item 1 – Section 32

governmental body responsible for setting international standards for combating money laundering and terrorism financing.

12. Section 32 of the Act provides that a reporting entity must generally not provide a designated service to a customer if the reporting entity is unable to carry out the applicable customer identification procedure (ACIP).\(^1\)

13. In 2015, the FATF’s MER recommended that the prohibition under the AML/CTF Act that a designated service can only be provided if customer due diligence (CDD) can be performed should be more explicit. The FATF also criticised Australia for not imposing an obligation under section 32 for a reporting entity to consider making a suspicious matter report (SMR) in circumstances where a service is not provided because the necessary CDD cannot be performed.

14. This item rectifies both of these deficiencies by making the operation of section 32 more explicit, and by providing a note that links section 32 to section 41 (the obligation to submit a SMR) if the ACIP cannot be performed.

**Items 2 and 3 – Sections 34 and 35**

15. Items 2 and 3 are consequential amendments to subsections 34(1) and 35(1) to address the insertion of new section 37A and 38.

**Item 4 – Section 37**

16. Item 4 inserts a note at the end of section 37 to clarify liability in the context of an agency arrangement under section 37.

17. The Statutory Review Report recommended that, in line with Recommendation 17 of the FATF standards, the Act should be amended to expand the ability of reporting entities to rely on customer identification procedures performed by a third party, subject to the following conditions:

- where the third party agrees to being relied on, the relying business remains ultimately responsible for CDD measures; and
- where the third party is outside of Australia, the third party is subject to appropriate regulation and similar CDD requirements as are applicable in Australia.

18. Separately, the MER criticised Australia’s compliance with Recommendation 17 because it is not explicitly stated in the Act that the reporting entity relying on a third party remains ultimately responsible for CDD measures.

19. Section 37 of the Act provides that the ACIP (defined in section 5) may be carried out by an agent of a reporting entity if the agent has been authorised by the reporting entity to carry out the ACIP on the reporting entity’s behalf. Section 37 of the Act is framed in line with the common law principle of agency. As such, a reporting entity is ultimately responsible or liable for the actions of its agent.

**Item 5 – After section 37**

20. Item 5 responds to a recommendation in the Statutory Review Report, providing reporting entities with greater flexibility to rely upon CDD procedures undertaken by a broader range of Australian and foreign entities. This is intended to create efficiencies enabling industry to reduce some of the costs associated with conducting CDD and fulfilling their AML/CTF obligations.

21. New section 37A allows reporting entities to enter into a written agreement or arrangement (‘CDD arrangement’) with another reporting entity or another person in order to rely on the ACIP (for domestic entities) or other customer identification procedure (as prescribed in the AML/CTF Rules) carried out by the other reporting entity or other foreign entity.

---

\(^1\) The ACIP is the means by which reporting entities fulfil their customer due diligence obligations.
22. This new section takes a broad approach to the third parties that may be relied upon. The key limitation on who can be relied upon is drawn from the FATF Standards. FATF Recommendation 17 requires that the third party is subject to appropriate AML/CTF regulation and supervision, and that where reliance on foreign entities is permitted, the money laundering and terrorism financing risks of the country are considered. New Chapter 7 of the AML/CTF Rules addresses these third party requirements.

23. This section also ensures that a ‘CDD arrangement’ may only be entered into if the reporting entity has reasonable grounds to believe that each of the requirements in the AML/CTF Rules (including that the other party is subject to relevant AML/CTF obligations and that party has appropriate measures in place for compliance with those obligations) are met at the time of entering into the arrangement.

24. New subsection 37A(2) gives effect to the ‘CDD arrangement’ by providing relying parties with a safe harbour from liability for breaches of section 32. Where the reporting entity:
   - has entered into the ‘CDD arrangement’ in accordance with new section 37A
   - has conducted regular assessments of the arrangement in accordance with new section 37B
   - has obtained relevant identity information, and
   - is satisfied of the requirements prescribed by the AML/CTF Rules (including that the reporting entity is able to obtain copies of any other relevant documentation without delay),

the relying party would not be held liable for isolated breaches of compliance with the ACIP (or other customer identification procedure) requirements committed by the relied on party.

25. However, if circumstances indicate that due diligence performed by the reporting entity on the ‘CDD arrangement’ does not meet the requirements in the AML/CTF Rules, the reporting entity relying on the other party’s ACIP (or other customer identification procedure) may be liable under section 32 (for providing a service before an appropriate ACIP has been carried out).

26. This ‘CDD arrangement’ model of providing a safe harbour from liability for isolated breaches of an ACIP failure is similar to section 33 of New Zealand’s Anti-Money Laundering and Countering Financing of Terrorism Act 2009. This section provides that a reporting entity (as regulated under New Zealand’s AML/CTF regime) relying on a third party to conduct the CDD procedure is not responsible for ensuring that CDD is carried out in accordance with the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 if the following conditions are met:
   - the reporting entity is acting in good faith when relying on a third party, and
   - the reporting entity has reasonable cause to believe the reporting entity that is relied on has conducted relevant CDD procedures to at least the standard required by the Act and regulations.

27. The belief that the ‘other party has conducted relevant CDD procedures to at least the standard required by the Act and regulations’ is akin to how the ‘CDD arrangement’ model operates, in that a reporting entity will conduct a due diligence assessment (and further assessments at regular intervals) in order to establish (and maintain) reasonable grounds to believe that the relied on party has the systems and procedures in place in order to meet compliance with the ACIP (or other customer identification procedure) requirements. As with the New Zealand model, there must also be a ‘reasonable’ basis for this belief. If circumstances indicate due diligence performed by the reporting entity on the other party’s procedures is insufficient, the reporting entity would lose the protection afforded by a ‘CDD arrangement’ and would be liable under section 32.

28. New subsection 37A(3) will automatically suspend the ‘CDD arrangement’ if, after completing an assessment under section 37B, the reporting entity does not have reasonable grounds to believe that
each of the requirements prescribed by the AML/CTF Rules for the purposes of paragraph 37A(1)(b) are being met. New subsection 37A(4) states that the ‘CDD arrangement’ will automatically resume once the reporting entity can again be satisfied on reasonable grounds that the requirements prescribed by the AML/CTF Rules are being met.

29. A reporting entity will generally have reasonable grounds to believe that the relevant requirements are being met where they have previously reached this conclusion and they are not aware of any circumstances that could bring this conclusion into significant doubt. Situations where significant doubt could arise could include those where a significant breach, or a series of other breaches, is detected, there is relevant adverse media or adverse information about the third party relied upon, inadequate communication from the relied-upon third party in response to queries by the reporting entity, or there has been considerable change in money laundering or terrorism financing risk that would render current arrangements inappropriate.

30. The length of the suspension period will depend on the time it takes the other party to remediate any breach, or breaches, and when there are reasonable grounds to believe that the requirements prescribed in the AML/CTF Rules are again being met. Throughout the suspension period, reporting entities will be required to undertake the ACIP themselves, or rely on a ‘CDD arrangement’ entered into with another party that has undertaken an ACIP or other customer identification procedure on the relevant customer in accordance with the requirements of section 37A.

31. Subsections 37A(3) and (4) compel reporting entities to take a proactive and considered approach to assessing and amending their ‘CDD arrangement’, and rewards the reporting entity for doing so by providing them with seamless protection from legal liability under section 32 for CDD carried out by third parties under arrangement.

32. New section 37B requires reporting entities that have entered into a ‘CDD arrangement’ to carry out regular assessments in accordance with the AML/CTF Rules, and to prepare a written record of each assessment within 10 business days after completion of the assessment. This is intended to ensure reporting entities are obliged to continually assess whether it is appropriate to continue the CDD arrangement.

Item 6 – Section 38

33. Item 6 repeals section 38 and substitutes a provision that enables reporting entities to rely on an ACIP or other customer identification procedure (as prescribed in the AML/CTF Rules) carried out by another reporting entity or foreign entity.

34. Currently, a reporting entity may rely on an ACIP undertaken by another reporting entity in limited circumstances. This is set out in section 38 of the Act and Chapter 7 of the AML/CTF Rules. These circumstances are:

- where a licensed financial adviser arranges for a customer to receive a designated service from a second reporting entity (e.g. where a financial adviser refers a customer to a bank, the bank can rely on the ACIP carried out by the adviser), and

- where a customer of one member of a designated business group becomes a customer of another member of the designated business group, and is required to undergo the ACIP.

35. With respect to foreign entities, a reporting entity is currently unable to rely on other customer identification procedures conducted outside Australia unless the AUSTRAC CEO provides the reporting entity with a modification. In March 2009, the AUSTRAC CEO made a declaration under subsection 248(1)(b) modifying subsection 38(b) to permit reliance on customer identification procedures conducted in a foreign country where:

- the customer identification procedure is carried out by an Australian reporting entity or a subsidiary of an Australian reporting entity (based overseas), and
• the reporting entity determines on a risk-basis that the customer identification procedure is comparable to that required under the Act.

36. This modification was primarily intended to allow Australian reporting entities to rely on a customer identification procedure conducted in New Zealand. The Explanatory Note to the declaration provides an example of an Australian reporting entity relying on a customer identification procedure comparable to the ACIP conducted by a New Zealand subsidiary.

37. Feedback from reporting entities has indicated that existing section 38 of the Act is of limited utility because it does not enable reliance in Australia or overseas on an ACIP or other customer identification procedure undertaken by other related parties (such as other members of a ‘designated business group’ within the meaning of this Act, or a ‘related body corporate’ within the meaning of the Corporations Act 2001).

38. The new section 38 takes a broad approach to the third parties that may be relied upon. The key limitation on who can be relied upon is drawn from the FATF Standards. FATF Recommendation 17 requires that the third party is subject to appropriate AML/CTF regulation and supervision, and that where reliance on foreign entities is permitted, the money laundering and terrorism financing risks of the country are considered. New Chapter 7 of the AML/CTF Rules address these third party requirements.

39. Given this provision is neutral as to the types of entities that can be relied upon, this will enable continued reliance on licensed financial advisors and other members of a designated business group. In addition, this will allow reporting entities to rely on other domestic and offshore members of their global corporate or designated business group without the need to enter into a ‘CDD arrangement’ as part of section 37A. In particular, this expansion will benefit multinational corporations (such as major financial institutions and fund managers) that can harness the opportunities of being part of a trusted network of members that have operations in Australia and all throughout the world.

40. Reporting entities can rely on these entities when they have reasonable grounds to believe that it is appropriate to rely on the ACIP or other customer identification procedure (as prescribed in the AML/CTF Rules) having regard to the money laundering and terrorism financing risks the relying reporting entity faces. For example, the relied on entity may have undertaken a simplified ACIP on the relevant customer given the service the customer was requesting was considered low risk. However, the reporting entity wishing to rely on that ACIP may be providing a different, higher risk service, which would require additional customer due diligence. As such, this requires reporting entities to apply the risk-based approach to determine whether the ACIP or other customer identification procedure is sufficient given the money laundering and terrorism financing risks associated with the customer type or service.

41. Aside from whether it is appropriate to rely on the other party having regard to the risks associated with the customer type or service, reporting entities will remain ultimately responsible or liable under section 32 for failure by the relied on party to carry out the ACIP or other customer identification procedure. This is in contrast to reliance under new section 37A that can afford reporting entities a safe harbour from liability where there exists isolated breaches of compliance with the ACIP (or other customer identification procedure) requirements.

42. Given there is a cost associated with entering into and maintaining a ‘CDD arrangement’ with other parties (under section 37A), those reporting entities that are members of multinational corporations that can rely on trusted third parties may benefit most from the expansion of section 38. For those entities, this reform is expected to create significant regulatory efficiencies and reduce the costs associated with conducting CDD.

**Item 7 – Section 104**

43. Item 7 amends the simplified outline at section 104 by removing reference to ‘a reporting entity must retain a record of an applicable customer identification procedure for 7 years after the end of the
reporting entity’s relationship with the relevant customer’. Instead, this item substitutes a requirement for a reporting entity to retain records relating to both the applicable customer identification procedures carried out, and the assessments it carries out of the ‘CDD arrangement’ it has entered into relating to its reliance on applicable customer identification procedures, or other procedures, carried out by another person.

**Item 8 – Division 3 of Part 10 (heading)**

44. Item 8 repeals the heading for Division 3 of Part 10 and inserts ‘Division 3—Records in connection with the carrying out of identification procedures’.

**Item 9 – Section 114**

45. Item 9 repeals section 114 and substitutes a new sections 114 and 114A.

46. Currently, section 114 facilitates the exchange of records relating to an ACIP undertaken by a reporting entity (either a licensed financial advisor or another member of a designated business group) as part of reliance permitted under section 38. This provision is unnecessarily complex, as it is premised on the exchange of records occurring following the provision of the designated service (after ‘the customer identification day’ in the words of section 114).

47. To address this complexity, new sections 37A and 38 require reporting entities (that are relying on other parties) to obtain information pertaining to the identity of a customer prior to the provision of a designated service. This allows for section 114 to be significantly simplified, because the exchange of records is dealt with under new sections 37A and 38. Accordingly, the new provision only applies to record-keeping of information obtained under sections 37A and 38 and not the exchange of information.

48. New section 114A requires reporting entities to retain records, or copies of records, of assessments of agreements or arrangements prepared under paragraph 37B(1)(c) for 7 years after the completion of the preparation of the record.

49. Subsection 114A(2) provides that subsection 114A(1) is a civil penalty provision.

**Item 10 – Application and saving provisions**

50. Item 10 provides the application and savings provisions for existing provisions prior to the commencement of the amendments.

51. The prohibition on providing a designated service without carrying out the ACIP, will apply in relation to a designated service that commences to be provided on or after the commencement of this item.

52. New section 37A applies in relation to an agreement or arrangement entered into on or after the commencement of this item.

53. Regarding reliance under section 38, reporting entities will be permitted to rely on an ACIP or other customer identification procedure (as prescribed in the AML/CTF Rules) carried out before, on or after the commencement of this item.

**Part 2 - Correspondent Banking**

*Anti-Money Laundering and Counter-Terrorism Financing Act 2006*

**Item 11 – Sections 94 to 99**

54. Item 11 repeals sections 94 to 99 to simplify and streamline Part 8 of the Act.

55. Part 8 provides obligations for financial institutions that are entering, or are currently in, a correspondent banking relationship. Section 5 defines a correspondent banking relationship as a relationship that involves the provision of banking services by a financial institution to another
financial institution in another country. Banking service includes all banking services that involve a vostro account.

56. Part 8 implements FATF Recommendation 13. Recommendation 13 requires financial institutions involved in correspondent banking relationships to perform certain measures on the respondent financial institution in addition to normal customer due diligence obligations.

57. Item 11 inserts section 94 which is the simplified outline of Part 8.

58. Item 11 inserts section 95 which prohibits correspondent banking relationships with shell banks. This prohibition is in recognition of the unreasonable risk of money laundering posed by such relationships.

59. Subsection 95(1) largely replicates existing subsection 95(1) which prohibits a financial institution entering a correspondent banking relationship with a shell bank, or a financial institution that has a correspondent banking relationship with a shell bank.

60. The requirement to prove that a financial institution has been reckless as to whether the other person is a shell bank, or a financial institution that has a correspondent banking relationship with a shell bank, has been removed. This will reduce unnecessary complexity and ensure industry are clear about their obligations under the Act. The concept of recklessness undermines the intent of the prohibition which is to impose an obligation on financial institutions to know that they are not dealing with a shell bank or a financial institution that has a correspondent banking relationship with a shell bank.

61. The existing prohibition has been expanded to prohibit a financial institution from entering a correspondent banking relationship with a financial institution that permits its accounts to be used by a shell bank. This amendment addresses the Statutory Review Report’s recommendation to prohibit corresponding banking relationships with institutions that are able to enter into a correspondent banking relationship with a shell bank. It will also improve Australia’s compliance with FATF Recommendation 13, which states that financial institutions ‘should be required to satisfy themselves that respondent financial institutions do not permit their accounts to be used by shell banks.’

62. Subsection 95(2) consolidates existing subsections 96(1) and (2) to streamline the provisions and to ensure the obligations on financial institutions are clear. This subsection provides that a financial institution must terminate its correspondent banking relationship within 20 days of becoming aware that the other financial institution in the relationship is either a shell bank, a financial institution that is in a relationship with a shell bank, or a financial institution that permits its accounts to be used by a shell bank. Alternatively, if the other financial institution is in a correspondent banking relationship with a shell bank, a financial institution may request that the financial institution terminate its relationship with the shell bank. The AUSTRAC CEO may determine a longer period than 20 days.

63. Subsection 95(3) largely replicates existing subsection 96(3). The provision has been simplified to reduce complexity and to ensure the obligations for financial institutions are clear. The subsection provides that if a financial institution has requested under subsection 95(2) that its correspondent bank terminate its relationship with a shell bank, and the request is not complied with, the financial institution must terminate the correspondent banking relationship within 20 days. The AUSTRAC CEO may determine a longer period than 20 days.

64. Subsection 95(4) replicates existing subsection 96(4) and provides that subsections 95(1), (2) and (3) are civil penalty provisions.

65. Item 11 inserts section 96, which provides for due diligence assessments of correspondent banking relationships upon entry and throughout the life of the relationship. The requirement to perform due diligence assessments is linked to FATF Recommendation 13, which requires financial institutions to gather information about their correspondent financial institutions’ business, reputation, AML/CTF controls, and supervision of these controls.
66. The requirement for additional due diligence is justified on the basis that correspondent banking relationships are vulnerable to misuse and exploitation for money laundering and terrorism financing because they involve a financial institution carrying out a transaction on behalf of another financial institutions’ customers where information on that customer is very limited. These risks are particularly high when the respondent financial institution is located in a country with weak money laundering and terrorism financing laws, or poor supervision of AML/CTF laws.

67. Subsection 96(1) differs to existing section 97 relating to due diligence assessments prior to entering a correspondent banking relationship. Existing section 97 provides that prior to entry into a correspondent banking relationship, the financial institution must carry out an assessment of the risk that the correspondent banking relationship might involve or facilitate money laundering or terrorism financing. The outcome of that preliminary risk assessment informs the obligation to undertake a due diligence assessment in accordance with the AML/CTF Rules.

68. Subsection 96(1) will remove the requirement for a preliminary risk assessment and introduce a mandatory due diligence assessment to be conducted in accordance with the AML/CTF Rules prior to entering into any correspondent banking relationship. This will address a key deficiency identified in Australia’s 2015 MER, and improve Australia’s compliance with FATF Recommendation 13. Subsection 96(1) will also require a financial institution to make a written record of the due diligence assessment, and obtain senior officer approval to enter the relationship having regard to the matters in the AML/CTF Rules. The latter replicates existing subsection 99(1), however, it applies to a correspondent banking relationship with a financial institution rather than ‘another person’ as currently provided. This ensures consistent terminology with the prohibition in subsection 96(1).

69. Subsection 96(2) largely replicates existing subsection 99(2), however, it applies to a correspondent banking relationship with a financial institution rather than ‘another person’ as currently provided. This ensures consistent terminology with the prohibition in subsection 96(1).

70. Subsection 96(2) introduces a timeframe for when a financial institution that has a correspondent banking relationship with another financial institution that involves a vostro account, must prepare a written record setting out the responsibilities of both parties. The amendment requires a written record to be prepared within 20 business days of the financial institution entering into the relationship. This subsection implements the requirement under FATF Recommendation 13 for a financial institution to clearly understand the respective responsibilities of each institution in a correspondent banking relationship.

71. Subsection 96(3) consolidates existing section 98. The subsection removes the requirement for regular assessments of risk on whether the correspondent institution may involve or facilitate money laundering or terrorism financing. Consistent with subsection 96(1), a financial institution will be required to conduct mandatory regular due diligence assessments in accordance with the AML/CTF Rules. The assessments must be performed as often as prescribed by the AML/CTF Rules and a written record of each assessment be prepared within 10 business days of its completion. A new requirement provides that a financial institution must obtain senior officer approval for remaining in the correspondent banking relationship within 20 business days following the assessment. This approval is consistent with that required for entering a correspondent banking relationship.

72. Subsection 96(4) replicates existing subsection 98(7) and provides that subsections 96(1), 96(2) and 96(3) are civil penalty provisions.

Item 12 – Division 6 of Part 10 (heading)

73. Item 12 repeals the heading for Division 6 of Part 10 and inserts ‘Division 6—Records about correspondent banking relationships’. This reflects that records will be made in relation to correspondent banking relationships, not only about due diligence assessments, but also the respective responsibilities of both parties.

Item 13 – Section 117 (heading)
74. Item 13 repeals the heading for section 117 and inserts ‘Retention of records about correspondent banking relationships’. This reflects that records will be made in relation to correspondent banking relationships, not only about due diligence assessments, but also the respective responsibilities of both parties.

**Item 14 – Subsection 117(1)**

75. Item 14 amends subsection 117(1) to remove references to subsection 97(2) or 98(2) and instead substitutes reference to section 96. This follows the consolidation and simplification of Part 4 and ensures that the record of the due diligence assessment made before entering into, or during, a correspondent banking relationship is retained for 7 years.

**Item 15 – Paragraph 1(5)(a) of Schedule 1**

76. Item 15 amends paragraph 1(5)(a) of Schedule 1 to omit reference to section 96 or section 99 following the consolidation and simplification of Part 4. Paragraph 1(5)(a) provides that the correspondent banking provisions in the Act are confined to the banking power within paragraph 51(xiii) of the Constitution.

**Item 16 – Paragraph 1(5)(b) of Schedule 1**

77. Item 16 amends paragraph 1(5)(b) of Schedule 1 to omit reference to section 96, 97 and 98 and substitute sections 95 and 96 following the consolidation and simplification of Part 4. Paragraph 1(5)(b) provides that the correspondent banking provisions in the Act are confined to the banking power within paragraph 51(xiii) of the Constitution.

**Item 17 – Application provisions**

78. Item 17 provides the application provisions for the amendments to Part 4.

79. The prohibition on entering into certain correspondent banking relationships with shell banks will apply in relation to a correspondent banking relationship that is entered into on or after the commencement of this item.

80. The requirement to terminate certain correspondent banking relationships will apply on and after the commencement of this item in relation to a correspondent banking relationship that was entered into before, on or after that commencement, where the financial institution becomes aware of the relevant matters on or after that commencement.

81. The requirement to conduct an entry due diligence assessment will apply in relation to a correspondent banking relationship that is entered into on or after the commencement of this item.

82. The requirement to make a written record of the responsibilities of both parties to a correspondent banking relationship within 20 business days will apply in relation to a correspondent banking relationship that is entered into on or after the commencement of this item.

83. The requirement to conduct ongoing due diligence assessments will apply on and after the commencement of this item in relation to a correspondent banking relationship that was entered into before, on or after that commencement, where the assessments are required to be carried out on or after that commencement.

**Item 18 – Saving provisions**

84. Item 18 provides the savings provisions for existing provisions prior to the commencement of the amendments.

85. The prohibition on entering into certain correspondent banking relationships that is in force immediately before the commencement of this item continues to apply on and after that commencement in relation to a correspondent banking relationship entered into before that commencement.
86. The requirement to terminate certain correspondent banking relationships that is in force immediately before the commencement of this item, continues to apply on and after that commencement in relation to a correspondent banking relationship that was entered into before that commencement, and the financial institution becomes aware of relevant matters before that commencement.

87. The requirement to conduct preliminary risk assessments and subsequent due diligence assessments that is in force immediately before the commencement of this item continues to apply on and after that commencement in relation to a correspondent banking relationship that was entered into before that commencement.

88. The requirement to conduct regular due diligence assessments that is in force immediately before the commencement of this item, continues to apply on and after that commencement in relation to a correspondent banking relationship that was entered into before that commencement, where the assessments were required to be carried out before that commencement.

89. The requirement to document the responsibilities of each party to a correspondent banking relationship that is in force immediately before the commencement of this item continues to apply on and after that commencement in relation to a correspondent banking relationship that was entered into before that commencement.

90. The requirement to retain records of due diligence assessments that is in force immediately before the commencement of this item continues to apply on and after that commencement in relation to a record prepared under subsection 97(2) or 98(2) before that commencement.

Part 3 - Tipping Off Offence

Anti-Money Laundering and Counter-Terrorism Financing Act 2006

Item 19 – Subsections 123(1), (2) and (3)

91. Item 19 repeals existing subsections 123(1), (2) and (3) and inserts new subsection 123(1), which simplifies and consolidates the prohibition on tipping off. This amendment responds to concerns from reporting entities about the complexity of obligations under the Act. It also addresses the Statutory Review Report's overarching recommendation that the Act be simplified so that reporting entities have greater clarity about their obligations.

92. The prohibition in new subsection 123(1) has not substantively changed from the prohibitions contained in existing subsections 123(1) and (2). Reporting entities remain prohibited from disclosing the fact that a SMR has been or is required to be given to AUSTRAC, or information from which it could be reasonably inferred that a SMR has been or is required to be given to AUSTRAC (related information), unless an exception applies.

93. Existing subsection 123(2) prohibits the disclosure of information related to a reporting entity having formed an ‘applicable suspicion’ under subsection 41(1). Stakeholders reported uncertainty around the scope of the term ‘applicable suspicion’, particularly around the point at which an applicable suspicion is considered to have been ‘formed.’ The new subsection 123(1) does not refer to an ‘applicable suspicion.’

94. New subsection 123(1) is consistent with FATF Recommendation 21, which states that financial institutions and their directors, officers and employees should be prohibited by law from disclosing the fact that a SMR or related information is being filed with a country’s Financial Intelligence Unit.

95. New subsection 123(2) replaces existing subsection 123(3). Existing subsection 123(3) provides that if a reporting entity is required under subsection 49(1) to give information or produce a document to a person, the reporting entity must not disclose to anyone else that the reporting entity has been required to do so. Consequently, if a reporting entity has been issued with a section 49 notice by AUSTRAC and a section 49 notice by another government agency in relation to the same person, the
reporting entity cannot disclose to either AUSTRAC or the other government agency that they have received a section 49 notice from either agency regarding the same person. This prohibition creates an administrative burden for reporting entities, and prevents opportunities for collaboration between government agencies.

96. Accordingly, new subsection 123(2) maintains the prohibition in relation to section 49 notices, with certain exceptions. A reporting entity can disclose the existence of a section 49 notice (as well as information provided in response to the notice) to an ‘AUSTRAC entrusted person’, to a government agency who gave the initial section 49 notice or to another government agency who has given a subsequent section 49 notice in relation to the same person.

Item 20 – Subsection 123(4) (heading)

97. Item 20 repeals the heading for subsection 123(4) and inserts ‘Exception—crime prevention’. In the current Act, exceptions to the tipping off offence are provided for under the heading ‘Exceptions.’ To make the exceptions clearer, each type of exception now has its own heading in the format ‘Exception—[type of exception]’.

Item 21 – Subsection 123(4)

98. Item 21 omits ‘Subsection (2)’ and substitutes ‘Subsection (1)’ in subsection 123(4) to reflect the amendment related to the consolidation of existing subsections 123(1) and (2).

Item 22 – Before subsection 123(5)

99. Item 22 inserts the heading ‘Exception—legal advice’ before subsection 123(5) consistent with the clearer drafting structure for the section.

Item 23 – Subsection 123(5)

100. Item 23 omits ‘Subsection (2)’ and substitutes ‘Subsection (1)’ in subsection 123(5) to reflect the amendment related to the consolidation of existing subsections 123(1) and (2).

Item 24 – After subsection 123(5A)

101. Item 24 creates a new exception to the prohibition on tipping off. Subsection 123(5B) allows a reporting entity to share a SMR and related information to external auditors that are auditing or reviewing the reporting entity’s AML/CTF program. Under Part 7 of the Act, reporting entities are required to have, and comply with, an AML/CTF program before commencing to provide a designated service.

102. Introducing this exception addresses recommendation 14 of the Statutory Review Report that, subject to appropriate controls and safeguards, the Act should be amended to permit reporting entities to disclose SMR and related information to external auditors that have been appointed under Part 13 of the Act. Access to this information will assist external auditors to determine whether reporting entities are identifying, mitigating and managing their money laundering and terrorism financing risks. The quality of SMR and related information provided by a reporting entity to AUSTRAC is used to demonstrate to an external auditor that a reporting entity’s ongoing CDD and enhanced CDD measures are effective.

103. This exception goes beyond the Statutory Review Report’s recommendation by also applying to external auditors that the reporting entity has engaged under a self-initiated audit or review of the reporting entity’s AML/CTF program (not just auditors appointed by AUSTRAC under Part 13). The intention of this extended application is that it will lead to better-informed self-initiated audits and reviews, and ultimately increase reporting entities’ compliance with their AML/CTF obligations.

104. Subsection 123(5C) prohibits external auditors from further disclosing the information, except in connection with the audit or review of the reporting entity’s AML/CTF program. This exception applies to external auditors that the reporting entity has been required to appoint under Part 13 of the
Act, and external auditors that the reporting entity has chosen to engage. This subsection introduces a safeguard to limit the on-disclosure of such sensitive information.

105. As noted in item 20, each type of exception to the tipping off offence now has its own heading in the format ‘Exception—[type of exception]’. Consequently, item 24 creates the headings ‘Exception—audit or review of anti-money laundering and counter-terrorism financing program’ immediately after subsection 123(5A) and ‘Exception—Charter of the United Nations Act 1945’ before subsection 123(6).

**Item 25 – Subsection 123(6)**

106. Item 25 omits ‘Subsection (2)’ and substitutes ‘Subsection (1)’ in subsection 123(6) to reflect the amendment related to the consolidation of old subsections 123(1) and (2).

**Item 26 – Subsections 123(7) and (7AA)**

107. Item 26 repeals existing subsection 123(7) and 123(7AA) and introduces an expanded exception to the prohibition on tipping off for members of a designated business group or a corporate group.

108. Currently, one of the exceptions provides that reporting entities could share SMR and related information with other reporting entities in their ‘designated business group’ (within the meaning of the Act) and/or their ‘corporate group’ (within the meaning of ‘related bodies corporate’ in the Corporations Act 2001). Disclosure is permitted for the purposes of informing the other reporting entity about the suspected risks involved in dealing with the customer to whom the SMR and related information concern. The requirement that both parties are reporting entities under the Act means that SMR and related information cannot be shared with designated business group or corporate group members outside of Australia. This requirement is unnecessarily restrictive and does not reflect the globalised nature of the financial industry where members of designated business groups or corporate groups can be based in countries all around the world, and may have centrally-located financial crime management hubs.

109. Accordingly, item 26 inserts new subsection 123(7) which expands the exception to allow a reporting entity to share SMR and related information with other bodies corporate in its corporate group, within or outside of Australia, provided that:

- the information relates to the affairs of a customer (a customer, former customer, or a person who made inquiries about a designated service) of the reporting entity, about whom an SMR has been submitted
- the other member of the corporate group is a reporting entity or is regulated by foreign laws that give effect to some or all of the FATF Recommendations
- if the other member of the corporate group is not a reporting entity, then that member has given written undertakings to:
  - protect the confidentiality of the information
  - control the use of information, and
  - ensure information is only used for the purpose it is disclosed
- the information is disclosed for the purpose of informing the other member of the corporate group about the risks involved in dealing with the customer who is the subject of the lodged SMR.

110. This amendment addresses, and goes beyond, the Statutory Review Report’s recommendation that, subject to appropriate controls and safeguards, the Act should be amended to permit reporting entities to disclose SMR and related information to foreign parent entities.

111. The intention of the expanded exception reflects a need to allow reporting entities, and related entities that are part of their global structures, to more effectively manage the risks associated with the international footprint of their business. Specifically, entities will be able to manage the risk posed by particular customers, noting that some reporting entities already regularly receive SMR and related information from foreign-related entities but are unable to reciprocate the disclosure. The revised
exception to the tipping off offence is consistent with FATF Recommendation 18 by supporting information sharing within corporate groups for the purposes of mitigating and managing money laundering and terrorism financing risks.

112. One of the safeguards afforded by this provision is the requirement for a non-reporting entity of a corporate group to be subject to foreign laws that implement at least some or all of the FATF recommendations. This ensures that the body corporate is subject to a similar level of AML/CTF regulation as imposed in Australia and therefore can be treated akin to a reporting entity. This safeguard is consistent with Recommendation 18 of the FATF standards which requires financial institutions to ensure that their foreign branches and majority-owned subsidiaries apply AML/CTF measures consistent with their obligations.

113. A second safeguard afforded by this provision is to ensure that a body corporate, who is not a reporting entity, provide written undertakings to protect and control the use of the SMR and related information. These undertakings are consistent with the safeguard in existing subsection 132(1), which requires undertakings where AUSTRAC information is being disclosed to foreign counterparts. This safeguard is consistent with Recommendation 18 of the FATF standards which requires corporate groups to implement adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping off.

114. The requirement to obtain undertakings also aligns with the Privacy Act 1988 (Privacy Act). As all reporting entities under the Act are subject to the Privacy Act, the protections contained in the Privacy Act will also apply to the cross-border disclosure of SMR and related information. Australian Privacy Principle (APP) 8 and section 16C of the Privacy Act apply to cross-border disclosure of personal information, which would include SMR and related information. This generally requires an APP entity, such as a reporting entity, to ensure that an overseas recipient will handle an individual’s personal information in accordance with the APPs, and makes the APP entity accountable if the overseas recipient mishandles the information.

115. Item 26 inserts subsection 123(7AA) which provides that a reporting entity that has received information under subsection 123(7) must not disclose the information unless it is to another reporting entity within the same corporate group for the purpose of informing them about the risks involved in dealing with a particular customer. This safeguard restricts what a reporting entity within a corporate group can do with SMR and related information if it has been disclosed to them. This provision largely replicates existing subsection 123(7AA).

116. Item 26 inserts subsection 123(7AB) which expands the existing exception in subsection 123(7) to allow a reporting entity to share SMR and related information about a customer with another entity in its designated business group, within or outside of Australia. The conditions for the exception are identical to those imposed for the exception for sharing with members of a corporate group.

117. Item 26 inserts subsection 123(7AC) which provides that a reporting entity who has received information under subsection 123(7AB) must not disclose the information unless it is to another reporting entity within the designated business group for the purpose of informing them about the risks involved in dealing with a customer. This safeguard restricts what a reporting entity within a designated business group can do with SMR and related information if it has been disclosed to them. This provision largely replicates existing subsection 123(7AA).

118. As noted in item 20, each type of exception to the tipping off offence now has its own heading in the format ‘Exception—[type of exception]’. Consequently, item 26 also creates the heading ‘Exception—remittance sector’ immediately after subsection 123(7AC).

Item 27 – Subsection 123(7A)

119. Item 27 omits ‘Subsection (2)’ and substitutes ‘Subsection (1)’ in subsection 123(7A) to reflect the amendment related to the consolidation of old subsections 123(1) and (2).

Item 28 – Before subsection 123(8)
120. Item 28 inserts the heading ‘Exception—ADI’ before subsection 123(8) consistent with the clearer structure for the section.

**Item 29 – Subsection 123(8)**

121. Item 29 omits ‘Subsection (2)’ and substitutes ‘Subsection (1)’ in subsection 123(8) to reflect the amendment related to the consolidation of old subsections 123(1) and (2).

**Item 30 – Before subsection 123(9)**

122. Item 30 inserts the heading ‘Exception—compliance with the law or law enforcement’ before subsection 123(9) consistent with the clearer structure for the section.

**Item 31 – Subsection 123(9)**

123. Item 31 omits ‘Subsection (2)’ and substitutes ‘Subsection (1)’ in subsection 123(9) to reflect the amendment related to the consolidation of old subsections 123(1) and (2).

**Item 32 – Before subsection 123(10)**

124. Item 32 inserts the heading ‘Courts or tribunals’ before subsection 123(10). The purpose of this insertion is to improve readability.

**Item 33 – Subsection 123(10)**

125. Item 33 omits references to subsections (2) and (3) and substitutes only subsection (2) to reflect the repeal of 123(3).

**Item 34 – Paragraph 123(11)(a)**

126. Item 34 omits reference to subsection (3) in paragraph 123(11)(a) to reflect the repeal of 123(3).

**Item 35 – Paragraph 123(11)(a)**

127. Item 35 inserts reference to new subsection 123(5C) in paragraph 123(11)(a). The effect of this amendment is to make it a criminal offence for a person appointed or engaged by a reporting entity to audit or review an AML/CTF program to disclose SMR and related information to another person outside of this purpose. The penalty for a contravention is two years imprisonment and/or 120 penalty units.

**Item 36 – Paragraph 123(11)(a)**

128. Item 36 inserts reference to new subsection 123(7AC) in paragraph 123(11)(a). The effect of this amendment is to make it a criminal offence for a reporting entity in a designated business group to disclose SMR information unless it is to a reporting entity within that designated business group for the purpose of informing them about risks of a particular customer. The penalty for a contravention is two years imprisonment and/or 120 penalty units.

**Item 37 – Application provision**

129. Item 37 is an application provision that provides that the amendments made to section 123 apply in relation to the disclosure of information on or after the commencement of this item, regardless of whether the information was obtained before, on or after that commencement.

**Part 4 - Secrecy and Access**

*Anti-Money Laundering and Counter-Terrorism Financing Act 2006*

**Item 38 – Section 5 (definitions of ASD Minister, ASD official, ASIO Minister, ASIO official, ASIS Minister and ASIS official)**

130. Item 38 repeals the definitions of ‘ASD Minister’, ‘ASD official’, ‘ASIO Minister’, ‘ASIO official’, ‘ASIS Minister’, and ‘ASIS official’. These amendments are consequential to the repeal of existing section 128 and more broadly Division 4 of Part 11.
Existing Division 4 outlines an information sharing model that ‘designates’ relevant agencies to access and disclose AUSTRAC information. The ‘designated agency’ model relies on legislative amendment, or new regulations, in order for new agencies to be designated to gain access to AUSTRAC information, which can be a protracted process, depending on the availability of an appropriate legislative vehicle and parliamentary priorities. For example, following the application of the Australian Charities and Not-for-profits Commission (the national charity regulator with responsibilities relevant to terrorism financing) to become a designated agency, it took almost two years before access was granted following legislative amendment.

The current designated agency model also does not reflect modern collaborative and agile approaches to intelligence generation and investigations. For example, it does not adequately deal with multi-agency teams, taskforces or fusion centres, and the associated coordination and collaboration among agencies, some of which may or may not be designated under the AML/CTF Act. The current model also does not reflect the growing importance of collaboration with the private sector to combat money laundering and terrorism financing, which requires the sharing of information between government and industry.

Division 4 has been modernised to better reflect the needs of modern approaches to combating and disrupting money laundering and terrorism financing by replacing the designated agency model with a more general information sharing power. Provisions around the use of information have been simplified, whilst ensuring there are appropriate limits and safeguards on use and disclosure. The AUSTRAC CEO may now authorise specified officials of a wider range of Commonwealth, State or Territory agencies to access and disclose AUSTRAC information. This will provide greater flexibility and ensure timely access to AUSTRAC information for agencies with an operational need to use AUSTRAC information.

The Statutory Review Report concluded that Part 11 was overly complex, inconsistent, and lacked clarity, which impeded information sharing. Amendments have sought to reduce this complexity and uncertainty.

**Item 39 – Section 5 (definition of AUSTRAC entrusted person)**

Item 39 inserts the definition of ‘AUSTRAC entrusted person’ which includes the AUSTRAC CEO, an AUSTRAC staff member, a person engaged as a consultant under subsection 225(1), a person whose services are made available to the AUSTRAC CEO under subsection 225(3), the Director of AUSTRAC or a person engaged as a consultant under the now repealed section 40A of the Financial Transaction Reports Act 1988 (FTR Act). The latter captures consultants who the Director of AUSTRAC had engaged to perform services for the agency. The office of the Director of AUSTRAC was replaced by the AUSTRAC CEO with the enactment of the AML/CTF Act in 2006. The definition will also include members of taskforces that have been established by the AUSTRAC CEO in accordance with his or her functions. The definition replaces the existing definition of ‘entrusted public official’ in section 121 and replicates it in the definitions section (section 5) of the Act. A note under the definition explains that the former office of Director of AUSTRAC was established under the Financial Transaction Reports Act 1988.

**Item 40 – Section 5 (definition of AUSTRAC information)**

Item 40 repeals and replaces the definition of ‘AUSTRAC information’ which means information obtained by, or generated by, an AUSTRAC entrusted person under or for the purposes of this Act; information obtained by an AUSTRAC entrusted person under or for the purposes of any other law of the Commonwealth, State or Territory; information obtained by an AUSTRAC entrusted person from a government body; and FTR information (within the meaning of the FTR Act).

The Statutory Review Report noted that the existing definition of ‘AUSTRAC information’ is narrow in practice and does not anticipate all the ways in which information is collected or obtained by the AUSTRAC CEO. The current definition focuses on the source of information which creates the
potential for information to fall outside the scope of Part 11’s safeguards and protections if the information comes from a source not identified under the Act.

138. The definition has been amended to reflect the full range of information that may be in AUSTRAC’s possession and applies the necessary protections to that information under Part 11.

**Item 41 – Section 5 (definition of Commonwealth, State or Territory agency)**

139. Item 41 inserts the definition of ‘Commonwealth, State or Territory agency’ including those with functions relating to, or responsible for, law enforcement, criminal investigation, investigation of corruption, criminal intelligence, security intelligence, foreign intelligence, financial intelligence, or the protection of public revenue, or has regulatory or oversight functions. The definition also includes Commonwealth Departments, Commonwealth Royal Commissions that are established to inquire into unlawful conduct, and State and Territory Royal Commissions that are established to inquire into unlawful conduct or are specified in the AML/CTF Rules. The definition also includes any other Commonwealth, State or Territory agencies, authorities, bodies or organisations that are prescribed by the AML/CTF Rules, taskforces that have been established by a Minister of the Commonwealth, or of a State or Territory or under a law of the Commonwealth, or of a State or Territory, or a person who holds an office or appointment prescribed by the AML/CTF Rules. This definition is intended to facilitate the sharing of information within multiagency taskforces established for the purposes of disrupting money laundering, terrorism financing, and other serious crime.

140. Under the new section 125, specified officials of a Commonwealth, State or Territory agency may access AUSTRAC information for the purposes of performing their functions and duties and exercising their agency’s powers if authorised by the AUSTRAC CEO and provided certain written undertakings are given.

141. The definition of ‘Commonwealth, State or Territory agency’ will cover agencies that are currently designated under the Act to access and disclose AUSTRAC information, in addition to other agencies that have a function related to combating money laundering and terrorism financing or other serious crimes.

**Item 42 – Sections 5 (definitions of defence intelligence agency, designated agency, Director-General of Security and eligible collected information)**

142. Item 42 repeals the definition of ‘defence intelligence agency’ which previously meant the Australian Geospatial-Intelligence Organisation or the Defence Intelligence Organisation which form part of the Department of Defence. These agencies will be captured under the new definition of ‘Commonwealth law enforcement or intelligence agency’ in section 5.

143. Item 42 repeals the definition of ‘designated agency’ which is consequential to the repeal of Division 4 of Part 11.

144. Item 42 repeals the definition of ‘Director-General of Security’ as this term is now captured in the definition of ‘officials of Commonwealth, State or Territory agencies’ in new section 22.

145. Item 42 also repeals the definition of ‘eligible collected information’ which is consequential to the repeal of the definition of ‘AUSTRAC information’ in section 5.

**Item 43 – Section 5 (definitions of entrusted investigating official and foreign agency)**

146. Item 43 inserts the definition of ‘entrusted investigating official’ which means the Commissioner of the Australian Federal Police; Chief Executive Officer of the Australian Crime Commission; Commissioner of Taxation; Comptroller-General of Customs; Integrity Commissioner; or an investigating officer. This replicates the definition defined in existing section 122(1) and moves it to the definitions section of the Act.

147. Where a SMR, threshold transaction report, or international funds transfer instructions report has been communicated to the AUSTRAC CEO, an ‘entrusted investigating official’ can require a reporting entity or other person to provide further information or documents under section 49 of the
Act. The ‘entrusted investigating official’ is currently restricted from further disclosing this information unless an appropriate exception arises in section 122. The secrecy offence and relevant exceptions in section 122 have been repealed and are now replicated in new section 50A.

148. Item 43 also inserts the definition of ‘foreign agency’ into section 5 which means a government body that has responsibility for intelligence gathering for, or the security of a foreign country, a government body that has responsibility for law enforcement in a foreign country or a part of a foreign country; a government body that has responsibility for the protection of the public revenue of a foreign country; a government body that has regulatory functions in a foreign country; the European Police Office (Europol); the International Criminal Police Organization (Interpol); or an international body prescribed by the regulations for the purposes of this paragraph.

149. Foreign agency is used in new section 127 which regulates the offshore disclosure of AUSTRAC information. Currently, for example, the AFP and the Australian Criminal Intelligence Commission may only share AUSTRAC information directly with a foreign law enforcement agency under section 132. If either of those agencies wish to provide AUSTRAC information to a non-counterpart foreign agency, they must request AUSTRAC to provide that information. This process is inefficient and can be timely.

150. Relying on the new definition of ‘foreign agency’, AUSTRAC information may now be shared by those Australian agencies listed in new subsection 127(2) with agencies or bodies in a foreign country that are non-counterpart agencies, and may include agencies that have regulatory or revenue protection functions, in addition to those with law enforcement or intelligence/security functions. However, the foreign agency is first required to provide undertakings to safeguard the information (see new subsection 127(2)).

**Item 44 – Section 5 (definitions of foreign intelligence agency, foreign law enforcement agency, Human Services Department, Human Services Minister, IGIS, IGIS official and Immigration Department)**

151. Item 44 repeals the definitions of ‘Human Services Department’, ‘Human Services Minister’, and ‘Immigration Department’ because of the repeal of the definition of ‘designated agency’ in section 5.

152. Item 44 repeals the definitions of ‘foreign intelligence agency’ and ‘foreign law enforcement agency’ due to the consolidation of existing sections 132, 133, 133A, 133B, 133BA and 133C into the new section 127 dealing with the disclosure of AUSTRAC information to foreign countries and agencies.

153. Item 44 repeals the definition of ‘IGIS’ which will be captured under the new definition of ‘Commonwealth, State or Territory agency’ in section 5.

154. Item 44 repeals the definition of ‘IGIS official’ which will be captured under the new definition of ‘Officials of Commonwealth, State or Territory agencies’ in section 22.

**Item 45 – Section 5 (definition of Integrity Commissioner)**

155. Item 45 inserts the definition of ‘Integrity Commissioner’ which means the person appointed under section 175 of the Law Enforcement Integrity Commissioner Act 2006 as the Integrity Commissioner. This definition is relevant to the definition of ‘entrusted investigating official’.

**Item 46 – Section 5 (definitions of Inter-Governmental Committee and non-designated Commonwealth agency)**

156. Item 46 repeals the definition of ‘Inter-Governmental Committee’ which has been removed due to the streamlining and consolidation of section 128, and is now captured in the new section 126.

157. Item 46 repeals the definition of ‘non-designated Commonwealth agency’ because of the repeal of the definition of ‘designated agency’ in section 5.
Item 47 – Section 5 (definition of official)

158. Item 47 repeals and replaces the definition of ‘official’ because of the repeal of the definition of ‘designated agency’. Officials will be captured under the new definition of ‘Officials of Commonwealth, State or Territory agencies’ in section 22.

Item 48 – Section 5 (definition of Treasury Department)

159. Item 48 repeals the definition of ‘Treasury Department’ because of the repeal of the definition of ‘designated agency’ in section 5.

Item 49 – Section 22

160. Item 49 repeals and replaces section 22 – ‘Officials of Commonwealth, State or Territory agencies’. Subsection 22(1) has been amended because of the repeal of the definition of ‘designated agency’. The list of officials of a Commonwealth, State or Territory agency is largely consistent with the list of officials of a designated agency in existing section 22 and has been streamlined where appropriate.

161. For consistency, a note has been inserted under subsection 22(3) which is identical to that in existing subsection 22(3) to refer to subsection 33(3) of the Acts Interpretation Act 1901 for the purposes of revocation.

162. Subsection (4) has been inserted to make it clear that an authorisation made under subsection (3) is not a legislative instrument. The instrument is exempt from the operation of the Legislation Act 2003 as a result of item 4 of the Legislation (Exemptions and Other Matters) Regulation 2015, and as such the statement that it is not a legislative instrument is merely declaratory of the law.

Item 50 – After section 50

163. Item 50 inserts section 50A which reproduces the secrecy offence in existing section 122. The definition of entrusted investigating official is unchanged but has been included as a standalone definition in section 5 for simplification.

164. Section 50A has the same effect as existing section 122 but has been simplified to reduce complexity and improve readability. The secrecy offence has been moved to Division 6 of Part 3 of the Act so that the offence provision sits alongside section 49 under which requests for further information can be made. The secrecy offence is consistent with the Australian Law Reform Commission’s 2010 Secrecy Laws and Open Government in Australia report.

165. It is fitting to have a secrecy offence preventing unlawful disclosure of information obtained under section 49 given that inappropriate disclosure of such information could risk damage to ongoing and potential money laundering, terrorism financing, and other investigations. Disclosure could also allow individuals to take action to frustrate investigations, prosecutions and avoid asset confiscation.

166. Subsection 50A(1) makes it an offence for an entrusted investigating official, or former entrusted investigating official, to disclose information that has been obtained under section 49 or section 50A. The penalty for the offence against subsection 50A(1) is two years imprisonment and/or 120 penalty units.

167. The exceptions listed in subsection 50A(2) consolidate and capture the exceptions currently listed in subsection 122(3). Subsection 50A(2) provides that an entrusted investigating official can disclose information obtained under section 49 or section 50A:

- for the purposes of, or in connection with, the performance or exercise of the entrusted investigating official’s functions, duties or powers, or
- to another entrusted investigating official for the purposes of, or in connection with, the performance or exercise of their functions, duties or powers.

168. Subsection 50A(3) provides that a current or former entrusted investigating official is not required to, but may choose to, produce a document or information obtained under section 49 or section
50A to a court or tribunal unless it is necessary to do so for the purposes of giving effect to the Act or the FTR Act. This reflects the importance of protecting the confidentiality of such sensitive information and provides protection to those providing the information. Information obtained under section 49 or section 50A is primarily used for intelligence purposes and can be in a format that is inappropriate for use in court proceedings.

**Item 51 – Divisions 1 and 2 of Part 11**

169. Item 51 repeals and replaces Divisions 1 and 2 of Part 11. The repeal addresses the recommendation of the Statutory Review Report to simplify and streamline information sharing provisions under the Act.

170. The new Division 1 (section 120) sets out a simplified outline of the new Part 11.

171. The new Division 2 inserts a new section 121 which expands the secrecy offence in existing section 121 by not only prohibiting a person from obtaining and disclosing AUSTRAC information, but also prohibiting their unlawful access to, making a record of, authorising access to, or otherwise using AUSTRAC information. This addresses a gap in the existing framework which only prevents an AUSTRAC staff member from disclosing the information to another person. Strengthening the offence reflects the protection that should be accorded to AUSTRAC information given its often confidential and sensitive nature. The definition of ‘entrusted public official’ has been replaced by the definition of ‘AUSTRAC entrusted official’ and has the same effect. The definition has been moved to section 5 to streamline Part 11.

172. Subsection 121(1) makes it an offence for an AUSTRAC entrusted person, or former AUSTRAC entrusted person, to access, make a record of, authorise access to, disclose or otherwise use AUSTRAC information. The penalty for the offence against subsection 121(1) is two years imprisonment and/or 120 penalty units. The principles contained in the Australian Law Reform Commission’s 2010 *Secrecy Laws and Open Government in Australia* were taken into account when developing the secrecy offence.

173. The exceptions listed in subsection 121(2) consolidate and capture the exceptions currently listed in subsection 121(3). Subsection 121(2) provides an exception to the offence specified in subsection 121(1) if the disclosure is:

- for the purposes of the Act or of the FTR Act
- for the purposes of the performance of the functions of the AUSTRAC CEO
- for the purposes of, or in connection with, the performance or exercise of the person’s functions, duties or powers in relation to AUSTRAC
- in accordance with a provision of Part 11, or
- for the purposes of the *Law Enforcement Integrity Commissioner Act 2006*.

174. The new section 121 is intended to, among other things, more effectively facilitate information sharing with the private sector (including academia) which is integral to an effective AML/CTF regime.

175. For example, in March 2017, AUSTRAC established the Fintel Alliance. The Fintel Alliance is a private-public partnership for combating money laundering and terrorism financing. It brings together law enforcement, national security, regulatory and private sector partners to focus on detecting, preventing and disrupting financial crime on a global scale. The Fintel Alliance optimises the use of over 100 million reports from industry each year to produce financial intelligence to better target Australia’s money laundering and terrorism financing risks.

176. Members of the Fintel Alliance second officers to AUSTRAC under subsection 225(3). These officers are considered to be AUSTRAC entrusted persons for the purposes of Part 11. The new section 121 will facilitate the sharing of pertinent AUSTRAC information within the Fintel Alliance.

177. Subsection 121(3) provides that a person will not commit an offence against subsection 121(1) if they disclose AUSTRAC information to a Commonwealth, State or Territory official for the purposes
of, or in connection with, the performance or exercise of that official’s functions, duties or powers in relation to their agency. This provision recognises the important role that AUSTRAC staff members play under the Act to retain, compile, analyse and disseminate AUSTRAC information, and to share AUSTRAC information to support domestic efforts to combat money laundering, terrorism financing and other serious crimes.

178. Subsection 121(3) also provides that a person will not commit an offence against subsection 121(3) if they disclose AUSTRAC information to a Minister for the purposes of, or in connection with, the performance of the Minister’s responsibilities. This provision recognises the practical reality of dealing with AUSTRAC information where an AUSTRAC staff member may be required to disclose financial intelligence to either the Minister responsible for AUSTRAC, or another Minister who requires the information for the performance of their responsibilities where that information is relevant.

179. Subsection 121(4) provides that the AUSTRAC CEO can impose conditions on a person who receives AUSTRAC information from an AUSTRAC entrusted person under section 121, at the time that person receives the information, if the other person is not an AUSTRAC entrusted person, an official of a Commonwealth, State or Territory agency, or a Minister of the Commonwealth or of a State or Territory. This will allow AUSTRAC to better manage the on-disclosure of AUSTRAC information by third parties (e.g. academic research).

180. Subsection 121(5) provides that a person who is not an AUSTRAC entrusted person, an official of a Commonwealth, State or Territory agency, or a Minister of the Commonwealth or of a State or Territory, who has received AUSTRAC information under subsection 121(2) without conditions will commit an offence if they disclose the information to another person. The purpose of this provision is to restrict the disclosure of AUSTRAC information once it has left AUSTRAC. This is an important safeguard reflecting the sensitive nature of the information. The penalty for breaching this provision is two years imprisonment and/or 120 penalty units.

181. Subsection 121(6) provides that a person who is not an AUSTRAC entrusted person, an official of a Commonwealth, State or Territory agency, or a Minister of the Commonwealth or of a State or Territory, who has received AUSTRAC information under subsection 121(2) subject to conditions will commit an offence if they make a record of, disclose, or use the information in breach of those conditions. The purpose of this provision is to restrict the ability to record, disclose or use AUSTRAC information once it has left AUSTRAC, and to provide an avenue to enforce the CEO’s conditions. The penalty for breaching this provision is two years imprisonment and/or 120 penalty units.

182. Subsection 121(7) provides that an instrument detailing the AUSTRAC CEO’s conditions under subsection 121(4) is not a legislative instrument. The instrument is exempt from the operation of the Legislation Act 2003 as a result of item 5 of the Legislation (Exemptions and Other Matters) Regulation 2015, and as such the statement that it is not a legislative instrument is merely declaratory of the law.

**Item 52 – Division 3 of Part 11 (heading)**

183. Item 52 repeals the heading and inserts ‘Division 3- Protection of information given under Part 3’.

**Item 53 – Paragraph 124(2)(a)**

184. Item 53 inserts additional sections 121, 126, 128, 129, 161, 162 and 165 into paragraph 124(2)(a). The effect of the amendment is to allow section 41 and section 49 information described in subsection 124(1) to be admitted into evidence for the purposes of criminal proceedings in addition to criminal proceedings against section 123, 136 and 137:

- against a person who is, or has been, an AUSTRAC entrusted person, who accesses, records, authorises access to, discloses or otherwise uses AUSTRAC information
- against a person who is, or has been, an official of a Commonwealth, State or Territory agency who unlawfully makes a record of, discloses or otherwise uses AUSTRAC information
- against a person who unlawfully accesses AUSTRAC information
- against a person who makes a record of, discloses or otherwise uses AUSTRAC information disclosed to them in contravention of Part 11
- against a reporting entity who does not comply with a notice given by the AUSTRAC CEO to
  a. appoint an external auditor
  b. arrange for an external audit of the reporting entity’s
     i. capacity to identify, manage or mitigate the money laundering or terrorism financing risks it faces, or
     ii. compliance with AML/CTF regulation
  c. arrange for the external auditor to give the reporting entity a written report about an audit, or
  d. provide a written report from the external auditor to the AUSTRAC CEO
- against a reporting entity who does not comply with a notice given by the AUSTRAC CEO to carry out a money laundering or terrorism financing risk assessment, prepare a written report about the assessment, or give the AUSTRAC CEO a copy of the report.

185. Including additional criminal proceedings facilitates the disclosure of information about potentially criminal or terrorism-related activity to effectively prosecute persons who do not comply with obligations under the Act. Successful prosecution of offences under the Act deters unlawful conduct and promotes compliance with AML/CTF regulation which hardens the environment making it more difficult to launder money or finance terrorism. It also assists Australia in fulfilling its international obligations to combat money laundering and countering terrorism financing. Concerns about tipping off the subject of an SMR report are lower where the offence being prosecuted relates to failures on the part of the reporting entity that submits an SMR, or where an SMR has been unlawfully disclosed.

Item 54 – Paragraph 124(2)(b)

186. Item 54 repeals the existing paragraph and inserts criminal proceedings against section 29 or 30 of the FTR Act or proceedings under section 175 of the Act. The effect of the amendment is to allow section 41 and section 49 information described in subsection 124(1) to be admitted into evidence for the purposes of civil proceedings:

- providing false, misleading or incomplete information under sections 29 or 30 of the FTR Act, or
- for determining the amount of pecuniary penalty for a person that has breached a civil penalty provision in the Act.

187. Including additional civil proceedings under the FTR Act ensures that enforcement can be undertaken across the entire AML/CTF regime. Including all civil proceedings under section 175, and not just for existing 41(2) or 49(2), ensures equal importance is afforded to all civil penalty provisions across the Act. Concerns about tipping off the subject of an SMR report are lower where the offence being prosecuted relates to failures on the part of the reporting entity that submits an SMR, or where an SMR has been unlawfully disclosed.

Item 55 – Division 4 of Part 11

188. Item 55 repeals and replaces Division 4.

189. The Statutory Review Report noted that the information sharing framework in the Act is highly technical and prescriptive, with different requirements applying to different agencies. There is also a distinction between designated and non-designated agencies. This generates uncertainty about what use of information is permissible and which officials are permitted to receive AUSTRAC information.

190. This designated agency approach to authorising access to and regulating subsequent use of AUSTRAC information hampers the timely, effective and efficient sharing of AUSTRAC information for legitimate purposes. It also does not sit neatly with the multi-agency taskforce model through which
law enforcement, national security, intelligence and revenue protection agencies are increasingly collaborating to target serious and organised crime.

191. Moving away from the designated agency model is intended to address the recommendation of the Statutory Review Report to simplify and streamline information sharing provisions and provide greater flexibility and agility to better support contemporary and innovative approaches to combating money laundering and terrorism financing, and other serious crime.

192. These amendments will provide a general power for the AUSTRAC CEO to authorise access to AUSTRAC information to specified Commonwealth, State or Territory agencies, and specify, in a more generic way, how such agencies may deal with that information once accessed. Criminal penalties will apply for unlawful access, making a record of, use and disclosure as well as unlawful secondary disclosure.

**Division 4 – Access to AUSTRAC information by Commonwealth, State or Territory agencies**

193. The new section 125 provides a less prescriptive and more flexible model for information sharing amongst officials of Commonwealth, State or Territory agencies.

194. Subsection 125(1) provides that the AUSTRAC CEO can authorise specified officials of a specified Commonwealth, State or Territory agency to access specified AUSTRAC information for the purposes of performing the agency’s functions and duties and exercising the agency’s powers. The new section 125 removes the existing distinction between designated agencies and non-designated agencies under the Act and now treats their access to AUSTRAC information as the same.

195. The instrument of authorisation provided by the AUSTRAC CEO will specify officials within a particular agency that are responsible for a particular function, and specify the type of AUSTRAC information that can be accessed. This will restrict access to AUSTRAC information and provide an additional protection to privacy where appropriate. To the extent that subsection 125(1) will authorise the collection of sensitive information by agency officials, the collection is consistent with the Australian Privacy Principles (APPs) because the collection is authorised for the purposes of performing an agency’s functions and duties, and exercising their powers.

196. Subsection 125(2) provides that the AUSTRAC CEO can only provide an authorisation under subsection 125(1) if the head of a relevant State or Territory agency has given a written undertaking to the AUSTRAC CEO that the agency and its officials will comply with the APPs in respect of the information obtained under subsections 121(2), 121(3), section 125 or subsection 126(2).

197. Subsection 125(3) provides that an authorisation under this section is not a legislative instrument. The instrument is exempt from the operation of the Legislation Act 2003 as a result of item 4 of the Legislation (Exemptions and Other Matters) Regulation 2015, and as such the statement that it is not a legislative instrument is merely declaratory of the law.

198. Specific references to the Commissioner of Taxation in existing section 125 and the Treasury Department in existing section 126 have been removed consistent with a less prescriptive information sharing model. It is intended that both agencies will continue to have access to AUSTRAC information under the general access provision in section 125 for Commonwealth, State and Territory agencies.

199. The new section 126 significantly simplifies and consolidates existing sections 127 and 128.

200. The new subsection 126(1) provides an offence for a person that is, or has been, an official of a Commonwealth, State or Territory agency, who has obtained AUSTRAC information under subsection 121(2), 121(3), section 125 or subsection 126(2), and makes a record of, discloses or otherwise uses the information. The penalty for the offence against subsection 126(1) is two years imprisonment and/or 120 penalty units.

201. The offence in new subsection 126(1) is an extension of the offence in existing section 127 which prohibits unlawful disclosure of AUSTRAC information once it has been disclosed to, or accessed by, a current or previous official of a Commonwealth, State or Territory agency. The new
provision will also prohibit making a record of, or otherwise using, in addition to disclosure of AUSTRAC information. The principles contained in the Australian Law Reform Commission’s 2010 Secrecy Laws and Open Government in Australia were taken into account when developing the secrecy offence. The offence reflects the importance of protecting AUSTRAC information which can be highly personal and sensitive.

202. Subsection 126(2) provides exceptions to the offence in subsection 126(1) to allow records to be made of AUSTRAC information, and for the use or disclosure of that information for the purposes of, or in connection with, the performance or exercise of the person’s functions, duties or powers as an official of a Commonwealth, State or Territory agency.

203. A further exception is provided where the disclosure is to another official of a Commonwealth, State or Territory agency for the purposes of, or in connection with, the performance or exercise of that official’s functions, duties or powers in relation to their agency.

204. A third exception is where the disclosure is to a Minister for the purposes of, or in connection with, the performance of the Minister’s responsibilities.

205. The fourth exception provided by subsection 126(2) is that the disclosure of AUSTRAC information is in accordance with section 127. This ensures that particular government officials are able to disclose AUSTRAC information offshore.

206. The exceptions are designed to simplify, but retain the effect of, sections 127 and 128. Existing section 128, in particular, is overly prescriptive and complex, generating confusion. The focus on an official of a designated agency’s functions, duties or powers (e.g. for an investigation or for engaging the Minister) is continued under the new subsection 126(2).

207. The exceptions continue to restrict the disclosure of AUSTRAC information to legitimate objectives. They ensure that Commonwealth, State or Territory agencies can investigate matters and take enforcement action consistent with their functions. They also allow AUSTRAC’s main partner agencies to use AUSTRAC information in making administrative decisions. However it is important to note that section 124 will continue to operate. This prohibits the admission of SMR information described in subsection 124(1) as evidence into court or tribunal proceedings (unless an exemption in subsection 124(2) applies).

208. Subsection 126(3) provides that the offence in subsection 126(1) does not apply if the disclosure is for the purposes of court or tribunal proceedings, proposed or possible court or tribunal proceedings, or obtaining legal advice.

209. Subsection 126(4) provides that a person who has been disclosed AUSTRAC information under subsection 126(3) must not disclose the information to another person. The penalty for the offence against subsection 126(4) is two years imprisonment and/or 120 penalty units.

210. Subsection 126(5) provides that a person who has been disclosed AUSTRAC information under subsection 126(3) can further disclose that information for the purposes of the court or tribunal proceedings, proposed or possible court or tribunal proceedings, obtaining legal advice, or if it is authorised by Division 4 of Part 11.

Division 5 – Disclosure of AUSTRAC information to foreign countries or agencies

211. Subsection 127(1) provides that the AUSTRAC CEO may disclose AUSTRAC information to the government of a foreign country or a foreign agency, if the AUSTRAC CEO is satisfied that, where the CEO considers appropriate, undertakings have been provided by the foreign government or foreign agency to protect the confidentiality of the information, control its use, and ensure that it is only used for the purpose for which it is disclosed. The CEO must also be satisfied that it is appropriate in all of the circumstances to disclose the information.

212. This provision replicates existing section 132 and extends the ability of AUSTRAC to disclose AUSTRAC information to foreign agencies that are not its direct counterpart. Extended disclosure is
necessary to reflect AUSTRAC’s role as Australia’s financial intelligence unit, and AML/CTF regulator, and subsequently the variety of foreign agencies that AUSTRAC collaborates and cooperates with in the global effort to combat money laundering and terrorism financing.

213. Unlike existing section 132, the CEO can also exercise discretion as to when undertakings are required from the government of a foreign country or a foreign agency which will allow for effective disclosure of less sensitive AUSTRAC information in international forums attended by AUSTRAC and international presentations/workshops given by AUSTRAC, for example, during capacity building exercises for regional partners.

214. Subsection 127(2) provides that the head of a Commonwealth, State or Territory agency referred to in subsection 127(3), or a person covered under an authorisation in subsection 127(4), may disclose AUSTRAC information to the government of a foreign country or a foreign agency if the person is satisfied undertakings have been provided by the foreign government or foreign agency to protect the confidentiality of the information, control its use, and ensure that it is only used for the purpose for which it is disclosed. The person must also be satisfied that it is appropriate in all of the circumstances to disclose the information. These safeguards reflect those in existing sections 132, 133, 133A, 133B, 133BA and 133C, and are essential to protecting sensitive information disseminated outside of Australia.

215. This provision consolidates existing section 132, and sections 133-133C and extends the ability of government agencies to disclose AUSTRAC information to foreign governments and foreign agencies that are not the direct counterparts of an agency. This amendment is intended to address the recommendation of the Statutory Review Report to simplify and streamline information sharing provisions to better support contemporary and innovative approaches to combating money laundering and terrorism financing, and other serious crime.

216. Extending the ability of Australian agencies to disclose AUSTRAC information to foreign agencies addresses a practical problem that currently exists where domestic agencies are working on overseas taskforces that consist of agencies other than their direct foreign counterparts. It also reflects the modern reality of international cooperation.

217. Unlike new subsection 127(1), the person under subsection 127(2) does not have discretion as to when undertakings are required and must obtain undertakings in all cases of offshore disclosure. Given AUSTRAC’s role as financial intelligence unit and AML/CTF regulator, it is the only appropriate agency to determine when AUSTRAC information is less sensitive and thus could be shared without undertakings.

218. Subsection 127(3) lists the Commonwealth, State or Territory agencies that are able to disclose AUSTRAC information offshore. The list of agencies adds to those currently listed in sections 132-133C of the Act to reflect the international role that these agencies play in fighting global issues, such as tax evasion, securities fraud and drug trafficking.

219. Subsection 127(4) provides that the head of a Commonwealth, State or Territory agency listed in subsection 127(3) can authorise in writing an official of that agency to make offshore disclosures in accordance with subsection 127(1). This reflects operational practice and removes ambiguity in the existing Part 11 where it is unclear whether the official (or the head) needs to be satisfied of the appropriate undertakings given by the foreign agency.

220. Subsection 127(5) provides that an authorisation under subsection 127(4) is not a legislative instrument. The instrument is exempt from the operation of the Legislation Act 2003 as a result of item 4 of the Legislation (Exemptions and Other Matters) Regulation 2015, and as such the statement that it is not a legislative instrument is merely declaratory of the law.

**Division 6 – Unauthorised accessing of or use or disclosure of AUSTRAC information**

221. Section 128 provides that it is an offence for a person to unlawfully access AUSTRAC information. The penalty for breaching this provision is imprisonment for two years and/or 120 penalty
units. The addition of this offence is intended to strengthen the secrecy and access framework and protect the confidentiality of financial intelligence.

222. Subsection 129(1) provides that it is an offence for a person who is disclosed AUSTRAC information in contravention of Part 11 to make a record of, disclose, or otherwise use the information. The penalty for the offence is two years imprisonment and/or 120 penalty units.

223. The addition of this offence closes a gap identified in the Statutory Review Report whereby a person who unlawfully receives AUSTRAC information, and then subsequently discloses the information is not covered. It is insufficient to rely on the general secrecy offences specified in the Criminal Code Act 1995 (Criminal Code), in particular section 122.4A. Section 129 is required in order to capture persons outside of this offence that only applies to current and former Commonwealth officers or other persons engaged to perform work for a Commonwealth entity. For example, a number of State and Territory agencies and their officers will be able to obtain, and therefore use and disclose, AUSTRAC information under Part 11.

224. Subsection 129(2) provides an exception to the offence in subsection 129(1) if the person discloses the information for the purposes of investigating the initial disclosure that was not in accordance with Part 11 (paragraph 129(1)(c)). It is pertinent to note that, under sections 9.3 and 9.4 of the Criminal Code, a person cannot escape liability under section 128 or 129 where they were mistaken about, or ignorant of, the existence or content of the law.

Item 56 – Division 5 of Part 11 (heading)

225. Item 56 repeals the heading and substitutes Division 7—Use of AUSTRAC information in court or tribunal proceedings.

Item 57 – Section 134

226. Item 57 repeals section 134 and substitutes a simplified provision that prohibits a person from being required to produce a document containing AUSTRAC information or to disclose AUSTRAC information to a court or tribunal unless it is necessary to do so for the purposes of giving effect to the Act or the FTR Act. This reflects the importance of protecting the confidentiality of such sensitive information and provides protection to those providing the information. AUSTRAC information is used for intelligence purposes and can be in a format that is inappropriate for use in court proceedings.

Item 58 – Subsection 190(4)

227. Item 58 removes a reference to ‘section 126’ in subsection 190(4) and substitutes ‘section 125’ to reflect the new provisions in Division 4 of Part 11. Section 190 deals with the monitoring of compliance with the Act and allows the AUSTRAC CEO to provide a report about a breach of the Act to a government body if certain conditions are met. The effect of the amendment is to not limit the power of the AUSTRAC CEO to provide access to AUSTRAC information under section 125.

Item 59 – Section 208

228. Item 59 removes a reference to ‘eligible collected information’ in section 208 and substitutes ‘AUSTRAC information’ to reflect the new definition in section 5. Section 208 is a simplified outline of Part 16 of the Act dealing with administrative matters such as the establishment of AUSTRAC.

Item 60 – Paragraph 212(1)(a)

229. Item 60 removes a reference to ‘eligible collected information or’ in paragraph 212(1)(a) to reflect the new definition of AUSTRAC information in section 5. The new amendment will specify that a function of the AUSTRAC CEO is to retain, compile, analyse and disseminate AUSTRAC information.

Item 61 – Paragraph 212(1)(b)

230. Item 61 removes a reference to ‘entitled or’ in paragraph 212(1)(b). The reference is considered redundant given the Australian Tax Office (ATO) is no longer ‘entitled’ to access AUSTRAC
information under existing section 125, and under the new information sharing framework, the ATO will be authorised to access AUSTRA
C information under new section 126. The new amendment will specify that a function of the AUSTRA
C CEO is to provide advice and assistance to the persons authorised to access AUSTRA
C information under Part 11.

**Item 62 – After paragraph 212(1)(da)**

231. Item 62 inserts a new function of the AUSTRA
C CEO in subsection 212(1). The function is to establish
such taskforces as the AUSTRA
C CEO considers appropriate. This new function recognises the establishment of the Fintel Alliance, and more importantly is linked to the definition of ‘AUSTRA
C entrusted person’. This ensures that persons seconded to taskforces, such as the Fintel Alliance, under the AML/CTF Act have clear authority to use and disclose AUSTRA
C information in accordance with Part 11.

**Item 63 – After paragraph 212(1)(e)**

232. Item 63 inserts a new function of the AUSTRA
C CEO in subsection 212(1). The function is to assist in the development of government policy or academic research. This will provide the AUSTRA
C CEO with the necessary flexibility to share AUSTRA
C information for these purposes.

**Inspector-General of Intelligence and Security Act 1986**

**Item 64 – Section 25A (note)**

233. Item 64 removes a reference to ‘section 128’ in the note to section 25A of the Inspector-General of Intelligence and Security Act 1986 and substitutes ‘Part 11’ to reflect the new information sharing provisions. The new amendment notes that notwithstanding the power in section 25A for the Inspector-General to provide an inspection report to a relevant Minister, the Inspector-General can only disclose AUSTRA
C information in accordance with Part 11

**Item 65– Application and transitional provisions**

234. Item 65 provides for the application and transitional provisions for the amendments to the Part 11 framework.

235. Section 50A will apply in relation to the making of a record of, the disclosure of or the use of information on or after the commencement of this item (whether the information was obtained before, on or after that commencement).

236. For the purposes of the operation of section 50A, information obtained under subsection 122(3) of the Act before the commencement of this item is taken on and after that commencement to be information obtained under section 50A of the Act.

237. The new section 121 will apply in relation to the accessing of, the making of a record of, the authorising of access to, the disclosure of or the use of information on or after the commencement of this item (whether the information came into existence before, on or after that commencement).

238. The amendments to section 124 apply in relation to proceedings instituted on or after the commencement of this item.

239. If immediately before the commencement of this item, an authorisation is in force under existing subsection 126(1) in relation to a designated agency, and on the commencement of this item, the agency is a Commonwealth, State or Territory agency (within the meaning of section 5 of the AML/CTF Act), then the authorisation has effect on and after the commencement of this item as if it were an authorisation in force under the new subsection 125(1). This does not prevent the variation or revocation of the authorisation on or after the commencement of this item.

240. New section 126 will apply in relation to the making of a record of, the disclosure of or the use of information on or after the commencement of this item (whether the information came into existence before, on or after that commencement).
241. For the purposes of the operation of the new section 126, accessed information (within the meaning of existing subsection 127(4)) obtained by a person before the commencement of this item is taken on and after that commencement to be AUSTRAC information obtained under new section 126.

242. If, at any time before the commencement of this item, a person was covered by existing subsection 127(1), then the person is taken to be a person who is or has been an official of a Commonwealth, State or Territory agency for the purposes of new section 126.

243. New section 127 will apply in relation to AUSTRAC information that came into existence before, on or after the commencement of this item.

244. New section 128 will apply in relation to the accessing of information on or after the commencement of this item.

245. New paragraph 129(1)(a) will apply in relation to a disclosure of information on or after the commencement of this item.

Item 66 – Saving provisions

246. Item 66 provides for the saving provisions for the Part 11 framework.

247. Existing sections 121, 122 and 127 continue to apply on and after the commencement of this item in relation to a disclosure of information before that commencement.

248. Existing subsections 128(5) to (7) continue to apply on and after the commencement of this item in relation to a disclosure of information before that commencement under existing paragraph 128(3)(a).

249. Existing subsections 128(10) to (12) continue to apply on and after the commencement of this item in relation to a disclosure of information before that commencement under existing subsection 128(8).

250. Existing section 130 continues to apply on and after the commencement of this item in relation to information obtained under existing subsection 129(1) or 131(2).

251. Existing subsections 131(4) to (6) continue to apply on and after the commencement of this item in relation to a disclosure of information before that commencement under existing subsection 131(3).

Part 5 – Reports about Cross-Border Movements of Monetary Instruments

Anti-Money Laundering and Counter-Terrorism Financing Act 2006

Item 67 – Section 4

252. Item 67 deletes the reference to ‘physical currency’ and substitutes ‘monetary instruments’ in the simplified outline of the Act. The simplified outline will read ‘Cross-border movements of monetary instruments must be reported to the AUSTRAC CEO, a customs officer or a police officer if the total amount moved is above a threshold’.

253. The introduction of cross-border reporting requirement for monetary instruments will consolidate existing reporting requirements for physical currency and bearer negotiable instruments (BNIs) and ensure they are consistent. This will address a recommendation of the Statutory Review Report to simplify and consolidate the reporting framework and align Australia with a number of key foreign counterparts that require mandatory reporting of BNIs above a certain threshold, including the United States and Canada.

Item 68 – Section 4

254. Item 68 deletes the part of the simplified outline of the Act in relation to the cross-border movements of BNIs. A person will now be required to report a BNI above a certain threshold. Currently, a police or customs officer can require a person to declare a BNI of any value.
Item 69 – Section 5 (definitions of monetary instrument, monetary instrument amount and move)

255. Item 69 inserts the definition of ‘monetary instrument’, which means physical currency, a BNI or a thing prescribed by the AML/CTF Rules. Physical currency refers to Australian or foreign currency. Section 17 of the Act defines a BNI as including instruments such as a cheque or a promissory note. The third part of the definition of ‘monetary instrument’ allows a thing to be prescribed by the AML/CTF Rules. This provides flexibility to accommodate emerging threats and the necessary technology to value items such as precious metals and stones, bullion or stored value cards. In future these items could be included as part of the definition of monetary instrument without the need for legislative amendments to the Act.

256. Item 69 inserts the definition of ‘monetary instrument amount’ which means for physical currency - the amount of that currency, for a BNI - the amount payable under the instrument, or for a thing prescribed by the AML/CTF Rules - the amount worked out in accordance with the Rules. The concept of monetary instrument amount is relevant when calculating the combined value of one or more monetary instruments in order to establish if the threshold for reporting has been met.

257. Item 69 inserts the definition of ‘move’ which refers to proposed sections 55 and 56 that define movements of monetary instruments into or out of Australia.

Item 70 – Section 5 (definitions of move physical currency into Australia and move physical currency out of Australia)

258. Item 70 repeals the definitions of ‘move physical currency into Australia’ and ‘move physical currency out of Australia’. The new definition of ‘move’ will replace these definitions.

Item 71 – Section 5 (definition of non-reportable cross-border movement of monetary instruments)

259. Item 71 inserts the definition of ‘non-reportable cross-border movement of monetary instruments’, which means a movement of one or more monetary instruments into or out of Australia for which a report under section 53 is not required. In practice, this means where there is the movement of one or more monetary instruments into or out of Australia with a combined value of less than $10,000. The definition is relevant in the context of the amended ‘structuring’ offence established in new section 143. The structuring offences involves conducting, or causing to conduct, movements of monetary instruments under the AUD$10,000 threshold to avoid triggering the reporting requirement.

Item 72 – Section 5 (definition of non-reportable cross-border movement of physical currency)

260. Item 72 repeals the definition of ‘non-reportable cross-border movement of physical currency’. Following the consolidation of reporting requirements for physical currency and BNIs, this definition will be incorporated into the new definition of ‘non-reportable cross-border movement of monetary instruments.’

Item 73 – Section 5 (definition of send)

261. Item 73 amends the definition of ‘send’ to refer to ‘monetary instrument’ rather than ‘physical currency’ following the consolidation of reporting requirements for physical currency and BNIs.

Item 74 – Part 4 (heading)

262. Item 74 repeals the heading for Part 4 and inserts ‘Part 4 – Reports about cross-border movements of monetary instruments’.

263. Part 4 of the Act implements FATF Recommendation 32 that deals with cash couriers and requires countries to have measures in place to detect the physical cross-border transportation of currency and BNIs.

264. The Interpretative Note to Recommendation 32 provides that countries can meet their obligations by implementing a declaration system requiring all persons making a physical cross-border transportation of currency or BNIs, which are of a value exceeding a threshold, to make a truthful declaration to competent authorities. Part 4 provides for Australia’s cross-border declaration system.
**Item 75 – Divisions 1 to 3 of Part 4**

265. Item 75 repeals Divisions 1, 2 and 3 of Part 4.

266. The primary effect of repealing Divisions 1, 2 and 3 is to consolidate and merge the cross-border reporting requirement for physical currency and BNIs. This will provide for a streamlined and simplified cross-border reporting framework.

267. Currently, a person only declares a BNI when required to do so by a customs or police officer. There is no general mandatory requirement to report a BNI. Imposing the same reporting requirements for BNIs as for physical currency recognises the risk that criminals can move BNI across borders to launder funds, pay for illicit goods, and complicate asset recovery. In particular, BNIs are an alternative method to cash for laundering money given they are less bulky and easier to conceal. Consolidating the reporting requirement strengthens Australia’s cross-border reporting framework and aligns it with comparable jurisdictions such as the United States, United Kingdom, and Canada.

268. The repeal of Division 2 will not replace existing section 54. Section 54 currently outlines the applicable timing rule for movements of physical currency into and out of Australia. In accordance with the overall simplification and clarification of the cross-border reporting framework, the AML/CTF Rules will now explain the applicable timing rule for movements of monetary instruments into and out of Australia. This will also align Australia with other international cross-border reporting frameworks such as New Zealand and Singapore.

269. Item 75 inserts a new Division 1, which is the simplified outline of Part 4.

270. Section 52 provides the simplified outline of Part 4 and states that cross-border movements of monetary instruments must be reported to the AUSTRAC CEO, a customs officer or a police officer, if the total value moved is AUD$10,000 or more.

271. Item 75 inserts a new Division 2, which deals with reports about monetary instruments.

272. Section 53 deals with reporting requirements for movements of monetary instruments into or out of Australia, which is the fundamental provision in Part 4. Section 53 largely replicates the existing offence in the Act for physical currency and applies it to monetary instruments.

273. Subsection 53(1) provides that it is an offence if a person does not make a report under section 53 and moves one or more monetary instruments into or out of Australia, the sum of which are equal to or more than AUD$10,000. The penalty for an offence against subsection 53(1) is two years imprisonment and/or 500 penalty units. Pursuant to sections 9.3 and 9.4 of the Criminal Code, a person cannot escape liability for this offence by arguing that they were mistaken about, or ignorant of, the existence or content of their reporting obligations under the AML/CTF Act and AML/CTF Rules.

274. For example, if a person did not make a report in the following circumstances, they would breach subsection 53(1):

- departing Australia on an aircraft with $10,000 of Australian currency
- arriving in Australia on a ship with AUD$10,000 worth of foreign currency
- departing Australia on a ship with a combined AUD$10,000 payable under two BNIs
- arriving in Australia on an aircraft with $5,000 of Australian currency and AUD$5,000 of foreign currency
- sending out of Australia via the post $5,000 of Australian currency and AUD$5,000 payable under a BNI, or
- sending into Australia AUD$5,000 of foreign currency and AUD$5,000 payable under one BNI.

275. The FATF recommends a maximum threshold of USD/EUR15,000 to trigger a reporting requirement for physical currency or BNIs. The proposed reporting requirement threshold for monetary instruments would ensure that Australia is compliant with Recommendation 32.
276. Subsection 53(2) provides that it is a civil penalty for a person who moves one or more monetary instruments into or out of Australia, the sum of which is equal to or more than AUD$10,000, and does not make the required report.

277. Subsection 53(3) provides that subsection 53(2) is a civil penalty provision.

278. Subsection 53(4) provides an exemption for commercial passenger carriers to report under section 53 when monetary instruments are in the possession of any of the carrier’s passengers. A commercial passenger carrier means a person who, in the normal course of a business, carries passengers for reward (for example, commercial airlines such as QANTAS). The onus should be on the individual carrying the monetary instruments to make a report if the sum of the monetary instruments is equal to or more than AUD$10,000. This subsection replicates the existing exemption in subsection 53(5).

279. Subsection 53(5) provides an exemption for commercial goods carriers to report under section 53 when monetary instruments are carried on behalf of another person. A commercial goods carrier means a person who, in the normal course of a business, carries goods or mail for reward (for example, FedEx).

280. This subsection largely replicates the existing exemption in subsection 53(6) but removes the element where the sender has not disclosed to the carrier that the goods include a monetary instrument (previously physical currency). This ensures the exemption is consistent for both commercial passenger carriers and commercial goods carriers. The onus should be on the individual sending, and the individual receiving, the monetary instruments to make a report under section 53 and 54 respectively, if the sum of the monetary instruments is equal to or more than AUD$10,000.

281. Subsection 53(6) provides that a commercial passenger carrier or commercial goods carrier relying on subsections 53(4) or (5) bear an evidential burden in the matter.

282. Subsection 53(7) provides that a report under section 53 must be in the approved form, contain such information as is specified in the AML/CTF Rules, be given to the AUSTRAC CEO, a customs officer or a police officer, and comply with the applicable timing rule in the AML/CTF Rules.

283. Section 54 deals with reporting requirements for a person who receives monetary instruments that have been sent into Australia. The intention of the provision is to identify monetary instruments that are sent into Australia, in particular through the post. The requirement to report upon receipt ensures that there are no gaps in the cross-border reporting framework so that all relevant financial intelligence is collected to identify and disrupt money laundering, terrorism financing and other serious crimes.

284. Section 54 largely replicates the existing offence in section 55 for physical currency and applies it to monetary instruments. Existing paragraph 55(1)(c) has been removed on the basis that it is unreasonable to expect a person to always know whether the sender of a monetary instrument has or has not made a report under section 53. Given it is also difficult to enforce the requirement to report on a sender who is outside Australia, ensuring that the recipient in Australia makes a report under section 55 ensures the collection of relevant financial intelligence. The removal of paragraph 55(1)(c) ensures the offence provision is consistent with other international cross-border reporting frameworks including New Zealand and Singapore.

285. Subsection 54(1) provides that it is an offence if a person does not make a report under section 54 and receives one or more monetary instruments, the sum of which is equal to or more than AUD$10,000. The penalty for an offence against subsection 54(1) is two years imprisonment and/or 500 penalty units. Pursuant to sections 9.3 and 9.4 of the Criminal Code, a person cannot escape liability for this offence by arguing that they were mistaken about, or ignorant of, the existence or content of their reporting obligations under the AML/CTF Act and AML/CTF Rules.
286. Subsection 54(2) provides that it is a civil penalty for a person who does not make a report and receives one or more monetary instruments sent into Australia, the sum of which is equal to or more than AUD$10,000.

287. Subsection 54(3) provides that subsection 54(2) is a civil penalty provision.

288. Subsection 54(4) provides that a report under section 54 must be in the approved form, contain such information as is specified in the AML/CTF Rules, and be given to the AUSTRAC CEO, a customs officer or a police officer within five business days from the day that the monetary instruments were received.

289. Section 55 provides that a person moves a monetary instrument into Australia if that person brings or sends the monetary instrument into Australia. This section replicates existing section 58 and applies it to monetary instruments. Existing section 58 and new section 55, appear earlier in Part 4 for clarity.

290. Subsection 56(1) provides that a person moves a monetary instrument out of Australia if the person takes or sends the monetary instrument out of Australia. This subsection consolidates existing subsections 57(1) and 57(2) for simplification and applies it to monetary instruments. Existing section 57 and new section 56 appear earlier in Part 4 for clarity.

291. Subsection 56(2) provides that a person is taken to have moved a monetary instrument out of Australia if he or she arranges to leave Australia on an aircraft or ship, and either has a monetary instrument in his or her baggage and enters, or takes the monetary instrument to, the place at which customs officers examine passports.

292. This subsection is based on existing subsection 56(3), but instead of referring to an embarkation area, ‘the place at which customs officers examine passports’ has been used to identify the final physical point in an airport or port by which a person is expected to have reported. After this point, if a person has AUD$10,000 or more of monetary instruments on their person (for example in a backpack or in his or her pocket), or in their checked-in baggage, they would be liable to the offence provision in section 53 if no report had been made.

293. Section 57 provides that where a customs officer or a police officer receives a report under either section 53 or 54, the officer must forward the report to the AUSTRAC CEO within five business days beginning on the day of receipt of the report. Section 57 replicates existing section 56 and moves it to the end of the Division for clarity.

**Item 76 – Section 143 (heading)**

294. Item 76 repeals the heading for section 143 and substitutes ‘Conducting transfers to avoid reporting requirements relating to cross-border movements of monetary instruments’.

**Item 77 – Paragraph 143(1)(a)**

295. Item 77 provides that it is an offence for a person to structure movements of monetary instruments into or out of Australia to avoid the reporting requirements in Part 4. The offence is based on the existing offence in section 143 of the Act for physical currency and applies it to monetary instruments.

296. Paragraph 143(1)(a) provides the first element of the offence, which is that 2 or more non-reportable cross-border movements of monetary instruments are conducted, and each movement was either conducted, or was caused to be conducted, by a person.

297. The offence will expand the existing offence in section 143 to ensure that it captures the circumstance where a person instructs one or more persons to conduct non-reportable cross-border movements. It also captures the circumstance where a person conducts the movement themselves and instructs one or more other persons to conduct non-reportable cross-border movements. The broadened offence strengthens the cross-border reporting framework to ensure that relevant financial intelligence is gathered to identify and disrupt money laundering and terrorism financing.
298. The offence is intended to capture circumstances such as where a person:

- carries AUD$5,000 of monetary instruments into Australia on two different occasions
- carries AUD$9,000 of monetary instruments, and causes another person to carry AUD$1,000 worth of monetary instruments, into Australia
- carries AUD$9,000 of monetary instruments, and causes two other persons to each carry AUD$1,000 worth of monetary instruments, out of Australia, or
- cause two other persons to each carry AUD$5,000 each worth of monetary instruments into Australia.

Item 78 – Paragraph 143(1)(b)

299. Item 78 deletes ‘physical currency’ from the offence provision in section 143 and substitutes ‘monetary instrument’ following the consolidation of reporting requirements for physical currency and BNIs.

Item 79– Subsection 143(2)

300. Item 79 deletes ‘defendant’ from subsection 143(2) and substitutes ‘first person’. This is a minor editorial amendment to reflect that the defendant and the first person are the same.

Item 80 – Subsection 143(2)

301. Item 80 deletes ‘physical currency’ from the offence provision in section 143 and substitutes ‘monetary instrument’ following the consolidation of reporting requirements for physical currency and BNIs.

Item 81 – Paragraphs 143(3)(a) and (b)

302. Item 81 repeals paragraphs 143(3)(a) and (b) and substitutes references to monetary instrument. This amendment will ensure that consideration is given to the sum of the monetary instrument amounts for each movement, and the total of the amounts of all movements, when determining whether subsection 143(1) has been breached.

Items 82 and 83 – Section 173

303. Items 82 and 83 amend the simplified outline for Part 15 replacing references to ‘physical currency and BNI with ‘monetary instruments’. Part 15 of the Act deals with enforcement including issuing infringement notices for unreported cross-border movements and the powers of customs and police officers to question, search and arrest persons in connection with cross-border movements.

Item 84 – Paragraphs 184(1A)(a) and (b)

304. Item 84 repeals paragraphs 184(1A)(a) and (b) and instead substitutes new paragraph (a) to reflect that an infringement notice provision under the Act includes new subsection 53(2) to deal with reports about movements of monetary instruments rather than physical currency.

305. Item 84 repeals paragraph 184(1A)(b) to reflect that an infringement notice provision under the Act no longer includes subsection 59(4) dealing with BNIs. BNIs are captured in the new paragraph 184(1A)(a).

Item 85 – At the end of subsection 185(1)

306. Item 85 inserts a note at the end of subsection 185(1), which refers the reader to sections 186A and 186B to determine the infringement notice penalty.

Item 86 – Section 186

307. Item 86 repeals section 186 to reflect that the amount of penalties for infringement notices under Part 4 are included in the amended section 186A.

Item 87 – Section 186A (heading)
Item 87 repeals the heading for section 186A and inserts ‘Amount of penalty—breaches of certain provisions of Part 3A, 4, 6 or 6A’. Part 4 has been added to the existing section 186A to apply the standard infringement notice penalties in the Act to breaches of cross-border reporting requirements. This addresses a recommendation of the Statutory Review Report to increase the civil penalties available for failing to comply with cross-border reporting requirements. This will also better align Australia’s penalties with international counterparts and the FATF standards.

**Item 88 – Subsection 186A(1)**

The effect of this amendment is to specify that the penalty for an infringement notice to a body corporate for a breach of the cross-border reporting requirement is 60 penalty units, or the number of penalty units specified in the Rules for an alleged contravention of a kind specified in the AML/CTF Rules. The previous penalty was 5 penalty units for an alleged contravention where the total amount of physical currency or BNI was $20,000 or more, or otherwise 2 penalty units.

310. The infringement notice provisions in existing subsection 186A(1) are replicated. However, in order to streamline and simplify the provision, references to Part 6 infringement notice provision, Part 6A infringement notice provision and Part 3A infringement notice provision and related subsections have been removed given the definitions are not used elsewhere in the Act.

**Item 89 – Subsection 186A(2)**

The penalty for an infringement notice issued to a person other than a body corporate for a breach of the cross-border reporting requirement will be 12 penalty units, or the number of penalty units specified in the Rules for an alleged contravention of a kind specified in the AML/CTF Rules. The previous penalty was 5 penalty units for an alleged contravention where the total amount of physical currency or BNI was $20,000 or more, or otherwise 2 penalty units.

312. The infringement notice provisions in existing subsection 186A(2) are replicated. However to streamline and simplify the provision, references to ‘Part 6 infringement notice provision’, ‘Part 6A infringement notice provision’ and ‘Part 3A infringement notice provision’ have been removed given the definitions are not used elsewhere in the Act.

**Item 90 – Paragraph 186A(3)(a)**

313. Item 90 amends the existing paragraph 186A(3)(a) to provide simplified drafting.

**Item 91 – Paragraph 186(3)(b)**

314. Item 91 amends the existing paragraph 186A(3)(b) to provide simplified drafting.

**Item 92 – Paragraphs 186A(4)(a) and (b)**

315. Item 92 repeals and substitutes new paragraphs 186A(4)(a) and (b) to provide simplified drafting.

**Item 93 – Subparagraphs 189(b)(i) and (c)(i)**

316. Item 93 amends section 189 to remove references to subsection 59(3), to reflect that the latter was repealed as part of the consolidation of the cross-border reporting requirement for physical currency and BNIs.

**Item 94 – Division 8 of Part 15 (heading)**

317. Item 94 repeals the heading for Division 8 of Part 15 and inserts ‘Powers of questioning, search and arrest in relation to cross-border movements of monetary instruments’. This amendment reflects the consolidation of the cross-border reporting requirement for physical currency and BNIs.

**Item 95 – Section 199 (heading)**
318. Item 95 repeals the heading for section 199 and inserts ‘Questioning and search powers in relation to monetary instruments’. The existing questioning and search powers in relation to physical currency will be extended to BNIs following the consolidation of the cross-border reporting requirement.

**Items 96, 97 and 98 – Paragraph 199(1)(c), 199(1)(d), 199(1)(e) and 199(1)(f)**

319. Items 96, 97 and 98 amend subsection 199(1) so that the questioning and search powers for a police officer or customs officers, in relation to a person leaving Australia, apply to a person carrying monetary instruments rather than physical currency. A police officer or customs officer can require a person to declare whether they are carrying a monetary instrument, the sum of monetary instruments being carried, whether or not a report under section 53 has been given, and to produce the monetary instrument to the officer. These powers are essential to promote compliance, and detect non-compliance, with the reporting requirements in Part 4.

**Items 99, 100 and 101 – Paragraph 199(2)(a), 199(2)(b), 199(2)(c) and 199(2)(d)**

320. Items 99, 100 and 101 amend subsection 199(2) so that the questioning and search powers for a police or customs officer, in relation to a person arriving in Australia, apply to a person carrying monetary instruments rather than physical currency. A police officer or customs officer can require a person to declare whether they are carrying monetary instruments, the sum of monetary instruments being carried, whether or not a report under section 53 has been given, and to produce the monetary instrument to the officer. These powers are essential to promote compliance, and detect non-compliance, with the reporting requirements in Part 4.

**Item 102 – After subsection 199(2)**

321. Item 102 inserts subsection 199(2AA). This provides that where a person produces a BNI or a thing prescribed by the AML/CTF Rules as a monetary instrument that is capable of being copied to a police officer or a customs officer under paragraph 199(1)(f) or 199(2)(d), the officer may make a copy of the instrument or thing. Once copied, the officer must return the instrument or thing to the person. This provision retains the current powers of customs and police officers in relation to BNIs under the existing subsection 200(3).

**Item 103 – Subsection 199(2A) (heading)**

322. Item 103 repeals the heading of subsection 199(2A) and inserts ‘Person leaving or arriving in Australia—seizing monetary instrument’.

**Items 104 to 114 – Section 199**

323. Items 104 to 114 delete references to ‘physical currency’ and replaces them with ‘monetary instrument’. This provides that a police officer or customs officers have the same powers of examination and search, including boarding ships, aircraft, and entry to eligible places, for monetary instruments as they currently do for physical currency. It also provides that a monetary instrument can be of interest where it may be relevant to the investigation or prosecution of a person for an offence against the law of a Commonwealth, State or Territory, or may be of assistance in the enforcements of a proceeds of crime matter.

**Item 115 – Section 200**

324. Item 115 repeals section 200, which relates to the questioning and search powers for a police officer or customs officer in relation to BNIs. Existing section 199 will incorporate these powers following the consolidation of physical currency and BNI into monetary instrument.

**Item 116 – Subsection 201(1)**

325. Item 116 deletes reference to subsection 59(3) which provided that a customs officer or police officer could arrest a person without a warrant where they had reasonable grounds to believe the person had committed a reporting offence in relation to BNIs. This is now captured in the reference to ‘53(1)’.
Item 117 – Subsection 244(1)
326. Item 117 deletes reference to ‘55 or 59’, and replaces it with ‘55’. The existing provision requires a person providing a report under sections 55 or 59 to sign the report, or otherwise authenticate the report in an approved way. This is now captured for BNIs in the reference to ‘53’ and ‘54’.

Item 118 – Subclause 1(4) of Schedule 1
327. Item 118 repeals and substitutes subclause 1(4) of Schedule 1 which means that a monetary instrument that is a BNI for the purposes of Division 2 of Part 4 (reports about monetary instruments) and section 199 (questioning and search powers in relation to monetary instruments) has the same effect as if those provisions expressly referred to a bill of exchange or promissory note (section 51(xvi) of the Constitution).

Proceeds of Crime Act 2002

Item 119 – Subsection 29(3)
328. Item 119 deletes ‘59,’ and replaces it with ‘former section 59 or section’ in subsection 29(3) following the consolidation of reporting requirements for physical currency and BNIs.

Item 120 – Section 338 ( subparagraph (ea)(i) of the definition of serious offence)
329. Item 120 deletes ‘physical currency’ and replaces it with ‘monetary instruments’ in section 338 following the consolidation of reporting requirements for physical currency and BNIs.

Item 121 – Section 338 ( subparagraph (ea)(ii) of the definition of serious offence)
330. Item 121 deletes ‘section 59’ and replaces it with ‘former section 59’ in section 338 following the consolidation of reporting requirements for physical currency and BNIs.

Surveillance Devices Act 2004

Item 122 – Subsection 6(1) ( paragraph (ca) of the definition of relevant offence)
331. Item 122 omits reference to ‘59’ in subsection 6(1) and substitutes ‘former section 59 or section’ to reflect the consolidation of reporting requirements for physical currency and BNIs.

Item 123 – Application, saving and transitional provisions
332. Item 123 provides for the application, saving and transitional provisions for the amendments to the cross-border reporting framework.
333. Reporting requirements will apply to the movement of monetary instruments into or out of Australia on or after the commencement of this item.
334. Reporting requirements will continue to apply for movements of physical currency into or out of Australia that occurred before the commencement of this item.
335. Reporting requirements for BNIs, and the power to arrest a person without a warrant in relation to a BNI, will exist on or after the commencement of this item if a movement of BNIs occurred before the commencement of this item.
336. The structuring offence in section 143, as in force immediately before the commencement of this item, continues to apply on and after that commencement in relation to non-reportable cross-border movements of physical currency that occurred before that commencement.
337. For the purposes of the amended structuring offence in section 143 that is effective on or after the commencement of this item, a non-reportable cross-border movement of physical currency that occurred before the commencement of this item is taken to have been a non-reportable cross-border movement of monetary instruments.
338. The penalties for an infringement notice issued for a breach of subsection 53(3) on or after the commencement of this item will be determined by section 186A.
339. Infringement notices in force immediately before the commencement of this item, continue to apply on and after that commencement in relation to an alleged contravention of subsection 53(3) or 59(4) occurring before that commencement.

340. The questioning and search powers under section 199 in relation to monetary instruments will apply in relation to a person who on or after the commencement of this item is about to leave Australia or is in an embarkation area for the purpose of leaving Australia, or arrives in Australia.

341. The questioning and search powers under section 200 in relation to BNIs, as in force immediately before the commencement of this item, continue to apply on and after that commencement in relation to a person who before that commencement was about to leave Australia, or was in an embarkation area for the purpose of leaving Australia, or arrived in Australia.

Part 6 - Money Laundering Offences in the Criminal Code

Criminal Code Act 1995

Item 124 – Subsection 400.2A(2) of the Criminal Code

342. Item 124 repeals and substitutes subsection 400.2A(2) to clarify that a person may be charged with an instruments of crime offence in Division 400 if one of the circumstances described in either subsection 400.2A(3) or subsection 400.2A(4) exists. Subsection 400.2A(3) and subsection 400.2A(4) list the circumstances that give the Commonwealth constitutional authority to prosecute instruments of crime offences.

343. Section 400.2A deals with the application of the money laundering offences in sections 400.3 to 400.8 if the money or property in question is intended to be, or is at risk of becoming, an instrument of crime. A person who deals with money or other property that is an instrument of crime can only be charged with a money laundering offence under sections 400.3 to 400.8 in circumstances that connect the offence to a relevant constitutional head of power.

344. The existing subsection 400.2A(2) provides that the money laundering offences in sections 400.3 to 400.8 would apply if ‘at least one of the circumstances described in subsections (3) and (4) exists.’ There has been uncertainty about the effect of the word ‘and’ in this phrase. A possible interpretation is that the prosecution is required to establish the existence of at least one of the circumstances described in subsection 400.2A(3) and at least one of the circumstances described in subsection 400.2A(4).

345. In the course of previous prosecutions, the Commonwealth Director of Public Prosecutions (CDPP) has held enough evidence to establish that a circumstance in subsection 400.2A(3) exists, but has not been able to establish that a circumstance in subsection 400.2A(4) also exists. The new subsection 400.2A(2) aims to rectify this uncertainty.

346. The intention of the new subsection 400.2A(2) is for money laundering offences in sections 400.3 to 400.8 to apply if at least one of the circumstances in either subsection 400.2A(3) or subsection 400.2A(4) exists. This was the original intention of Parliament.

Item 125 – After section 400.10 of the Criminal Code

347. Item 125 inserts section 400.10A which provides that money or property provided by a law enforcement participant, or a civilian participant acting in accordance with the instructions of a law enforcement officer, during a controlled operation, does not need to be proved to be the proceeds of crime for the purposes of offences under sections 400.3 to 400.8.

348. Where a controlled operation occurs, the CDPP is currently unable to commence a prosecution for dealing with the proceeds of crime offences given that the money or property dealt with is not in fact the proceeds of crime. Although it may be possible to rely on an extension of criminal liability by charging an individual for conspiracy or attempt, this often renders the prosecution more complex and difficult.
349. The intention of section 400.10A is to ensure that where money or property is provided by a law enforcement or civilian participant as part of a controlled operation that will be sufficient to establish the physical element that the money or property is the proceeds of crime. This item will apply to all of the offences in sections 400.3, 400.4, 400.5, 400.7 or 400.8. The prosecution will still be required to prove the requisite fault element for each offence.

350. Given the severity of money laundering offences and the adverse consequences caused to society, individuals who are prosecuted following the supply of money in a controlled operation should be subject to the same penalty as individuals who deal with actual proceeds of crime.

351. This item also inserts the definitions of ‘civilian participant’ (in a controlled operation), ‘controlled operation’, ‘law enforcement officer’ and ‘law enforcement participant’ (in a controlled operation). These definitions are the same as those in the Crimes Act 1914.

**Item 126 – Application and transitional provisions**

352. Item 126 provides that new subsection 400.2A(2) does not affect interpretation of old subsection 400.2A(2). It should not be inferred that because new subsection 400.2A(2) only requires the existence of one circumstance in either subsection 400.2A(3) or (4), the word ‘and’ in old subsection 400.2A(2) was not to be read conjunctively.

353. This item also provides that subsection 400.10A applies in relation to offences committed on or after the commencement of this subsection. This means that money or property provided by a law enforcement or civilian participant in accordance with the instructions of a law enforcement officer as part of a controlled operation will be taken to be proceeds of crime if both the following occurred after commencement of subsection 400.10A:

- the money or property was provided by a law enforcement or civilian participant in accordance with the instructions of a law enforcement officer in a controlled operation; and
- the offender dealt with the money or property.

**Part 7 – Dishonestly Representing Conferral of Police Awards**

**Australian Federal Police Act 1979**

**Item 127 – After section 61**

354. Item 127 inserts new section 62, which creates an offence of dishonestly representing conferral of police awards.

355. Subsection 62(1) establishes that a person commits an offence if the person dishonestly represents that a police award has been conferred on the person. This offence is punishable by six months imprisonment and/or a maximum fine of 30 penalty units (these penalty units may be imposed in accordance with subsection 4B(2) of the Crimes Act 1914). This penalty aligns with the similar offence for the improper use of service decorations at subsection 80B(1) of the Defence Act 1903.

356. Subsection 62(2) defines the term ‘police award’. This subsection outlines that, for the purposes of section 62, a police award is an award, commendation, citation, medal or other decoration (however described) that has been or may be conferred on the Commissioner or an Australian Federal Police (AFP) appointee for police services that are provided by the Commissioner of Police or AFP appointee.

357. This definition ensures that the offence applies to awards that can be conferred on sworn or unsworn officers, including those under the Australian Federal Police Act 1979 (AFP Act), the Australian Honours System (such as the National Police Service Medal and Police Overseas Service Medal), and those administered by foreign governments.

358. The definition also ensures that the offence only extends to awards that have been or may be conferred on an AFP appointee or Commissioner for ‘police services’, which under section 4 of the AFP Act ‘includes services by way of the prevention of crime and the protection of persons from injury
or death, and property from damage, whether arising from criminal acts or otherwise’. This ensures that the offence is appropriately confined to awards for police services.

359. Subsection 62(3) defines the test of dishonesty as the fault element of this offence. According to this subsection, dishonesty means conduct that is dishonest according to the standards of ordinary people and known by the defendant to be dishonest according to the standards of ordinary people. This definition of dishonesty is consistent with the definition of dishonesty at section 130.3 of the Criminal Code.

360. Subsection 62(4) provides that, in a prosecution for an offence against section 62, the determination of dishonesty is a matter for the trier of fact.

**Dishonesty as a fault element**

361. The incorporation of a fault element of dishonesty as part of this offence deviates from the standard fault element of intention for conduct as per subsection 5.6(1) of the Criminal Code. According to the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, any deviation from the standard application of the Criminal Code fault elements must be justified. One possible justification for deviation is that ‘it is not possible to achieve the Government’s objectives through the Criminal Code options’ (p. 20).

362. The use of the fault element of dishonesty is necessary to achieve the Government’s objectives by ensuring that the offence strikes a balance between punishing individuals who unjustifiably represent themselves as a recipient of a police award while allowing individuals who have not received an award to wear these awards in permissible circumstances without committing an offence.

363. The definition of dishonesty at subsection 62(3) means dishonest according to the standards of ordinary people and known to the defendant to be dishonest according to the standards of ordinary people.

364. Pursuant to this definition, a person would not be considered to have dishonestly represented that a police award has been conferred on them where that person wears this award in permissible circumstances, for example:

1. in a dramatic presentation, such as a film, to convey that a fictional person is the recipient of the award, or
2. to honour a deceased family member, close relative or colleague who was the true recipient of the award.

365. However, a representation will be dishonest if a person falsely represents that they received a police award to secure employment or to increase their standing in the community.
Regulation Impact Statement

ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING AND OTHER LEGISLATION AMENDMENT BILL 2019
# TABLE OF CONTENTS

- Executive Summary 53
- 1. The Problem 54
  - Customer Due Diligence reliance 55
  - Secrecy and access of AUSTRAC information 57
  - Consolidating cross border currency reporting 58
  - Correspondent banking 59
  - CDD procedure requirements (service prohibition where CDD not completed) 59
  - Money laundering offences 59
- 3. Policy Options 60
  - Impacts 60
- 4. Impact Analysis 63
- 5. Consultation 64
- 6. Implementation 65
  - Attachment A: Comparative summary of Options 66
  - Attachment B - Indicative Costings and Assumptions 70
  - Attachment C: List of submissions to AML/CTF Review 1
  - Attachment D: Stakeholder Engagement 3
EXECUTIVE SUMMARY

This regulatory impact statement (RIS) examines proposed reforms to the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (the AML/CTF Act) and the money laundering offences in the Criminal Code 1995.

Comprehensive domestic and international reviews of Australia’s anti-money laundering and counter-terrorism financing (AML/CTF) regime have highlighted a range of difficulties and opportunities for better regulation. The Government is implementing the recommendations of these reviews in phases and the first phase of amendments was implemented in 2017. The next phase is being implemented through the Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Bill 2019. This bill contains a range of reforms including:

- expanding the circumstances in which reporting entities can rely on customer due diligence (CDD) conducted by a third party
- clarifying the prohibition on ‘tipping off’ to allow designated business groups and corporate groups to better manage their ML/TF risks
- simplifying the provisions governing the secrecy and access of AUSTRAC information
- simplifying and consolidating cross border movement reporting requirements
- strengthening the money laundering offences in the Criminal Code 1995, and
- measures to improve Australia’s compliance with international standards in relation to correspondent banking\(^2\) and CDD\(^3\).

The proposed reforms in this bill address feedback from industry that the current regime is too complex and therefore frustrates compliance with AML/CTF obligations. In addressing this feedback, the proposed reforms also focus on streamlining obligations, lowering the regulatory burden where possible and improving compliance with international standards.

Regulatory impact

The AML/CTF Act requires reporting entities to identify and verify their customers through CDD procedures, which represents a major component of AML/CTF compliance costs. The preferred option for reform outlined in this RIS (Option 3) will provide reporting entities with further options to rely on CDD procedures undertaken by a third party. As projected, these options could reduce the time involved in identifying each customer by 66 percent and the cost of verifying each customer by 80 percent. This is expected to deliver a very significant reduction in regulatory burden for reporting entities under the AML/CTF Act, leading to significantly reduced compliance costs and an estimated saving of $3,106,996,010 over ten years.

The other proposed measures in the bill have either a neutral or low regulatory impact.

\(^2\) FATF recommendation 13 refers.
\(^3\) FATF recommendation 10 refers.
1. THE PROBLEM

Globally, money laundering is a key enabler of transnational, serious and organised crime. Every year, criminals generate huge amounts of funds from illicit activities, including among other things, drug trafficking, tax evasion, theft, fraud and corruption. In order to identify and combat these threats, in 2006 Australia established an anti-money laundering and counter-terrorism financing (AML/CTF) regulatory regime in consultation with industry. This regime is based on the Financial Action Task Force’s (FATF) international AML/CTF standards and establishes a strong regulatory regime for combating money laundering and terrorism financing (ML/TF), as well as other serious crimes. This provides for the collection of valuable information from the private sector about the movement of money and other assets to the Australian Transaction Reports and Analysis Centre (AUSTRAC). AML/CTF regulation imposes a necessary regulatory cost to businesses in order to harden Australia’s financial system against threats to our national security. However, it is important that such regulation strike the right balance of achieving AML/CTF objectives while minimising the impact on business.

The pursuit of illicit profits comes at a significant cost to the Australian economy. In 2014, the Australian Criminal Intelligence Commission estimated that serious and organised crime costs Australia $36 billion per year. Additionally, funds for terrorism can come from a range of sources, legitimate and illegitimate, and can have similar characteristics to that observed in money laundering. Relatively small amounts of money placed in the hands of terrorists and terrorist organisations can have catastrophic consequences, funding attacks on Australian soil or supporting terrorist activities overseas.

In response to these significant threats, the primary objectives in updating Australia’s AML/CTF system is to balance imperatives such as better prevention, disruption and detection of ML/TF in Australia, with complementary regulatory efficiencies while enhancing compliance with the FATF’s international standards.

The statutory review

Section 251 of the AML/CTF Act required a review of the operation of the regulatory regime to commence before the end of the period of seven years after the commencement of that provision. The review commenced in December 2013 and involved an extensive consultation process with industry and government agencies. The review was completed in 2016.

As well as taking into account feedback from industry, it also considered the findings of 2015 FATF ‘mutual evaluation’ of Australia’s AML/CTF regime. The mutual evaluation identified a number of deficiencies and made a series of recommendations to strengthen compliance with the FATF standards and the effectiveness of Australia’s AML/CTF regime.

In April 2016 the then-Minister for Justice tabled the report of the statutory review in Parliament with 84 recommendations to strengthen, modernise, streamline and simplify Australia’s AML/CTF regime, and enhance Australia’s compliance with the FATF standards. It also contained guiding principles for reform which included the need to minimise the regulatory burden on regulated businesses, while maintaining a regime that is an appropriate, efficient and effective means of achieving government objectives.

The Government committed to implementing the recommendations of the statutory review in phases. The first legislative reforms were included in the Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2015.

---

4 The FATF is an intergovernmental body that sets global policy for combating ML/TF. Australia is a founding member of the FATF. The FATF 40 Recommendations can be accessed at the following link: http://www.fatf-gafi.org/topics/fatfrecommendations/documents/internationalstandardsoncombatingmoneylaunderingandthefinancingofterrorismproliferation-thefatfrecommendations.html

5 As a member of the FATF, Australia periodically undergoes a mutual evaluation for the purposes of assessing compliance with the FATF’s international standards and the effectiveness of AML/CTF measures.


7 The report on the review is available at: https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/report-on-the-statutory-review-of-the-anti-money-laundering.pdf. The Department of Home Affairs is now the lead agency for progressing AML/CTF reform having received policy and administrative responsibility from the Attorney-General’s Department through a Machinery of Government change in December 2017.
Act 2017. The Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Bill 2019 represents the next phase of reform and progresses the following prioritised initiatives:

- expanding the circumstances regulated businesses may rely upon customer due diligence conducted by a third party (customer due diligence reliance)
- streamlining and simplifying the provisions governing the secrecy and access of AUSTRAC information
- clarifying the prohibition on 'tipping off' to allow ML/TF risk to be better managed at the designated business group and corporate group-level
- consolidating and enhancing cross border currency reporting requirements
- enhancing correspondent banking requirements in line with international best practice
- explicitly clarifying the prohibition on providing designated services without customer identification (CDD procedure requirements), and
- strengthening the money laundering offences in the Criminal Code 1995.

The CDD reliance and tipping off reforms will provide regulatory efficiencies for industry.

Other measures are expected to have neutral or a low regulatory impact. The correspondent banking reforms is assessed as having a low impact as the amendments largely reflect existing industry practice in line with global best practice. These amendments are necessary to enhance Australia’s compliance with FATF standards and improve our global reputation. Reforms to the CDD procedure requirements make clear an already existing requirement. Any costs to bring industry practice into line are therefore not a direct result of this legislative change.

Customer Due Diligence reliance

Broadly, the primary components of the AML/CTF regime require regulated businesses, known as reporting entities, to:

- establish, implement and maintain an AML/CTF compliance program
- conduct CDD to identify and verify customers
- keep records, and
- lodge specified transaction and suspicious matter reports with AUSTRAC.

Reporting entities must obtain a range of information from customers and use independent and reliable information to ensure they meet the obligation to ‘Know-Your-Customer’. They are also required to keep up to date information on their customers so they know if there has been any change in circumstances or business activities. These obligations enable reporting entities to better understand their customers and their financial dealings so that they can determine the ML/TF risk posed by each customer and efficiently manage this risk.

Given the intensive and ongoing nature of these obligations, CDD represents a major component of AML/CTF compliance costs.

Breaches of the obligation to undertake CDD procedures prior to providing a ‘designated service’ under the Act attract a civil penalty (section 32). Reporting entities therefore are concerned to ensure the CDD procedures are carried out in accordance with the Act.

Reforms are proposed to provide greater options for reporting entities to rely on CDD procedures (including equivalent procedures required under a foreign law) undertaken by a third party based in Australia or offshore. The costs incurred by a business to rely on a CDD procedure that has already been carried out on a customer are expected to be significantly less than undertaking the CDD.

---

8 Tipping off refers to the disclosure that a suspicious matter report, or related information, is being filed such that it ‘tips off’ the relevant person.
9 Defined in section 6 AML/CTF Act.
These options include reliance on a CDD procedure performed by:

1. an agent
2. another reporting entities (eg. a foreign equivalent)
3. parties to a ‘CDD arrangement’.

Liability for breaches of CDD will remain with the relying party in 1 and 2, but generally shift for 3. These options are expected to provide reporting entities with opportunities to reduce a significant amount of administrative cost by effectively reducing the pool of new customers that require CDD procedures to be undertaken. This will provide efficiencies and greater flexibility for reporting entities to rely on CDD procedures undertaken by other reporting entities within Australia and a range of foreign entities, providing certain safeguards are met.

There are also linkages with the Review into Open Banking in Australia\textsuperscript{10} (Open Banking review), which will give customers a right to direct that the information they already share with their bank be safely shared with others they trust. The Open Banking review recommends that the outcomes of a CDD procedure required by the AML/CTF Act should be shared as part of Open Banking. The CDD reliance reforms will facilitate this recommendation of the Open Banking review by requiring reporting entities to obtain information collected in carrying out the CDD from the relied on entity prior to the provision of the service.

**CDD arrangements**

The proposed amendments will allow reporting entities to enter into CDD arrangements with other regulated businesses in Australia and overseas, which will provide a greater range of circumstances where reliance can be applied between parties, and address some industry concerns around liability for CDD procedure breaches.

For illustration, under current arrangements, should a person have bank accounts with multiple lenders it is expected that each of those lenders will have undertaken CDD procedures on that person and absorbed the administrative cost associated with performing those procedures. Broadly speaking, under the proposed reform, should a relevant lender be party to a CDD arrangement, then CDD procedures need not be performed on an individual for the opening of subsequent accounts.

To ensure that the proposed CDD arrangements are adopted by industry, and thus realising the full deregulation potential, the reform is designed to give reporting entities a ‘safe harbour’ from liability for CDD breaches under section 32 of the AML/CTF Act. This addresses industry concerns about exposure to liability that stems from relying on the CDD procedure undertaken by third parties. More specifically, where the reporting entity has entered into the CDD arrangement, conducted due diligence on the arrangement and can show that it was appropriate to rely on the third party, the relying party would not be held liable for isolated breaches of compliance with the CDD requirements by the third party. However, where there are systemic breaches that indicate due diligence on the CDD arrangement was insufficient, the reporting entity relying on the third party’s CDD procedure would be liable for breaches.

**Reliance under the current regime - Members of a Designated Business Group (DBG) and licensed financial advisers**

Currently, there are only limited circumstances in which reporting entities can rely on a CDD procedure performed by a third party. This includes where the CDD procedure has been undertaken by another entity within their DBG. Despite the fact that a DBG may include offshore entities, the current provisions only allow

\textsuperscript{10} The Review into Open Banking in Australia was commissioned by the Hon Scott Morrison MP on 20 July 2017 to recommend the most appropriate model for open banking in Australia. The Review’s final report was published in December 2017. https://treasury.gov.au/consultation/c2018-t247313/
reliance within a DBG where the other reporting entity is a domestic reporting entity.\textsuperscript{11} This is set out in section 38 of the AML/CTF Act and chapter 7 of the AML/CTF Rules.

The other circumstance where reliance is permissible is where a licensed financial adviser who is also a reporting entity arranges for a customer to receive a service listed in the Act from a second reporting entity. For example, where a financial adviser refers a customer to a bank, the bank can rely on the CDD carried out by the adviser.

In both of the above cases, liability for a breach of the CDD procedure rests with the relying party.

Under current provisions, a reporting entity is unable to rely on CDD procedures conducted by a member of the DBG outside Australia unless the AUSTRAC CEO provides the reporting entity with an exemption. A limited exemption was provided in 2009 that permits reporting entities to rely on CDD conducted in a foreign country where:

- the CDD procedure is carried out by an Australian reporting entity or a subsidiary of an Australian reporting entity, and
- the reporting entity determines on a risk-basis that the CDD procedure is comparable to that required under Australia's AML/CTF legislation.

Feedback from industry has indicated that the availability of additional options would enable them to fulfil their CDD obligations in a more cost efficient way. Some have suggested reliance would be more widely used if liability did not remain with the relying party in all instances, and that the conditions that apply under section 38 of the AML/CTF Act are too restrictive. Some businesses are less concerned about liability and more concerned with having the ability to rely more broadly within their corporate structures.

Reform is therefore proposed to introduce CDD arrangements that either shift liability for isolated breaches would shift when an agreement is in place, or will retain liability for the relying entity when no agreement is in place.

**Secrecy and access of AUSTRAC information**

The provisions in the AML/CTF Act governing the secrecy and access of AUSTRAC information ensure that the sensitive information under AUSTRAC's control is secure and protected from unauthorised access, use and disclosure. However, a key finding in the report of the statutory review is that these provisions are unduly complex and impede the sharing of AUSTRAC information to support a modern, collaborative approaches to combating and disrupting ML/TF and other serious crimes. The review report recommends the development of a simplified model for sharing information collected under the AML/CTF Act that is:

- responsive to the information needs of agencies tasked with combating ML/TF and other serious crimes commensurate with the changing threat environment (ensuring that information can be exchanged in a timely manner)
- supports collaborative approaches to combating ML/TF and other serious crime at the national and international level, and
- establishes appropriate safeguards and controls that are readily understood and consistently applied.

The report also makes related recommendations to improve information sharing and collaboration with the private sector and provide the AUSTRAC CEO with new functions to facilitate a more effective information sharing framework.

\textsuperscript{11} Designated Business Group is defined in chapter 2 of the AML/CTF Rules.
The proposed amendments to Part 11 of the AML/CTF Act will simplify and streamline the provisions, and ensure that the legislation facilitates timely, efficient and effective sharing of AUSTRAC information with relevant partner agencies and the private sector. For the purposes of this RIS, relevant key measures include:

- allowing the AUSTRAC CEO to disclose AUSTRAC information in a manner consistent with the CEO’s function and powers;
- streamlining the process for disclosing AUSTRAC information to international bodies and the private sector (including with the Fintel Alliance), and
- revising the current strict limitations on disclosure of suspicious-matter report (SMR)-related information to ensure that the ‘tipping off’ provisions do not unnecessarily impede action being taken by government agencies and reporting entities to combat ML/TF and other serious crimes.

These reforms will enable industry to better manage ML/TF in delivering their services by allowing greater sharing of information about known or suspected risks which is crucial to combat and disrupt ML/TF. The reforms also support the Government’s agenda of having our national security, law enforcement and regulatory agencies joined up and provided with timely access to vital financial intelligence.

**Consolidating cross border currency reporting**

Currently, cross-border movements of physical currency of $10,000 or more (or foreign currency equivalent) must be reported to AUSTRAC, a police or a customs officer (a ‘CBM-PC’ report). This requirement also captures the carrying, mailing or shipping of physical currency. However, a traveler need only disclose that they are carrying bearer negotiable instruments (BNIs), such as travelers cheques, when requested by a police or customs officer (a ‘CBM-BNI’ report).

The report of the statutory review recommends the consolidation of these dual reporting regimes and the expansion of the range of reportable monetary instruments to simplify and strengthen the cross-border reporting regime. The proposed amendments will amend Part 4 of the AML/CTF Act to consolidate physical currency and BNI reporting requirements and establish an obligation to report the movement of a “monetary instrument” equal to or more than $10,000.

This measure will be further supported by a provision in the Bill for additional items to be prescribed by regulation to ensure the legislation is “future proofed”, for example, when stored value card readers become available then such items can be made declarable at the border.

In addition, the review recommended an increase in the penalties available for failing to comply with the reporting requirements to align with comparable regimes internationally. The proposed amendments increase the current penalty amounts to deter the undeclared movement of monetary instruments across the border, particularly the bulk smuggling of cash.

This will increase the penalties that can be imposed, by way of an infringement notice, for failing to comply with the relevant cross-border reporting requirements and ensure penalties are consistent with other infringement notices that can be issued under the AML/CTF Act.

The proposed amendments will also provide additional flexibility regarding the timing of CBM reports by moving the ‘timing rule’ from the primary legislation into the regulations. This will allow the timing rule to easily be amended in the future once technology is introduced that enables travellers to make a report prior to arriving at an airport.

---

12 Personal information held by AUSTRAC will continue to be accessed, used and disclosed in accordance with the Privacy Act 1988 and the accompanying Australian Privacy Principles, and include other proportionate safeguards and controls necessary to protect the confidentiality of sensitive AUSTRAC information.

13 These include to provide access to and to share AUSTRAC information to support efforts to combat ML/TF and other serious crimes.

14 The Fintel Alliance, launched by AUSTRAC, is a world-first alliance between the public and private sector which enhances information sharing to combat money laundering and terrorism financing.
Correspondent banking

Reforms are proposed to implement the remaining recommendations from the report of the statutory review on strengthening correspondent banking obligations. These reforms will simplify and streamline the correspondent banking obligations to establish a one-step process for conducting due diligence assessments on respondent financial institutions, and prohibit financial institutions from entering into a corresponding banking relationship with an institution that permits its accounts to be used by a shell bank.

Although the AML/CTF Act already prohibits correspondent banking arrangements with shell banks, it currently does not explicitly prohibit a bank from entering into or continuing a correspondent banking relationship with a respondent institution that permits their accounts to be used by shell banks. The proposed reforms would provide a civil penalty provision that would prohibit entering into, or continuing, correspondent banking arrangements with a bank that permits their accounts to be used by shell banks. Banks would also be required to terminate arrangements if they became aware that a respondent bank is a shell bank or permits accounts to be used by shell banks.

The reforms will also require financial institutions to obtain senior official approval to continue a correspondent banking relationship following a regular due diligence assessment. This is similar to the requirement that currently exists to obtain senior official approval before entering a correspondent banking relationship.

The proposed amendments will largely mirror existing industry and international banking practice and are expected to have a minor cost to banks. They represent an important step in enhancing compliance with relevant international standards set by the FATF.

CDD procedure requirements (service prohibition where CDD not completed)

In addition to the CCD reliance reform discussed above, reforms are proposed to implement a statutory review recommendation to explicitly prohibit reporting entities from providing a designated service in circumstances where the CDD procedure cannot be carried out, and require reporting entities to consider making a suspicious matter report if such circumstances arise.

This explicit prohibition will deter reporting entities from providing designated services to a customer that cannot be identified in accordance with the requirements of the AML/CTF regime and provide for the reporting of information to AUSTRAC when an inability to complete the CDD occurs in suspicious circumstances. This reform is to make clear an already existing requirement under s32.

The proposed reform will address a deficiency identified in the FATF mutual evaluation of Australia’s AML/CTF regime in 2015 and strengthen CDD measures.

The proposal to require reporting entities to consider making a suspicious matter report when the CDD cannot be completed is likely to have a low regulatory impact, as this type of reporting is consistent with existing requirements to generally report suspicious matters associated with the provision of a designated service.

Money laundering offences

Reforms are proposed to amend the money laundering offences contained in Division 400 of the Criminal Code. These amendments will strengthen the offences by addressing a number of practical issues identified through prosecutorial experience of the Commonwealth Director of Public Prosecutions (CDPP).

These issues include difficulties in establishing that a money laundering offence is related to a possible instrument of crime. In these instances, the CDPP has been required to re-frame the prosecution or not proceed with an instrument of crime offence. Proposed amendments to the Criminal Code will therefore clarify that only one circumstance connected to a Commonwealth head of power and not two circumstances is required when establishing that a person was dealing with money or property that is, or is at risk of, becoming an instrument of crime.
A second issue relates to situations where law enforcement agencies use undercover law enforcement officers posing as criminals seeking the services of a syndicate to launder large sums of cash to gather evidence to support complex money laundering investigations. The CDPP has advised that where these operations occur, the money or property provided by the undercover law enforcement officers and dealt with by the syndicate is not actually the proceeds of crime, so no money laundering offence can be proved under Division 400 of the Criminal Code. In these circumstances, the CDPP is forced to rely on an extension of criminal responsibility under Division 11 of the Criminal Code, such as conspiracy or attempt. However, prosecutions under Division 11 are significantly more complex and difficult to successfully prosecute.

An amendment is therefore proposed to the Criminal Code that provides that the money supplied in an undercover operation by a law enforcement participant, or civilian participant acting in accordance with the instructions of a law enforcement officer, is the proceeds of crime and therefore is not required to be proved to be proceeds of crime by the CDPP.

3. POLICY OPTIONS

A number of options have been considered in developing the proposed reforms. For the purpose of the RIS, the focus is on the reforms that are most likely to have a regulatory impact on industry – CDD reliance, CDD procedure requirements reforms, and correspondent banking.

- **Option 1: Maintain the status quo.** This would involve making no changes.
- **Option 2: Minimal changes to the existing AML/CTF requirements.** Under this option, reforms to CDD reliance would retain the current reliance framework but broaden the parties that can be relied upon with liability remaining with the relying party. Under option 2, changes to correspondent banking, and other CDD procedure requirements (service prohibition where CDD not completed) would also not be pursued.
- **Option 3 (preferred): Detailed reform.** In addition to the reform under option 2, this option would include an additional option permitting reporting entities to enter into ‘CDD arrangements’ for reliance to occur. This offers greater opportunity for regulatory efficiency, with liability linked to the relying party undertaking due diligence on the third parties’ CDD processes, rather than being liable for each case of inadequate CDD that may arise.

Comparative detail concerning these options can be found at Attachment A.

**Impacts**

**OPTION 1 – MAINTAIN THE STATUS QUO**

Option 1 would not address the recommendations of the statutory review, and therefore would not address stakeholder concerns about undue complexity, regulatory burden or address deficiencies in compliance with international standards identified by the FATF.

**CDD – reliance**

The AML/CTF Act and Rules currently allow a reporting entity to rely on customer identification and verification procedures carried out by another reporting entity in limited circumstances. A reporting entity is unable to rely on customer identification conducted outside of Australia unless the AUSTRAC CEO provides the reporting entity with an exemption.

Outside of the licenced financial advisors options, Industry stakeholders have indicated that the reliance provisions under the AML/CTF Act are rarely used, as they lack clarity and certainty, are too restrictive and reporting entities are reluctant to expose themselves to the risk of being held accountable for a breach of CDD requirements performed by a third party.
Due to the restrictive nature of the reliance provision and limited uptake from industry, reporting entities generally complete CDD for every customer they on-board. CDD is a major aspect of AML/CTF compliance and carries a substantial cost. With the current structure, this cost can be duplicated where customers adopt multiple designated services offered by different reporting entities.

Based on the comprehensive consultation process conducted during the course of the review and through the development of the current phase of legislative amendments, industry generally does not support the option of maintaining the status quo. Doing so would fail to provide flexibility to industry to meet their AML/CTF obligations in a more efficient way and would not be in line with the broader ‘Open Banking’ reforms.

**CDD procedure requirements – service prohibition where CDD not completed**

The FATF identified in Australia’s mutual evaluation that the CDD identification provision does not explicitly prohibit reporting entities from providing a designated service in circumstances where the CDD cannot be carried out, and does not require reporting entities to consider making a suspicious matter report in such circumstances. Maintaining the status would not address the FATF deficiency.

**Correspondent banking**

Correspondent banking relationships are vulnerable to ML/TF as they involve a financial institution carrying out transactions on behalf of another financial institution’s customers where information on those customers is very limited. The ML/TF risks are particularly high where a respondent institution permits their accounts to be used by shell banks. As shell banks do not have an actual place of business in any country, it is difficult to regulate them or ensure they are not violating anti-money laundering regulations. As a result, the FATF standards contain a prohibition on the use of shell banks.

Australia’s AML/CTF regime recognises this threat and prohibits regulated financial institutions from entering correspondent banking relationships with another financial institution that has a correspondent banking relationship with a shell bank. Financial institutions must also terminate a correspondent banking relationship if they become aware that a respondent bank has a correspondent banking relationship with a shell bank. However, the FATF has identified a deficiency in Australia’s AML/CTF regime as financial institutions are not required to satisfy themselves that a respondent financial institution that they are entering into a correspondent banking relationship with does not permit its accounts to be used by shell banks. This exposes Australian financial institutions to unnecessary risk that they may be misused by shell banks for ML/TF purposes. If the status quo is maintained, the FATF deficiency and associated risks will remain.

**OPTION 2 – MINIMAL CHANGES TO THE EXISTING AML/CTF REQUIREMENTS**

Option 2 would reform the CDD reliance regime by expanding the parties (both domestically and internationally) that a reporting entity may rely upon when conducting CDD but maintaining liability for all breaches with the relying party (a civil penalty provision).

The expansion of the parties that a reporting entity may rely upon when conducting CDD will address one of the key concerns for industry regarding the restrictive nature of the reliance provisions under the current regime. Under this option, while reporting entities may rely on a broader range of businesses, the ultimate liability for one off individual breaches of the CDD requirements will remain with the relying party, thus making reliance less attractive.

During consultation with industry, some expressed concerns that the CDD reliance would continue to be under-utilised if this option was pursued alone due to issues around liability for breaches and tolerance for risk. Reporting entities indicated option 2 would not adequately address liability for one off breaches of the CDD requirements by a third party.
Under Option 2, reforms to correspondent banking would not be pursued, and as such, impacts outlined above would remain relevant.

**OPTION 3 – COMPREHENSIVE REFORM**

Option 3 would involve more comprehensive reforms of the CDD reliance, clarification of CDD requirements, and correspondent banking arrangements. This approach would best address both industry feedback and FATF deficiencies. This is the preferred option.

**CDD – reliance and service prohibition where CDD cannot be completed**

Given that CDD is currently a major aspect of a business’ AML/CTF compliance costs, this option will provide industry with greater flexibility by allowing increased options for CDD reliance. It will also deliver significant regulatory savings.

Proposed reforms will allow reporting entities to enter into a ‘CDD arrangement’ with a third party which provides a framework for relying on a CDD performed by the third party. As part of entering into the CDD arrangement, the reporting entity will be required to conduct due diligence on the third party’s CDD processes and procedures to ensure they are compliant with the FATF standards and that it is reasonable to rely in the circumstances.

Under this proposal, where a reporting entity has relied on the CDD performed by a third party pursuant to a CDD arrangement, and there is a breach of identification requirements, the relying entity will not be liable for a one-off breach if it is able to show it was reasonable to have relied upon the CDD in circumstances having conducted robust due diligence on the third party’s CDD processes.

Where there are more systemic breaches of CDD requirements by the third party, and the relying reporting entity has relied on this CDD in the absence of conducting adequate due diligence on the third party’s CDD processes (including ongoing diligence), the relying party will be ultimately responsible for the individual breaches and liable to the civil penalty provision.

Reporting entities that choose to use the CDD arrangements model will face an initial increase in regulatory costs to establish the arrangements and undertake due diligence on a third party’s CDD procedures. However, after this initial phase, the proposal is expected to significantly reduce costs and regulatory burden for users. It is noted that the uptake of this measure will be dependent on a range of factors including company structure, type of service and customer, and ability to broker CDD arrangements with other entities. Allowing a reporting entity to rely on another entity’s CDD processes will reduce duplication of effort across regulated business and reduce the requirements on customers to provide identity documentation at the on-boarding stage for various services. The proposal will also be consistent with the reforms of the Review into Open Banking in Australia.

Estimating the regulatory costs and savings of this option across the spectrum of reporting entities is difficult as they service a customer base that includes natural persons, non-individuals and beneficial owners of varying type, size and complexity. Based on AUSTRAC engagement with industry, it is assumed that CDD activities currently require a minimum of approximately three hours to complete for a new customer, and cost approximately $15 per new customer in third-party service provider and database search fees. It is expected that CDD obligations under the new model will reduce the time costs to approximately 1 hour for basic information verification for natural person customers, and will reduce the third-party costs to approximately $2.50 - $3.00 for identity verification searches.
This reduction, when applied across the anticipated 1,630 effected reporting entities with the number of new customers (which ranges from 50 up to 25,000 per entity), is expected to result in an average regulatory saving of $310,722,924 each year for ten years.

To maximise the potential of this option, it establishes a regulatory environment whereby a significant saving of effort can be achieved through encouraging cooperation between reporting entities. Further, it is expected that through the process of establishing agreements, that parties through a natural evaluation process of each other’s CDD procedures, will drive a higher overall standard of AML/CTF compliance.

The proposal will also prohibit reporting entities from providing a designated service in circumstances where the CDD cannot be carried out, and require reporting entities to consider making a suspicious matter report in such circumstances. This reform will address a further deficiency identified by the FATF.

During consultation with industry, stakeholders agreed that this option presented the greatest opportunity for reducing burden while strengthening Australia’s compliance with FATF standards and international reputation.

**Correspondent banking**

The reforms would extend the civil penalty provision that prohibits reporting entities from entering into, or continuing correspondent banking relationships with a shell bank, to banks that permits their accounts to be used by a shell bank. The reforms would also explicitly clarify that banks must conduct due diligence and have appropriate senior management approvals prior to entering or continuing correspondent banking arrangements.

The reforms will address the remaining deficiencies identified by the FATF in relation to Australia’s correspondent banking regime and will mitigate any risks that Australia financial institutions are misused by shell banks for ML/TF purposes.

The proposed changes reflect a codification of existing practices and are expected to carry a low regulatory cost to reporting entities.

### 4. IMPACT ANALYSIS

The groups likely to be affected, directly or indirectly, by Options 2 and 3 are:

- reporting entities – financial institutions, bullion and gambling sectors
- AUSTRAC and partner government agencies, and
- consumers.

The impact of Option 1 is not addressed in detail in this RIS because it does not impose any regulatory obligations on reporting entities.
Compliance costs

A summary of the estimated overall annualised cost and savings over 10 years of the regulatory impacts/offsets identified in the previous section, as well as the assumptions used to estimate the cost/offsets can be found at Attachment B.

Regulatory savings will arise under both options 2 and 3 and will outweigh the costs in both cases.

**Costs excluded from the Regulatory Burden Measurement framework**

**Non-compliance and enforcement costs**

There may be costs for businesses under Options 2 and 3.

**Indirect costs**

Businesses that incur compliance costs as a result of regulation under Option 2 or 3 are expected to pass part of these costs to consumers.

5. CONSULTATION

Throughout 2014-15, the Attorney-General’s Department, in consultation with AUSTRAC, conducted extensive consultation with industry and government agencies as part of the statutory review of the AML/CTF regime. Over 75 submissions were received from industry, government agencies and other interested parties (see Attachment C for a list of entities providing a submission). A series of roundtable meetings were also held with the cash-in-transit, gaming, remittance, not-for-profit, banking and finance sectors in late 2014 and early 2015.

A roundtable meeting with government agencies was held in late January 2015.

A list of industry and government agencies that participated in round-table discussions is at Attachment D.

Input provided by industry and government during the lengthy consultation was considered in developing the review recommendations.

The Department of Home Affairs then undertook consultation on the detail of the review recommendations for implementation in this Bill which commenced in mid-2017 with the release of consultation papers and a workshop with industry representatives on the CDD reliance reforms. Attendance at the workshop was facilitated by the Australian Bankers Association and the Australian Financial Markets Authority.

Meetings were held with government agencies in 2017 and 2018 on the secrecy and access reforms. Consultation with industry has also occurred through the Fintel Alliance.

Throughout these engagements, industry feedback in relation to the proposed amendments has been positive, often providing constructive input resulting in incremental improvements in Australia’s AML/CTF regime.

Further consultation will occur during 2019, including targeted consultation with industry sectors and further meetings or workshops if required. The Department will also consult with industry about an appropriate implementation period.

If the Bill is passed by Parliament, the Department of Home Affairs, in partnership with AUSTRAC, will continue to engage with industry and government on implementation issues and consider opportunities for targeted education and guidance to both regulated and non-regulated sectors.
6. IMPLEMENTATION AND REVIEW

Delayed commencement

It is proposed that measures in the Bill would commence 6-12 months from the date of Royal Assent to enable industry time to make any changes to systems. After a suitable time has elapsed to allow consideration on whether these reforms are operating as intended, AUSTRAC and the Department of Home Affairs will seek industry feedback.

AUSTRAC support and guidance

AUSTRAC will consult closely with industry about the reforms and consider opportunities for targeted education and guidance to regulated and non-regulated sectors.
ATTACHMENT A: COMPARATIVE SUMMARY OF OPTIONS

The following is a summary of the options considered in this RIS:

<table>
<thead>
<tr>
<th></th>
<th>OPTION 1: MAINTAIN THE STATUS QUO</th>
<th>OPTION 2: MINIMAL CHANGES TO THE AML/CTF REQUIREMENTS</th>
<th>OPTION 3: DETAILED REFORM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SUMMARY</strong></td>
<td>No change to the current reliance provisions.</td>
<td>Expand parties (domestically and internationally) that a reporting entity may rely upon when conducting CDD but liability will remain with the relying for individual breaches of CDD.</td>
<td>Expand parties (domestically and internationally) that a reporting entity may rely upon when conducting CDD. Clarify that where a reporting entity relies on a third party, they remain responsible if a breach of CDD requirements occurs. Allow reporting entities to enter CDD arrangements with other regulated business, which will enable the entity to show it was reasonable for it to rely upon CDD undertaken by the third party and not be held responsible for a one off breach of CDD requirements.</td>
</tr>
<tr>
<td><strong>RESOURCE IMPLICATIONS</strong></td>
<td>No change to resource implications.</td>
<td>Minor reduction in compliance costs for regulated business.</td>
<td>Initial increase in compliance costs for regulated business, followed by a significant reduction in compliance costs over longer period.</td>
</tr>
<tr>
<td><strong>ADVANTAGES</strong></td>
<td>No advantages.</td>
<td>Expands the parties that a reporting entity may rely upon both domestically and internationally.</td>
<td>Expands the parties that a reporting entity may rely upon both domestically and internationally. Addresses key deterrent for reporting entities to adopt CDD reliance provisions. Potential for significantly reduced compliance costs.</td>
</tr>
</tbody>
</table>
### CUSTOMER DUE DILIGENCE (CDD) RELIANCE

| DISADVANTAGES | Provisions remain unused by reporting entities. No reduction of compliance costs for reporting entities. | Provisions may remain unused by reporting entities. No reduction of compliance costs for reporting entities. | Possibility that provisions remain unused by reporting entities. |

---

### CORRESPONDENT BANKING

<table>
<thead>
<tr>
<th>SUMMARY</th>
<th>OPTION 1: MAINTAIN THE STATUS QUO</th>
<th>OPTION 2: MINIMAL CHANGES TO THE AML/CTF REQUIREMENTS</th>
<th>OPTION 3: DETAILED REFORM</th>
</tr>
</thead>
<tbody>
<tr>
<td>No change to the current correspondent banking provisions.</td>
<td>No change to the current correspondent banking provisions.</td>
<td>Provide a civil penalty provision that prohibits entering into, or continuing a correspondent banking relationship with a shell bank or bank that permits their accounts to be used by shell banks. Require banks to conduct CDD and have appropriate approvals prior to entering into and continuing a correspondent banking relationship.</td>
<td></td>
</tr>
</tbody>
</table>

|-----------------------|--------------------------|--------------------------|-------------------------------------------------|

<table>
<thead>
<tr>
<th>ADVANTAGES</th>
<th>No advantages.</th>
<th>No advantages.</th>
<th>Addresses remaining correspondent banking deficiencies identified by the FATF.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>DISADVANTAGES</th>
<th>Deficiencies of corresponding banking framework as identified by the FATF mutual evaluation of Australia’s AML/CTF regime remain. Australian banks may enter/carry on correspondent banking relationships with respondent institutions that permit their accounts to be used by shell banks (carrying higher ML/TF risks).</th>
<th>Deficiencies of corresponding banking framework as identified by the FATF mutual evaluation of Australia’s AML/CTF regime remain. Australian banks may enter/carry on correspondent banking relationships with respondent institutions that permit their accounts to be used by shell banks (carrying higher ML/TF risks).</th>
<th>Minimal compliance costs for regulated business.</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDD REQUIREMENTS – SERVICE PROHIBITION WHERE IDENTIFICATION INCOMPLETE</td>
<td>OPTION 1: MAINTAIN THE STATUS QUO</td>
<td>OPTION 2: MINIMAL CHANGES TO THE AML/CTF REQUIREMENTS</td>
<td>OPTION 3: DETAILED REFORM</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>SUMMARY</td>
<td>No changes to the customer identification regime.</td>
<td>No changes to the customer identification regime.</td>
<td>Explicitly prohibit reporting entities from providing a designated service in circumstances where the applicable customer identification procedure cannot be carried out. Require reporting entities to make a suspicious matter report in the above circumstances.</td>
</tr>
<tr>
<td>ADVANTAGES</td>
<td>No advantages.</td>
<td>No advantages.</td>
<td>Address deficiency identified during the FATF mutual evaluation of Australia’s AML/CTF regime.</td>
</tr>
<tr>
<td>DISADVANTAGES</td>
<td>Deficiencies of customer identification framework as identified by the FATF mutual evaluation of Australia’s AML/CTF regime remain. Risk exists where business that offers a designated service do not have capability to undertake necessary customer identification processes.</td>
<td>Deficiencies of customer identification framework as identified by the FATF mutual evaluation of Australia’s AML/CTF regime remain. Risk exists where business that offers a designated service do not have capability to undertake necessary customer identification processes.</td>
<td>Minimal compliance costs for regulated business.</td>
</tr>
</tbody>
</table>
ATTACHMENT B - INDICATIVE COSTINGS AND ASSUMPTIONS

## Regulatory costs and offsets

<table>
<thead>
<tr>
<th>Obligation imposed or removed</th>
<th>Options:</th>
<th>Impact ($)(^{15})</th>
<th>Assumptions and Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1 – Maintain the status quo</td>
<td>Annualised one-off cost</td>
<td>Annualised ongoing cost</td>
</tr>
<tr>
<td>Customer Due Diligence (CDD) - Reliance</td>
<td>1</td>
<td>Unchanged</td>
<td>Unchanged</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>$2,395,523</td>
<td>($104,475,332)</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>$5,362,793</td>
<td>($311,259,204)</td>
</tr>
<tr>
<td>Correspondent Banking</td>
<td>1, 2</td>
<td>Unchanged</td>
<td>Unchanged</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>$6,927</td>
<td>Nil</td>
</tr>
</tbody>
</table>

\(^{15}\)Timings are indicative. Positive figures are costs. Figures in brackets are savings.
<table>
<thead>
<tr>
<th>Obligation imposed or removed</th>
<th>Options: 1 – Maintain the status quo 2 – Minimal changes 3 – Detailed reform</th>
<th>Impact ($)</th>
<th>Assumptions and Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Options: 1 – Maintain the status quo 2 – Minimal changes 3 – Detailed reform</td>
<td>1, 2</td>
<td>Unchanged</td>
</tr>
<tr>
<td></td>
<td>Options: 1 – Maintain the status quo 2 – Minimal changes 3 – Detailed reform</td>
<td>3</td>
<td>Nil</td>
</tr>
<tr>
<td>CDD Procedure requirements – Service Prohibition where CDD not completed</td>
<td>Options: 1 – Maintain the status quo 2 – Minimal changes 3 – Detailed reform</td>
<td>1, 2</td>
<td>Unchanged</td>
</tr>
</tbody>
</table>
|                             | Options: 1 – Maintain the status quo 2 – Minimal changes 3 – Detailed reform | 3          | Nil       | Nil        | Nil       | Nil       | There is no existing or future impost on reporting entities for CBM reporting. CBM reporting impacts:  
  - Travellers, flight and ship crews for providing details about |
| Cross Border Movement (CBM/BNI) Reporting | Options: 1 – Maintain the status quo 2 – Minimal changes 3 – Detailed reform | 1, 2       | Unchanged | Unchanged | Unchanged | Unchanged | |
| Obligation imposed or removed | Options:  
1 – Maintain the status quo  
2 – Minimal changes  
3 – Detailed reform | Impact ($) $^{15}$ | | | | Assumptions and Comments |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Annualised one-off cost</td>
<td>Annualised ongoing cost</td>
<td>Average cost per year</td>
<td>Total cost over 10 years</td>
</tr>
<tr>
<td>themselves, their travel and the physical currency and/or bearer negotiable instruments (BNIs) they are carrying</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Department of Home Affairs (Immigration and Border Protection) and Australian Federal Police (AFP) are responsible for collecting and handling CBM reports from travellers and issuing infringement notices, if required</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>There is a negligible time factor of less than five seconds for travellers, flight and ship crews to confirm whether they are carrying physical currency of $10,000 or more (or foreign equivalent) on passenger cards. And if carrying that amount of physical currency or declaring BNIs when asked, on average the time taken to complete a CBM form is less than five minutes.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consolidating the existing CBM reporting requirements will impose a small but incalculable regulatory impact on travellers and crews. This is because the change might require a small number of people to mandatorily report that may currently</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obligation imposed or removed</td>
<td>Options: 1 – Maintain the status quo 2 – Minimal changes 3 – Detailed reform</td>
<td>Impact ($)(^{15})</td>
<td>Assumptions and Comments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>-----------------</td>
<td>-----------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Annualised one-off cost</td>
<td>Annualised ongoing cost</td>
<td>Average cost per year</td>
<td>Total cost over 10 years</td>
<td></td>
</tr>
<tr>
<td>Secrecy and Access</td>
<td>1, 2 Unchanged</td>
<td>Unchanged</td>
<td>Unchanged</td>
<td>Unchanged</td>
<td>There is no proposed change to the current regime with options 1 and 2.</td>
</tr>
</tbody>
</table>
|                             | 3 $226,298 | Nil | $22,630 | $226,298 | The intention is to overhaul Part 11 of the AML/CTF Act to:  
• Provide greater flexibility of the use and disclosure of AUSTRAC information to a range of government and industry stakeholders with appropriate privacy safeguards  
• Improve information sharing and collaboration within the private sector  
In effect the new requirement will be a cost saving rather than a cost as currently reporting entities cannot share SMR information within their corporate group (see also the reforms contained under Phase 1) or with government bodies other than |
<table>
<thead>
<tr>
<th>Obligation imposed or removed</th>
<th>Options: 1 – Maintain the status quo 2 – Minimal changes 3 – Detailed reform</th>
<th>Impact ($)</th>
<th>Assumptions and Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Annualised one-off cost</td>
<td>Annualised ongoing cost</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Assumptions

RELIANCE OPTION 2 – NO CDD ARRANGEMENTS

<table>
<thead>
<tr>
<th>Obligation imposed or removed</th>
<th>Option</th>
<th>Impact ($)(^{16})</th>
<th>Total cost over 10 years</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Annualised one-off cost</td>
<td>Annualised ongoing cost</td>
</tr>
<tr>
<td>Customer Due Diligence (CDD)</td>
<td>2</td>
<td>Minimal</td>
<td></td>
</tr>
</tbody>
</table>

The assumptions for Reliance Option 2 are based on those for Option 3 (below).

In comparison to the full model in Option 3, we have assumed that all assumptions remain the same with the exception of the following:

- Reporting entities who choose to use reliance will not be required to prove that they have conducted due diligence on the institution they are relying on, as they will maintain the liability of the CDD activities at all times. This reduces the time associated with establishing reliance agreements, and removes the need for annual reviews of their partner institutions.

- Reporting entities will not be required to enter into formal agreements with other institutions in order to undertake reliance activities. This will reduce the time associated with commencing reliance arrangements.

- The number of reporting entities that will utilise the reliance provisions will drop significantly. This is due to the fact that the provisions will require every reporting entity to maintain liability for conducting due diligence on their customers, regardless of whether they have relied on the due diligence of another institution. This situation could pose too high a business risk for most reporting entities, and feedback received from industry indicates that domestic banks would be largely unwilling to consider reliance options.

- It is expected that foreign banks will be the primary users of the reliance provisions under this option. Some remitters and financial services intermediaries are also expected to utilise the provisions. Only approximately 695 reporting entities are expected to utilise the provisions under this model.

\(^{16}\)Timings are indicative. Positive figures are costs. Figures in brackets are savings.
CALCULATIONS FOR RELIANCE OPTION 2

<table>
<thead>
<tr>
<th>Sector</th>
<th>Sub-Sector</th>
<th>Population</th>
<th>Impacted Population (IP)</th>
<th>Understand requirements (hours x pop.)</th>
<th>Implement business processes (hours x IP)</th>
<th>Implement Agreements (hours x IP)</th>
<th>Analyse CDD of partner institutions (hours x IP)</th>
<th>Suitable Customers per IP per annum</th>
<th>Old CDD requirements (hours x Cust. x IP)</th>
<th>Old CDD Requirements ($Cost x Cust. x IP)</th>
<th>Reliance model (hours x Cust. x IP)</th>
<th>Reliance model ($Cost x Cust. x IP)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Financial Services</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Banks Domestic</td>
<td>Small</td>
<td>94</td>
<td>-</td>
<td>2</td>
<td>10</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>25,000</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>25,000</td>
</tr>
<tr>
<td>Banks Foreign</td>
<td>Small</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>50</td>
<td>20</td>
<td>2</td>
<td>10</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Remittance Dealers</td>
<td>Small</td>
<td>5,050</td>
<td>150</td>
<td>2</td>
<td>5</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>500</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>50</td>
<td>5</td>
<td>2</td>
<td>10</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>5,000</td>
<td>3</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>Custodians</td>
<td>Small</td>
<td>108</td>
<td>-</td>
<td>2</td>
<td>5</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>250</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>20</td>
<td>-</td>
<td>2</td>
<td>5</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>500</td>
<td>3</td>
</tr>
<tr>
<td>Digital Currency Exchanges</td>
<td>Small</td>
<td>115</td>
<td>-</td>
<td>2</td>
<td>5</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>25</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>5</td>
<td>-</td>
<td>2</td>
<td>5</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>100</td>
<td>3</td>
</tr>
<tr>
<td>Financial Service Intermediaries</td>
<td>Small</td>
<td>1,426</td>
<td>500</td>
<td>2</td>
<td>5</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>150</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>50</td>
<td>20</td>
<td>2</td>
<td>5</td>
<td>-</td>
<td>-</td>
<td>150</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Foreign Exchange Providers</td>
<td>Small</td>
<td>89</td>
<td>-</td>
<td>2</td>
<td>5</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>250</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>20</td>
<td>-</td>
<td>2</td>
<td>5</td>
<td>-</td>
<td>-</td>
<td>500</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Insurance Product Issuers</td>
<td>Small</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>38</td>
<td>-</td>
<td>2</td>
<td>5</td>
<td>-</td>
<td>-</td>
<td>1000</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Non-Bank Lenders &amp; Financiers</td>
<td>Small</td>
<td>1,119</td>
<td>-</td>
<td>2</td>
<td>5</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>10,000</td>
<td>3</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>50</td>
<td>-</td>
<td>2</td>
<td>5</td>
<td>-</td>
<td>-</td>
<td>25,000</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Non-Bank Wealth Creation Groups</td>
<td>Small</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>1</td>
<td>-</td>
<td>2</td>
<td>5</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>500</td>
<td>3</td>
</tr>
<tr>
<td>Payment Systems &amp; Service Providers</td>
<td>Small</td>
<td>2</td>
<td>-</td>
<td>2</td>
<td>5</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>5,000</td>
<td>3</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>3</td>
<td>-</td>
<td>2</td>
<td>5</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>25,000</td>
<td>3</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>Stockbrokers</td>
<td>Small</td>
<td>467</td>
<td>-</td>
<td>2</td>
<td>5</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>500</td>
<td>3</td>
</tr>
<tr>
<td>Sector</td>
<td>Sub-Sector</td>
<td>Population (IP)</td>
<td>Impacted Population (hours x pop.)</td>
<td>Understand requirements (hours x IP)</td>
<td>Implement business processes (hours x IP)</td>
<td>Implement Agreements (hours x IP)</td>
<td>Analyse CDD of partner institutions (hours x IP)</td>
<td>Suitable Customers per IP per annum</td>
<td>Old CDD requirements (hours x Cust. x IP)</td>
<td>Old CDD Requirements ($Cost x Cust. x IP)</td>
<td>Reliance model (hours x Cust. x IP)</td>
<td>Reliance model ($Cost x Cust. x IP)</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------</td>
<td>-----------------</td>
<td>-------------------------------------</td>
<td>-------------------------------------</td>
<td>-----------------------------------------</td>
<td>-----------------------------------</td>
<td>-----------------------------------------------</td>
<td>-------------------------------------</td>
<td>--------------------------------------</td>
<td>------------------------------------------</td>
<td>--------------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>Superannuation Fund Trustees</td>
<td>Small</td>
<td>50</td>
<td>2</td>
<td>10</td>
<td>-</td>
<td>-</td>
<td>2,500</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>10</td>
<td>2</td>
<td>5</td>
<td>-</td>
<td>-</td>
<td>25,000</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Trustees of Managed Investment Schemes</td>
<td>Small</td>
<td>440</td>
<td>2</td>
<td>5</td>
<td>-</td>
<td>-</td>
<td>50</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Large</td>
<td>350</td>
<td>2</td>
<td>10</td>
<td>50</td>
<td>3</td>
<td></td>
<td>15</td>
<td>1</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gambling Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Betting Agencies/TABs</td>
<td>Small</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Large</td>
<td>13</td>
<td>-</td>
<td>2</td>
<td>10</td>
<td>-</td>
<td>-</td>
<td>2,500</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Bookmakers</td>
<td>Small</td>
<td>313</td>
<td>-</td>
<td>2</td>
<td>5</td>
<td>-</td>
<td>50</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Large</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>Casinos</td>
<td>Small</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Large</td>
<td>13</td>
<td>-</td>
<td>2</td>
<td>10</td>
<td>-</td>
<td>-</td>
<td>5,000</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Pubs and Clubs</td>
<td>Small</td>
<td>3,655</td>
<td>-</td>
<td>2</td>
<td>5</td>
<td>-</td>
<td>50</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Large</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Bullion Services</td>
<td>Precious Metal Dealers</td>
<td>Small</td>
<td>100</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>50</td>
<td>3</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>Large</td>
<td>5</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>100</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
RELIANCE OPTION 3 – WITH CDD ARRANGEMENTS

<table>
<thead>
<tr>
<th>Obligation imposed or removed</th>
<th>Option</th>
<th>Impact ($)(^{17})</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Annualised one-off cost</td>
</tr>
<tr>
<td>Customer Due Diligence (CDD) -Reliance</td>
<td>3 Detailed</td>
<td>$5,362,793</td>
</tr>
</tbody>
</table>

We have assumed that all reporting entities will be required to consider the new regulatory provisions in the first instance to determine whether they suit their business model, business relationships, and customer base. All reporting entities will therefore require approximately 2 hours to interpret and consider the new provisions.

As part of our assessment, we have assumed that because the take up of reliance is not mandatory, its uptake will vary considerably between industry sectors. On this basis, we have assumed that it is:

- Likely for banks (also in the context of the Government’s Open Banking initiative) and other financial service providers, but unlikely to be utilised by small credit unions and building societies\(^{18}\) other than on a customer-by-customer basis
- Unlikely for casinos due to competition for high value or commission-based customers who are primarily domiciled overseas. Casinos do not have any corporate customers, they are all natural persons.
- Unlikely that businesses that operate in a (near-to) exclusively on-line environment, as their technology systems (including CDD) are likely to be highly automated and have minimal personal involvement.

The uptake and application of reliance depends on the size and structure of businesses, e.g.:

- Likely with global companies, corporate groups, businesses with foreign relationships and designated business groups
- Likely with businesses that have extensive existing relationships with other regulated businesses for the provision of services to common customers
- Likely with businesses that have large customer bases and customer turnover, and in particular, have a large number of corporate customers
- Likely with financial institutions that are participating in the New Payments Platform or impacted by the Government’s open-banking initiative

\(^{17}\) Timings are indicative. Positive figures are costs. Figures in brackets are savings.

\(^{18}\) Community based banking typically has a local focus and customers tend not to use the products and services of larger financial institutions
• Unlikely with small businesses and independent operators where customers are not required to open or maintain an account.

It is assumed that some businesses will not enter into a formal reliance agreement with other regulated businesses, preferring to use reliance as and when required.

This will be influenced by the size and scale of the entities involved. For example, it is assessed that the largest five banking institutions will enter into formal reliance arrangements, whereas 20 out of the remaining 94 banks may enter into these arrangements. The remainder are considered unlikely to enter into these arrangements, but may still use the expanded reliance measure as and when required. Similarly, just over half of the foreign and investment banking sector might enter into formal reliance arrangements. The assumptions recognise that some businesses will already have or are working towards having reliance style mechanisms in place through the New Payments Platform (NPP) arrangements. Under the NPP, those financial institutions that are currently using the platform for domestic transactions have agreed to trust one another in regards to the standards of CDD undertaken in regards to customers.

The estimated proportion of businesses in other cohorts in the financial sector that will adopt formal reliance arrangements is variable. For example, it is expected that no digital currency exchanges will enter into formal reliance arrangements because of the online nature of their businesses and the higher ML/TF risk of the sector. However, in the financial intermediary cohort (Financial Planners, etc.), it is expected that more than two-thirds of businesses in this sector will adopt formal reliance arrangements. These entities already have informal arrangements in place.

We have assumed an overall uptake of approximately 1630 reporting entities.

For those reporting entities who opt to utilise reliance provisions, each entity will be required to implement business processes, analyse the CDD activities of other reporting entities, and establish agreements with other reporting entities. The time required to prepare these reliance agreements and business processes will vary between reporting entities, from 5 – 20 hours, depending on the size, nature and risk profile of the sector. These would also need to be reviewed at least once every two years. It is likely that this review process would take approximately two hours.

Not all customers will be suitable for the use of reliance as part of the CDD process due to a range of factors, including the individual customer’s risk profile, or the fact that they are not customers of an institution with which a reliance agreement is in place. Reliance is also dependent on customer consent during the on-boarding process or when an existing customer takes on additional services or products. The estimated number of “suitable customers” ranges from 50,000 to 25 per reporting entity.

Cost savings have been difficult to estimate due to the gaps in understanding the effort required to verify natural persons, non-individuals and beneficial ownership, having regards to the customer base and type, size of business, frequency or volume of use, and the nature of initial customer due diligence conducted by each cohort in the regulated sector. It is assumed that CDD activities currently require a minimum of approximately
three hours to complete for a new customer, and cost approximately $15 per new customer in third-party service provider fees and database search fees. It is expected that CDD obligations under the new model will reduce the time costs to approximately 1 hour for basic information verification for natural person customers, and will reduce the third-party costs to approximately $2.50 - $3.00 for ID searches.

Therefore, it is expected that each affected entity will save approximately 2 hours in labour and $12.00 in third-party fees per new customer under this reliance model. When amplified by the number of affected reporting entities (1,630) and the number of new customers per affected reporting entity (which ranges from 50 up to 25,000 per entity), the cost savings from this initiative could be significant. It is important to note that the assumption used in this RIS are conservative, as the uptake could be higher than expected, resulting in additional affected entities and customers, and current compliance costs could be higher, resulting in higher savings per instance.
### CALCULATIONS FOR RELIANCE OPTION 3

<table>
<thead>
<tr>
<th>Sector</th>
<th>Sub-sector</th>
<th>Population</th>
<th>Impacted Population (IP)</th>
<th>Understand requirements (hours x pop.)</th>
<th>Implement business processes (hours x IP)</th>
<th>Implement Agreements (hours x IP)</th>
<th>Analyse CDD of partner institutions (hours x IP)</th>
<th>Suitable Customers per IP per annum</th>
<th>Old CDD requirements $(Cost x Cust. x IP)</th>
<th>Old CDD Requirements $(Cost x Cust. x IP)</th>
<th>Reliance model (hours x Cust. x IP)</th>
<th>Reliance model $(Cost x Cust. x IP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Services</td>
<td>Small</td>
<td>94</td>
<td>20</td>
<td>2</td>
<td>10</td>
<td>20</td>
<td>20</td>
<td>20</td>
<td>25,000</td>
<td>3</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>3</td>
<td>5</td>
<td>2</td>
<td>10</td>
<td>20</td>
<td>20</td>
<td>20</td>
<td>25,000</td>
<td>3</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>50</td>
<td>30</td>
<td>2</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>25,000</td>
<td>3</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>Remittance Dealers</td>
<td>Small</td>
<td>5,050</td>
<td>500</td>
<td>2</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td>500</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>50</td>
<td>20</td>
<td>2</td>
<td>10</td>
<td>20</td>
<td>20</td>
<td>5,000</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>2.5</td>
</tr>
<tr>
<td>Custodians</td>
<td>Small</td>
<td>109</td>
<td>-</td>
<td>2</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td>250</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>20</td>
<td>2</td>
<td>2</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td>500</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Digital Currency Exchanges</td>
<td>Small</td>
<td>115</td>
<td>-</td>
<td>2</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td>25</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>5</td>
<td>5</td>
<td>2</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td>100</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Financial Service Intermediaries</td>
<td>Small</td>
<td>1,426</td>
<td>1000</td>
<td>2</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td>50</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>50</td>
<td>40</td>
<td>2</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td>150</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Foreign Exchange Providers</td>
<td>Small</td>
<td>89</td>
<td>-</td>
<td>2</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td>250</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>20</td>
<td>5</td>
<td>2</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td>500</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Insurance Product Issuers</td>
<td>Small</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>38</td>
<td>-</td>
<td>2</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td>1000</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Non-Bank Lenders &amp; Financiers</td>
<td>Small</td>
<td>1,119</td>
<td>-</td>
<td>2</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td>10,000</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>50</td>
<td>-</td>
<td>2</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td>25,000</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Non-Bank Wealth Creation Groups</td>
<td>Small</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>1</td>
<td>-</td>
<td>2</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td>500</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Payment Systems &amp; Service Providers</td>
<td>Small</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td>25,000</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Stockbrokers</td>
<td>Small</td>
<td>467</td>
<td>-</td>
<td>2</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td>500</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>50</td>
<td>5</td>
<td>2</td>
<td>10</td>
<td>20</td>
<td>20</td>
<td>2,500</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Superannuation Fund Trustees</td>
<td>Small</td>
<td>50</td>
<td>-</td>
<td>2</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td>25,000</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>10</td>
<td>-</td>
<td>2</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>50,000</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Trustees of Managed Investment Schemes</td>
<td>Small</td>
<td>440</td>
<td>-</td>
<td>2</td>
<td>5</td>
<td>10</td>
<td>10</td>
<td>50</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>350</td>
<td>-</td>
<td>2</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>500</td>
<td>3</td>
<td>15</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>

**Gambling Services**
<table>
<thead>
<tr>
<th>Category</th>
<th>Small</th>
<th>Medium</th>
<th>Large</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Betting Agencies/TABs</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Small</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Large</td>
<td>13</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>Bookmakers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Small</td>
<td>313</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>Large</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Casinos</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Small</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Large</td>
<td>13</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>Pubs and Clubs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Small</td>
<td>3,655</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>Large</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Bullion Services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Precious Metal Dealers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Small</td>
<td>100</td>
<td>-</td>
<td>2</td>
</tr>
<tr>
<td>Large</td>
<td>5</td>
<td>-</td>
<td>2</td>
</tr>
<tr>
<td>TOTAL</td>
<td>1630</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## ATTACHMENT C: LIST OF SUBMISSIONS TO AML/CTF REVIEW

<table>
<thead>
<tr>
<th>Accounting</th>
<th>Financial planners</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australian Auditing and Accounting Public Policy Committee</td>
<td>Mr Ashok Sherwal</td>
</tr>
<tr>
<td><strong>AML compliance</strong></td>
<td>Financial Planning Association of Australia</td>
</tr>
<tr>
<td>AML Master</td>
<td><strong>Gaming services industry</strong></td>
</tr>
<tr>
<td>GRC Institute</td>
<td>Australian Bookmakers’ Association Pty Ltd</td>
</tr>
<tr>
<td><strong>Banking</strong></td>
<td>Australian Hotel Association</td>
</tr>
<tr>
<td>Australian Bankers Association</td>
<td>Australian Wagering Council</td>
</tr>
<tr>
<td>Australian Finance Conference</td>
<td>Casinos and Resorts Australasia</td>
</tr>
<tr>
<td>Australian Financial Markets Association</td>
<td>Clubs NSW/Clubs Australia</td>
</tr>
<tr>
<td>Customer Owned Banking Association</td>
<td>Mercury Group Victoria Inc</td>
</tr>
<tr>
<td>HSBC Australia Limited</td>
<td>Peter Shepherd</td>
</tr>
<tr>
<td>1 confidential submission</td>
<td>One confidential submission</td>
</tr>
<tr>
<td><strong>Cash-in-transit</strong></td>
<td><strong>Government (confidential)</strong></td>
</tr>
<tr>
<td>Australian Security Industry Association Limited</td>
<td>Australian Crime Commission (two submissions)</td>
</tr>
<tr>
<td>Mr Rick &amp; Ms Anna Biela</td>
<td>Australian Customs and Border Protection Service</td>
</tr>
<tr>
<td>Security Specialists Australia</td>
<td>Australian Federal Police</td>
</tr>
<tr>
<td>2 confidential submissions</td>
<td>Australian Security intelligence Organisation</td>
</tr>
<tr>
<td>SNP Security</td>
<td>Australian Taxation Office (two submissions)</td>
</tr>
<tr>
<td><strong>Individuals and academia</strong></td>
<td>Cyber &amp; Identity Security Policy Branch, Attorney-General’s Department</td>
</tr>
<tr>
<td>Ms Anne Imobersteg Harvey</td>
<td>Department of Foreign Affairs and Trade</td>
</tr>
<tr>
<td>One confidential submission</td>
<td>Department of Human Services</td>
</tr>
<tr>
<td>Mr Douglas Allen</td>
<td>Inspector General of Intelligence and Security</td>
</tr>
<tr>
<td>Faculty of Law, University of New South Wales</td>
<td>NSW Crime Commission</td>
</tr>
<tr>
<td>Mr Michael Robson</td>
<td>NSW Police Integrity Commission</td>
</tr>
<tr>
<td>Professor Louis de Koker and Mr Kayne Harwood</td>
<td>Office of the Australian information Commissioner</td>
</tr>
<tr>
<td><strong>Legal</strong></td>
<td>Treasury</td>
</tr>
<tr>
<td>Financial Services Committee, Law Council of Australia</td>
<td><strong>Lenders</strong></td>
</tr>
<tr>
<td>One confidential submission</td>
<td>Capricorn Society Limited</td>
</tr>
<tr>
<td>Law Council of Australia</td>
<td>Mortgage &amp; Finance Association of Australia</td>
</tr>
<tr>
<td><strong>Remitters</strong></td>
<td>National Financial Services Federation Ltd</td>
</tr>
<tr>
<td>Capital Money Exchange Pty Ltd (confidential)</td>
<td>SP AusNET</td>
</tr>
<tr>
<td>Eastern &amp; Allied Pty Ltd/Hai Ha Money Transfer</td>
<td><strong>Managed investment schemes</strong></td>
</tr>
<tr>
<td>Kapruka Pty Ltd</td>
<td>Fawkner Property Pty Ltd</td>
</tr>
<tr>
<td>MoneyGram Payment Systems Inc.</td>
<td>Fundhost Limited</td>
</tr>
<tr>
<td>Western Union</td>
<td><strong>New payment methods</strong></td>
</tr>
<tr>
<td><strong>Salary packaging</strong></td>
<td>Mr Kevin Beck (three submissions)</td>
</tr>
<tr>
<td>McMillan Shakespeare Group</td>
<td>PayPal Australia Pty Ltd (appendices confidential)</td>
</tr>
<tr>
<td><strong>Superannuation</strong></td>
<td>Universal Gift Cards Pty Ltd</td>
</tr>
<tr>
<td>Association of Superannuation Funds of Australia Limited</td>
<td></td>
</tr>
<tr>
<td>Australian Institute of Superannuation Trustees</td>
<td></td>
</tr>
<tr>
<td>Financial Services Council</td>
<td></td>
</tr>
<tr>
<td>----------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Technology providers</strong></td>
<td></td>
</tr>
<tr>
<td>iSignthis Ltd (White Paper confidential)</td>
<td></td>
</tr>
<tr>
<td>One confidential submission</td>
<td></td>
</tr>
<tr>
<td><strong>NGOs</strong></td>
<td></td>
</tr>
<tr>
<td>Australian Privacy Foundation and Privacy International</td>
<td></td>
</tr>
<tr>
<td>Transparency International Australia</td>
<td></td>
</tr>
<tr>
<td>Uniting Church in Australia Synod of Victoria and Tasmania</td>
<td></td>
</tr>
</tbody>
</table>
# ATTACHMENT D: STAKEHOLDER ENGAGEMENT

<table>
<thead>
<tr>
<th>ROUNDTABLE DATE</th>
<th>PARTICIPANTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>19 September 2015</td>
<td><strong>NGO sector</strong>&lt;br&gt;Uniting Church in Australia, Synod of Victoria and Tasmania&lt;br&gt;Transparency International Australia&lt;br&gt;Australian Council for International Development&lt;br&gt;OXFAM</td>
</tr>
<tr>
<td></td>
<td><strong>Gaming sector: Gaming machines</strong>&lt;br&gt;Australian Hotels Association&lt;br&gt;ClubsNSW&lt;br&gt;Mercury Group Victoria Inc&lt;br&gt;ALH Group Pty Ltd</td>
</tr>
<tr>
<td></td>
<td><strong>Gaming sector: Casinos</strong>&lt;br&gt;Casinos and Resorts Australasia</td>
</tr>
<tr>
<td></td>
<td><strong>Gaming sector: Wagering</strong>&lt;br&gt;Australian Wagering Council&lt;br&gt;Australian Bookmakers Association Limited&lt;br&gt;TattsGroup</td>
</tr>
<tr>
<td></td>
<td><strong>Cash-in-transit sector</strong>&lt;br&gt;Australian Security Industry Association Limited&lt;br&gt;Linfox Armaguard&lt;br&gt;Prosegur</td>
</tr>
<tr>
<td>24 September 2015</td>
<td><strong>Gaming sector: Gaming machines</strong>&lt;br&gt;Australian Hotels Association&lt;br&gt;ClubsNSW&lt;br&gt;Mercury Group Victoria Inc&lt;br&gt;ALH Group Pty Ltd</td>
</tr>
<tr>
<td></td>
<td><strong>Gaming sector: Casinos</strong>&lt;br&gt;Casinos and Resorts Australasia</td>
</tr>
<tr>
<td></td>
<td><strong>Gaming sector: Wagering</strong>&lt;br&gt;Australian Wagering Council&lt;br&gt;Australian Bookmakers Association Limited&lt;br&gt;TattsGroup</td>
</tr>
<tr>
<td></td>
<td><strong>Cas-in-transit sector</strong>&lt;br&gt;Australian Security Industry Association Limited&lt;br&gt;Linfox Armaguard&lt;br&gt;Prosegur</td>
</tr>
<tr>
<td>25 September 2015</td>
<td><strong>Remittance sector: Large remitters</strong>&lt;br&gt;Western Union</td>
</tr>
<tr>
<td></td>
<td><strong>Remittance sector: Small/medium remitters</strong>&lt;br&gt;UAE Exchange&lt;br&gt;Hai Ha&lt;br&gt;MoneyGram&lt;br&gt;OzForex Group&lt;br&gt;RIA</td>
</tr>
<tr>
<td></td>
<td><strong>AML compliance sector</strong>&lt;br&gt;AML Master</td>
</tr>
<tr>
<td></td>
<td><strong>2 October 2015</strong>&lt;br&gt;<strong>AML compliance sector</strong>&lt;br&gt;Yarra Valley Associates</td>
</tr>
<tr>
<td>26 September 2015</td>
<td><strong>Banking sector: Australian Finance Conference</strong>&lt;br&gt;Australian Finance Conference&lt;br&gt;Toyota Finance Australia Limited&lt;br&gt;Pepper Group&lt;br&gt;Marubeni Equipment Finance</td>
</tr>
<tr>
<td></td>
<td><strong>Banking sector: Australian Banking Association</strong>&lt;br&gt;Australian Bankers’ Association&lt;br&gt;Commonwealth Bank of Australia&lt;br&gt;Macquarie&lt;br&gt;Westpac&lt;br&gt;ANZ&lt;br&gt;ING Direct&lt;br&gt;HSBC</td>
</tr>
<tr>
<td></td>
<td><strong>19 November 2014</strong>&lt;br&gt;<strong>Banking sector: Australian Financial Markets Association</strong>&lt;br&gt;Australian Financial Markets Association&lt;br&gt;Western Union&lt;br&gt;Bank of America Merrill Lynch&lt;br&gt;Westpac</td>
</tr>
<tr>
<td>ROUNDTABLE DATE</td>
<td>PARTICIPANTS</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------</td>
</tr>
</tbody>
</table>
|                 | Morgan Stanley  
|                 | ANZ           
|                 | NAB           
|                 | UBS           
|                 | AMP           |

**Banking sector: Financial Services Council**
- Financial Services Council
- BT Financial Group
- HWL Ebsworth
- K&L Gates
- Schroders
- Perpetual
- Commonwealth Bank
- Minter Ellison Lawyers
- Bell Asset Management
- Vanguard
- KPMG

**Banking sector: Customer Owned Banking Association**
- Customer Owned Banking Association
- Teachers Mutual Bank
- Maritime, Mining & Power Credit Union
- Heritage Bank
- Community First Credit Union
- Greater Building Society
- The University Credit Society
- People’s Choice Credit Union
- Bankmecu
- Beyond Bank
- Victoria Teachers Mutual Bank

**17 December 2015**

**New payment methods**
- PayPal

**28 January 2015**

**Government agencies**
- Australian Crime Commission
- Australian Federal Police
- Attorney-General’s Department
- Australian Security and Intelligence Organisation
- Australian Taxation Office
- Australian Transaction Reports and Analysis Centre
- Department of Foreign Affairs and Trade
- Department of Human Services
- Department of Immigration and Border Protection
- Australian Customs and Border Protection Service
- Inspector-General of Intelligence and Security
- Office of the Australian Information Commissioner
- Treasury
- NSW Crime Commission