2016 - 2017

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING AMENDMENT BILL 2017

EXPLANATORY MEMORANDUM

Circulated by authority of the
Minister for Justice, the Hon Michael Keenan MP

ACRONYMS

AML/CTF	Anti-money laundering and counter-terrorism financing
AML/CTF Act	*Anti-Money Laundering and Counter-Terrorism Financing Act 2006*
AML/CTF Rules	*Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)*
APP	Australian Privacy Principles
AUSTRAC	Australian Transaction Reports and Analysis Centre
AUSTRAC CEO	Chief Executive Officer of the Australian Transaction Reports and Analysis Centre
BNI	Bearer negotiable instrument
DBG	Designated business group
FATF	Financial Action Task Force
FTR Act	*Financial Transaction Reports Act 1988*
ICCPR	*International Covenant on Civil and Political Rights*
ML	Money laundering
SVC	Stored value card
TF	Terrorism financing

ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING AMENDMENT BILL 2017

GENERAL OUTLINE

1. This Bill amends the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) and the *Financial Transaction Reports Act 1988* (FTR Act).

2. The Bill implements a first phase of reforms arising from the recommendations of the *Report on the Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and Associated Rules and Regulations* (the Report). The Minister for Justice, the Hon Michael Keenan MP, tabled the Report in the Parliament on 29 April 2016.

3. The AML/CTF Act and FTR Act provide the basis for regulation of certain businesses 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 and FTR 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 designated agencies, non-designated Commonwealth agencies and AUSTRAC's international counterparts in order to combat money laundering (ML), terrorism financing (TF) and other serious crimes.

4. The Bill contains a range of measures to strengthen Australia's capabilities to address ML and TF risks, and generate regulatory efficiencies, including amendments to:

- expand the objects of the AML/CTF Act to reflect the domestic objectives of AML/CTF regulation
- close a regulatory gap by regulating digital currency exchange providers
- provide regulatory relief to industry by:
    - clarifying due diligence obligations relating to correspondent banking relationships and broadening the scope of these relationships
    - de-regulating the cash-in-transit sector, insurance intermediaries and general insurance providers
    - qualifying the term 'in the course of carrying on a business', and
    - allowing related bodies corporate to share information
- strengthen AUSTRAC's investigation and enforcement powers by:
    - giving the AUSTRAC CEO the power to issue infringement notices for a greater range of regulatory offences, and
    - allowing the AUSTRAC CEO to issue a remedial direction to a reporting entity to retrospectively comply with an obligation that has been breached

- give police and customs officers broader powers to search and seize physical currency and bearer negotiable instruments (BNI) and establish civil penalties for failing to comply with questioning and search powers

- revise the definitions of 'investigating officer', 'signatory' and 'stored value card'(SVC) in the AML/CTF Act, and

- clarify other regulatory matters, including:

    - granting the AUSTRAC CEO a power to perform tasks that are necessary or incidental to his or her functions, and

    - the weight given to ML and TF risk in certain decisions made by the AUSTRAC CEO.

5. The Bill also expands the rule-making powers of the 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.

FINANCIAL IMPACT

6. The Bill will be implemented within existing resources.

REGULATION IMPACT STATEMENT

7. A Regulation Impact Statement has been developed in relation to the Bill. The Regulation Impact Statement is at **Annex A**.

8. The overall financial impact of the Bill is estimated to be savings to industry each year for the ten years after the measures come into force totalling $36,086,393.

9. This financial impact includes average annual regulatory costs of $662,221 for business and community organisations arising from measures to regulate digital currency exchange providers. The financial impact also includes offsets for each year for the ten years after the measures come into force arising from measures to:

- deregulate the cash-in-transit sector (total annual offset of $32,683,251)

- clarify correspondent banking relationships (total annual offset of $9,028)

- allow related bodies corporate to share information (total annual offset of $3,987,549), and

- de-regulate insurance intermediaries and general insurance providers under the FTR Act (total annual offset of $68,786).

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 Bill 2017

10. This 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

11. The Bill amends the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) and the *Financial Transaction Reports Act 1988* (FTR Act).

12. The Bill implements a first phase of reforms arising from the recommendations of the *Report on the Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and Associated Rules and Regulations* (the Report).
The Minister for Justice, the Hon Michael Keenan MP, tabled the Report on the statutory review in the Parliament on 29 April 2016.

13. The AML/CTF Act and FTR Act provide 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 in and outbound travellers about the movement of money and other assets. AUSTRAC shares this information and associated financial intelligence with designated agencies in an effort to combat money laundering (ML), terrorism financing (TF) and other serious crimes.

14. The Bill contains a range of measures to strengthen Australia's capabilities to address ML and TF risks, and generate regulatory efficiencies, including amendments to:

- expand the objects of the AML/CTF Act to reflect the domestic objectives of AML/CTF regulation
- close a regulatory gap by regulating digital currency exchange providers
- provide regulatory relief to industry by:
    - clarifying due diligence obligations relating to correspondent banking relationships and broadening the scope of these relationships
    - de-regulating the cash-in-transit sector, insurance intermediaries and general insurance providers
    - qualifying the term 'in the course of carrying on a business', and
    - allowing related bodies corporate to share information

- strengthen AUSTRAC's investigation and enforcement powers by:
    - giving the AUSTRAC CEO the power to issue infringement notices for a greater range of regulatory offences, and
    - allowing the AUSTRAC CEO to issue a remedial direction to a reporting entity to retrospectively comply with an obligation that has been breached
- give police and customs officers broader powers to search and seize physical currency and bearer negotiable instruments (BNI) and establish civil penalties for failing to comply with questioning and search powers
- revise the definitions of 'investigating officer', 'signatory' and 'stored value card' in the AML/CTF Act, and
- clarify other regulatory matters, including:
    - granting the AUSTRAC CEO a power to perform tasks that are necessary or incidental to his or her functions, and
    - the weight given to ML and TF risk in certain decisions made by the AUSTRAC CEO.

Human rights implications

15. This Bill engages the following human rights:

- the right to privacy in Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR), and
- the right to the presumption of innocence in Article 14(2) of the ICCPR.

Right to privacy

16. This Bill engages the right to privacy in Article 17 of the ICCPR by:

- closing a regulatory gap by regulating digital currency exchange providers
- allowing related bodies corporate to share information, and
- giving police and customs officers broader powers to search and seize physical currency and BNIs.

17. Article 17 of the ICCPR provides that no-one shall be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence. Lawful interference with the right to privacy is permitted under Article 17 of the ICCPR, provided it is not arbitrary. In order for an interference with the right to privacy to be permissible, the interference must be authorised by law, be for a reason consistent with the ICCPR and be reasonable in the particular circumstances. The United Nations Human Rights Committee has interpreted the requirement of 'reasonableness' to imply that any interference with privacy must be proportional to the end sought and be necessary in the circumstances.

18. To the extent that the measures in the Bill limit the rights protected under Article 17 of the ICCPR, these limitations are not arbitrary, and are reasonable, necessary and proportionate to the achievement of legitimate objectives by strengthening Australia's AML/CTF framework.

19. The human rights implications of these measures are discussed in turn below.

Close a regulatory gap by regulating digital currency exchange providers

20. Digital currencies largely operate outside the scope of the regulated financial system and are becoming a popular method of paying for goods and services and transferring value in the Australian economy.[1]

21. While digital currencies offer the potential for cheaper, more efficient and faster payments, the associated ML and TF risks are well-documented. Key risks include:

- greater anonymity compared with traditional non-cash payment methods
- limited transparency because transactions are made on a peer-to-peer basis, generally outside the regulated financial system, and
- different components of a digital currency system may be located in many countries and subject to varying degrees of AML/CTF oversight.

22. Digital currency exchange providers are not currently regulated under the AML/CTF Act. The regulatory regime under the AML/CTF Act only applies to an 'e-currency' which is backed by a physical thing and excludes convertible digital currencies, such as Bitcoin, which are backed by a cryptographic algorithm.

23. In June 2015, the Financial Action Task Force (FATF)[2] released guidance on how countries can apply a risk-based approach to address the ML and TF risks associated with digital currency payment products and services. The guidance provides that countries should consider applying the FATF standards to convertible digital currency exchanges and any other types of institution that act as nodes where convertible digital currency activities intersect with the regulated financial system. This includes:

- requiring convertible digital currency exchanges to conduct customer due diligence, keep transaction records and make suspicious matter reports
- applying registration/licensing requirements to domestic entities providing convertible digital currency exchange services between digital currencies and money, and
- subjecting domestic entities providing convertible digital currency exchange services to adequate supervision and regulation.

[1] Digital currencies can be divided into two basic types: convertible and non-convertible. Convertible digital currencies can be readily exchangeable for money, either centralised with a central administering authority or decentralised. Non-convertible digital currency is not readily exchangeable for money and is restricted to a centralised or 'closed-loop' environment, such as Flybuys and game credits or money issued by massively-multiplayer online role-playing games.

[2] The FATF is the global standard-setting body for combating money laundering and the financing of terrorism & proliferation. Its website is at www.fatf-gafi.org.

24. Based on this FATF guidance and broader international developments, the Report recommends that new regulation should focus on digital currency exchanges, as this is the point of intersection between digital currencies and the regulated financial system.

25. The amendments to the AML/CTF Act in Part 2 of Schedule 1 to the Bill will apply AML/CTF regulation to businesses which exchange digital currencies for money.

26. In particular, digital currency exchange providers will be required to:

- enrol and register on the Digital Currency Exchange Register maintained by AUSTRAC and provide prescribed registration details
- adopt and maintain an AML/CTF program to identify, mitigate and manage the ML and TF risks they may face
- identify and verify the identities of their customers
- report suspicious matters and transactions involving physical currency that exceed $10,000 or more (or foreign equivalent) to AUSTRAC, and
- keep certain records related to transactions, customer identification and their AML/CTF program for seven years.

27. Overall, the measures in the Bill extend Australia's existing AML/CTF regime to close a regulatory gap in relation to a small number of businesses involved in providing digital currency exchange services. Closing this regulatory gap will reduce the ML and TF risks associated with the growth of the digital currency sector and provide vital financial intelligence to AUSTRAC in its ongoing efforts to combat ML and TF.

28. This regulatory gap is also currently having an impact on the standing and public perception of the legitimacy of the digital currency sector, with some businesses choosing not to use or accept this payment method because of concerns about the risks associated with dealing with digital currency. Continued non-regulation of digital currency exchange providers under the AML/CTF regime may impede the development or use of these currencies in the future and the growth of this sector and may also increase the likelihood that the sector could by targeted for nefarious purposes.

29. As a result of the amendments in this Bill, businesses which convert digital currency to money will have to collect and store personal information, and report certain transactions to AUSTRAC. This reporting process will occur in accordance with the existing requirements of the AML/CTF Act. Some of this information may then be compiled, analysed and disseminated by AUSTRAC as actionable financial intelligence to authorised government agencies and international counterparts to aid ongoing efforts to combat and disrupt ML and TF, and other serious crimes.

30. To the extent that these measures limit the rights protected under Article 17 of the ICCPR, these limitations are not arbitrary, and are reasonable, necessary and proportionate to achieve legitimate objectives. This modest extension of Australia's AML/CTF regime is for legitimate objectives – minimising the ML and TF risks associated with the growing use of digital currencies in the Australian economy, strengthening the standing and public

perception of the legitimacy of the digital currency sector and fulfilling Australia's ongoing international obligations to combat ML and TF.

31. Similarly, although the amendments will result in the collection and storage of personal information, all reporting entities under Australia's AML/CTF regime are obliged to comply with the Australian Privacy Principles (APP). Disclosure of personal information to government officials will also be subject to strict existing safeguards. In particular, Part 11 of the AML/CTF Act will continue to provide strict controls on the use and disclosure of AUSTRAC information. In essence, the AML/CTF Act prohibits the disclosure of AUSTRAC information, regardless of the type or format, unless a specified exception applies.

Allow related bodies corporate to share information

32. The Report concludes that the definition of 'designated business group' (DBG) is too restrictive, prohibiting the sharing of information within a corporate group to manage the ML and TF risks associated with a common customer. In order to rectify this deficiency, and to ensure that the group construct under the AML/CTF regime better reflects the reality of business structures, recommendation 7.5 of the Report recommends replacing the concept of a DBG with the concept of a 'corporate group'.

33. A DBG is a group of two or more associated businesses or persons who are reporting entities and join together to share certain obligations under the AML/CTF Act. Importantly, reporting entities can share information about SMRs with fellow members of their DBG to manage their ML and TF risks without breaching the tipping-off provisions in the AML/CTF Act. DBGs may include a range of business types, including lawyers, accountants, joint ventures and reporting entities that provide designated remittance services.

34. Items 51-55 in Part 4 of Schedule 1 to the Bill amend Part 11 of the AML/CTF Act to supplement the concept of a DBG with the concept of a 'corporate group', as defined in accordance with the definition of 'related bodies corporate' under section 50 of the *Corporations Act 2001*. This amendment will allow businesses to share information within a 'corporate group' as well as within a DBG to manage their ML and TF risks associated with common customers – without breaching the tipping-off provisions in the AML/CTF Act. Supplementing, rather than replacing, the concept of the DBG will ensure that businesses that fall within the DBG concept, but may not fall within the definition of 'corporate group' (for example, businesses acting under partnership or mixed arrangements), can continue to share information for the purposes of Part 11 of the AML/CTF Act.

35. The proposed amendments engage the right to privacy in Article 17 of the ICCPR. However, they are introduced for a reason consistent with the ICCPR because they concern the limited sharing of information about potentially criminal or terrorism-related activity, and therefore promote the interests of national security and public order. The measures are proportionate because they merely amend Australia's AML/CTF regime to ensure that it conforms with the realities of modern business structures, do not constitute a radical departure from current information-sharing practices under the AML/CTF regime and assist to ensure that Australia's AML/CTF framework remains robust in the face of the threat of serious crime and terrorism.

36. The measures in Items 51-55 of the Bill are also proportionate, as all reporting entities under the AML/CTF regime are subject to the APPs and are obliged to protect sensitive personal information.

37. For these reasons the measures in Items 51-55 of the Bill represent a reasonable, necessary and proportionate interference with the right to privacy.

Give police and customs officers broader powers to search and seize physical currency and bearer negotiable instruments

38. Police and customs officers do not currently have general search and seizure powers at the border under the AML/CTF Act. Instead, the search and seizure powers under the AML/CTF Act are linked to breaches of the current cross-border reporting requirements, which require travellers to declare physical currency of $10,000 or more and declare, on being questioned, if they are carrying a BNI. This leaves gaps in the ability of police and customs officers to search and seize physical currency and BNIs under the AML/CTF Act where officers have a suspicion that funds or instruments may be linked to ML, TF or other serious crimes, but the person has not breached the reporting requirements in Part 4 of the AML/CTF Act.

39. Recommendation 12.4 of the Report recommends removing this gap and broadening the search and seizure powers under sections 199 and 200 of the AML/CTF Act to allow police and customs officers to search and seize physical currency and BNIs where there is:

(a) a suspicion of ML, TF or other serious criminal offences, or

(b) a breach of the cross-border reporting requirements under the AML/CTF Act.

40. Items 67-75 of the Bill amend the AML/CTF Act to implement this recommendation.

41. The proposed amendments engage the right to privacy in Article 17 of the ICCPR. However, the proposed amendments are consistent with the ICCPR because they concern the power to seize physical currency and BNIs that are suspected to be relevant to criminal or terrorism-related conduct and therefore promote the interests of national security and public order. The new powers will also only be exercised by duly authorised police and customs officers in relation to certain persons who are imminently departing or recently arrived in Australia and specified conveyances such as aircraft and ships.

42. The measures are proportionate because they broaden existing powers in order to deter ML and TF, do not constitute a radical departure from current search and seizure powers and assist authorities in ensuring that Australia's AML/CTF framework is robust in the face of the threat of serious crime and terrorism.

43. For these reasons the measures in Items 67-75 of the Bill represent a reasonable, necessary and proportionate interference with the right to privacy, as permitted under Article 17 of the ICCPR.

Presumption of innocence

44. This Bill engages the right to the presumption of innocence in Article 14(2) of the ICCPR by introducing strict liability offences for conduct related to providing a digital

currency exchange service. Article 14(2) of the ICCPR provides that a person charged with a criminal offence has a right 'to be presumed innocent until proven guilty according to law.' Strict liability offences engage article 14(2) because, where strict liability is applied to an offence, the requirement for the prosecution to prove fault is removed and a defence of honest and reasonable mistake of fact may be raised. Strict liability provisions will not violate the presumption of innocence so long as they are reasonable in the circumstances and maintain rights of defence.

45. The offences and the strict liability components of the offences in Part 2 of Schedule 1 of the Bill are not inconsistent with the presumption of innocence because they are reasonable, necessary and proportionate in the pursuit of a legitimate objective. The offences will provide an effective enforcement mechanism for the regulation of digital currency exchange providers. Notably, each offence retains a fault element of recklessness regarding the requirements under either subsections 76A(1) or 76A(2) of the Bill. Requiring proof of fault for all the physical elements of the offences would undermine the deterrent effect of these provisions because it would allow for entities to argue that they did not know or were reckless as to whether they had obligations under the Act.

46. Section 9.2 of the Criminal Code allows a defence of honest and reasonable mistake of fact to be raised for strict liability offences. Under this defence, a defendant must turn his or her mind to the existence of the facts and be under a mistaken, but reasonable, belief about those facts. This defence would be applicable to the strict liability provisions in the Bill.

47. The offences and the strict liability components of the offences in Part 2 of Schedule 1 of the Bill contribute to the legitimate objectives of the Bill – namely, to minimise the ML and TF risks associated with the growing use of digital currencies in the Australian economy, strengthen the standing and public perception of the legitimacy of the digital currency sector and fulfil Australia's ongoing international obligations to combat ML and TF. A robust enforcement framework is necessary to ensure that digital currency exchange providers are registered in timely manner so as to reduce the risk of their exploitation for ML, TF and other serious crime.

48. For these reasons, the strict liability offences in Item 20 of the Bill are not inconsistent with the presumption of innocence and are reasonable, necessary and proportionate in pursuit of a legitimate objective.

Conclusion

49. While the Bill engages a range of human rights, to the extent that it limits some rights, those limitations are reasonable, necessary and proportionate in achieving a legitimate objective.

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 Amendment Act 2017* (the Act).

Clause 2 – Commencement

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

3. Subclause 2(1) provides that each provision of this 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. The table provides that the whole of this Act commences 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 Act receives the Royal Assent, they commence on the day after the end of that period.

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

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

Clause 3 – Schedules

7. 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—Objects of the Act

8. Part 1 makes amendments to the AML/CTF Act to expand the objects of the AML/CTF Act.

9. Section 3 of the AML/CTF Act sets out the objects of the AML/CTF Act. The current objects focus on compliance with the international standards for combating ML, TF and other international obligations.

10. The Report recommends including additional objects to articulate the domestic objectives of AML/CTF regulation. Expanding the objects in this manner will more clearly articulate the policy intent of the legislation and assist in the interpretation of specific provisions.

Anti-Money Laundering and Counter Terrorism Financing Act 2006

Item 1 – Before paragraph 3(1)(a)

11. Item 1 inserts new paragraphs 3(1)(aa), 3(1)(ab), 3(1)(ac) and 3(1)(ad) to provide four new objects of the AML/CTF Act. These additional objects articulate the intent of AML/CTF regulation at the domestic level and are examples of mechanisms that implement Australia's international obligations in reliance on the external affairs power. They do not expand, or alter, the constitutional basis for the AML/CTF Act.

12. Paragraph 3(1)(aa) provides that it is an object of the AML/CTF Act to provide for measures to detect, deter and disrupt ML, TF, and other serious financial crimes.

13. Paragraph 3(1)(ab) provides that it is an object of the AML/CTF Act to provide relevant Australian government bodies and their international counterparts with the information they need to investigate and prosecute ML offences, offences constituted by TF, and other serious crimes.

14. Paragraph 3(1)(ac) provides that it is an object of the AML/CTF Act to support cooperation and collaboration among reporting entities, AUSTRAC and other government agencies, particularly law enforcement agencies, to detect, deter and disrupt ML, TF, and other serious crimes.

15. Paragraph 3(1)(ad) provides that it is an object of the AML/CTF Act to promote public confidence in the Australian financial system through the enactment and implementation of controls and powers to detect, deter and disrupt ML, TF and other serious crimes.

Part 2—Digital currencies

16. Part 2 closes a regulatory gap that has emerged since the AML/CTF Act was enacted in 2006 by expanding AML/CTF regulation to digital currency exchange providers.

17. Digital currencies largely operate outside the scope of the regulated financial system and are growing in popularity as a method of paying for goods and services and transferring value in the Australian economy.[3]

18. While digital currencies offer the potential for cheaper, more efficient and faster payments, the associated ML and TF risks are well-documented. Key risks include:

- greater anonymity compared with traditional non-cash payment methods
- limited transparency because transactions are made on a peer-to-peer basis, generally outside the regulated financial system, and
- different components of a digital currency system may be located in many countries and subject to varying degrees of AML/CTF oversight.

19. Digital currency exchange providers are not currently regulated under the AML/CTF Act. The regulatory regime under the AML/CTF Act currently only applies to an 'e-currency' which is backed by a physical thing and excludes convertible digital currencies which are backed by a cryptographic algorithm.

20. In June 2015, the Financial Action Task Force (FATF)[4] released guidance on how countries can apply a risk-based approach to address the ML and TF risks associated with digital currency payment products and services. The guidance provides that countries should consider applying the FATF standards to convertible digital currency exchanges and any other types of institution that act as nodes where convertible digital currency activities intersect with the regulated financial system. This includes:

- requiring convertible digital currency exchanges to conduct customer due diligence, keep transaction records, and make suspicious matter reports
- applying registration/licensing requirements to domestic entities providing convertible digital currency exchange services between digital currencies and money, and
- subjecting domestic entities providing convertible digital currency exchange services to adequate supervision and regulation.

[3] Digital currencies can be divided into two basic types: convertible and non-convertible. Convertible digital currencies can be readily exchangeable for money, either centralised with a central administering authority or decentralised. Non-convertible digital currency is not readily exchangeable for money and is restricted to a centralised or 'closed-loop' environment, such as Flybuys and game credits or money issued by massively-multiplayer online role-playing games.

[4] The FATF is the global standard-setting body for combating money laundering and the financing of terrorism & proliferation. Its website is at www.fatf-gafi.org.

21. Based on this FATF guidance and broader international developments, recommendations 4.9 and 4.10 of the Report recommend that the AML/CTF Act be amended to:

- expand the definition of e-currency to include convertible digital currencies not backed by a physical 'thing', and
- regulate activities relating to convertible digital currency, particularly activities undertaken by digital currency exchange providers.

22. The amendments to the AML/CTF Act in Part 2 of Schedule 1 to the Bill will apply AML/CTF regulation to businesses which exchange digital currencies for money.

23. In particular, digital currency exchange providers will be required to:

- enrol and register on the Digital Currency Exchange Register maintained by AUSTRAC and provide prescribed registration details
- adopt and maintain an AML/CTF program to identify, mitigate and manage the ML and TF risks they may face
- identify and verify the identities of their customers
- report suspicious matters, and transactions involving physical currency that exceed $10,000 or more (or foreign equivalent) to AUSTRAC, and
- keep certain records related to transactions, customer identification and their AML/CTF program for seven years.

Anti-Money Laundering and Counter-Terrorism Financing Act 2006

Item 2 – Section 4

24. Item 2 amends the simplified outline of the AML/CTF Act in section 4 to insert a reference to the new requirement for providers of registrable digital currency exchange services to register with the AUSTRAC CEO. As outlined below, this requirement is similar to the requirement for providers of registrable designated remittance services or registrable remittance network services to register with the AUSTRAC CEO.

Item 3 – Section 5

25. Item 3 inserts a new definition into section 5 of the AML/CTF Act to define the term 'digital currency'. The definition of digital currency replaces, and is broader than, the previous definition of e-currency (which is repealed in Item 4 of the Bill and only related to internet-based, electronic means of exchange backed by precious metal, bullion or another prescribed thing). Digital currency encompasses all things formerly referred to as 'e-currency'.

26. The definition of digital currency covers a digital representation of value that meets the following specified criteria:

- consistent with the general understanding of currency, it must function as a medium of exchange, a store of economic value, or a unit of account

- it must not be issued by or under the authority of a government body, drawing a clear distinction between digital currencies and money (discussed below at paragraph 31)

- it must be interchangeable with money (including through the crediting of an account) and may be used as consideration for the supply of goods or services, and

- it must be generally available to members of the public without any restriction on its use as consideration.

27. The last two criteria above exclude such things as loyalty programs (e.g. frequent flyer programs) where points may not be redeemed as money, and game money or credits issued by the operators of massively-multiplayer online role-playing games where its use is limited to a specific community.

28. Item 3 gives the AUSTRAC CEO power to make AML/CTF Rules to expand or narrow the scope of the digital currency definition. This recognises that the concept of digital currency is likely to continue to evolve and the AML/CTF regulation of digital currencies will need to be responsive to mitigate emergent risks.

29. Item 3 also provides that 'Digital Currency Exchange Register' has the meaning given by section 76B.

Item 4 – Section 5 (definition of *e-currency*)

30. Item 4 repeals the definition of 'e-currency', which has been replaced by the broader definition of 'digital currency'.

Item 5 – Section 5 (paragraph (c) of the definition of *money*)

Item 6 – Section 5 (paragraph (d) of the definition of *money*)

Item 7 – Section 5 (definition of *precious metal*)

Item 8 – Section 5 (definition of *property*)

31. Items 5 to 8 amend the definition of 'money', repeal the definition of 'precious metal', and amend the definition of 'property'. These amendments are consequential to the repeal of the definition of e-currency and give effect to the new definition of digital currency. It should be noted that digital currency does not fall within the amended definition of money or property, reflecting the different obligations under the AML/CTF Act that apply to digital currency and money. The term 'precious metal' was only used in reference to the repealed e-currency definition.

Item 9 – Section 5

Item 10 – Section 5 (definition of *registration*)

32. Items 9 and 10 insert the definitions of 'registered digital currency exchange provider' and 'registrable digital currency exchange service' and amend the definition of 'registration'

in section 5 to reflect the introduction of the requirement for registrable digital currency exchange providers to register with the AUSTRAC CEO.

Item 11 – Section 5 (paragraph (b) of the definition of *threshold transaction*)

Item 12 – Section 5 (after paragraph (c) of the definition of *threshold transaction)*

Item 13 – Section 5 (definition of *threshold transaction*)

33. Item 11 repeals a reference to e-currency in the definition of 'threshold transaction' in section 5. Transactions involving digital currency will only trigger threshold transaction reporting obligations under section 43 of the AML/CTF Act where they also involve an amount of physical currency that is not less than $10,000. However, Item 12 provides that the definition of threshold transaction can also apply to a specified transaction involving digital currency of a value specified in regulations. This provision recognises that the concept of digital currency will likely continue to evolve and the AML/CTF regulation of digital currencies will need to be responsive to mitigate emergent risks.

34. Item 13 is a consequential amendment related to the removal of paragraph (b) of the definition of threshold transaction.

Item 14 - Section 5 (note 2 at the end of the definition of *threshold transaction*)

35. Item 14 repeals a reference to e-currency in the definition of threshold transaction in section 5. Transactions involving digital currency will only trigger threshold transaction reporting obligations under section 43 of the AML/CTF Act where they also involve an amount of physical currency that is not less than $10,000, unless otherwise specified in regulations.

Item 15 – Subsection 6(2) (after table item 50)

36. Item 15 creates a new designated service of exchanging money for digital currency (and vice versa) by inserting item 50A into Table 1 (financial services) of section 6. This designated service relates to exchanges provided in the course of carrying on a digital currency exchange business. The inclusion of this new designated service means that persons providing such a service become 'reporting entities', triggering a range of AML/CTF obligations under the AML/CTF Act. Item 15 also establishes that the customer of such a service is 'the person whose digital currency or money is exchanged'. The designated service is not intended to capture either digital wallets or digital wallet providers. Financial institutions providing a digital currency exchange service under item 50A will also not be required to register on the Digital Currency Exchange Register (this will be provided for in the AML/CTF Rules); however financial institutions will be subject to the other relevant obligations of the AML/CTF Act when providing this designated service.

Item 16 – Subsection 6(4) (table item 7)

Item 17 – Subsection 6(4) (table item 8)

37. Items 16 and 17 update the designated service of exchanging money for gaming chips or tokens (and vice versa) to include exchanging digital currency for gaming chips or tokens

(and vice versa). The exchange of e-currency for gaming chips and tokens was previously a designated service because of its inclusion in the former definition of money.

Item 18 – Section 19 (heading)

Item 19 – Section 19

38. Items 18 and 19 amend section 19 of the AML/CTF Act to replace references to e-currency with digital currency. Section 19 sets out how the value of digital currency is to be determined when obligations under the AML/CTF Act refer to amounts in Australian dollars.

Item 20 – After Part 6

39. Item 20 inserts a new Part 6A, which establishes a new Digital Currency Exchange Register. The registration obligations and procedures under Part 6A are modelled on the existing Part 6 of the AML/CTF Act which established the Remittance Sector Register.

40. Section 76 sets out a simplified outline of the new Part 6A.

41. Section 76A imposes requirements on a person providing a registrable digital currency exchange service. Subsection 76A(1) requires that a person must not provide a registrable digital currency exchange service to another person if the first person is not a registered digital currency exchange provider. Subsection 76A(2) requires that a person must not breach a condition to which the registration of the person as a digital currency exchange provider is subject.

42. Subsection 76A(3) creates an offence with three physical elements: (a) that the person is subject to a requirement under subsection 76A(1) or 76A(2); and (b) the person engages in conduct; and (c) the person's conduct breaches the requirement. The penalty for an offence against subsection 76A(3) is imprisonment for 2 years or 500 penalty units, or both.

43. Subsection 76A(4) provides that strict liability applies to paragraphs 76A(3)(b) and (c). A note to subsection 76A(4) provides that 'strict liability' is defined in section 6.1 of the Criminal Code.

44. Subsections 76A(5), 76A(7) and 76A(9) create aggravated offences with increased penalties for breaching the requirements of subsections 76A(1) and 76A(2). Where:

- the AUSTRAC CEO has previously given, on one occasion, the person a remedial direction (under subsection 191(2)), or accepted an undertaking given by the person under section 197, the penalty is imprisonment for 4 years or 1,000 penalty units, or both;

- the AUSTRAC CEO has on more than one occasion given a remedial direction to the person or accepted an undertaking from the person, the penalty is imprisonment for 7 years or 2,000 penalty units, or both; and

- a person has previously been convicted of any of the offences in section 76A, or has had an order previously made against them under section 19B of the *Crimes Act 1914* in respect of any of the offences in section 76A, the penalty is imprisonment for 7

years or 2,000 penalty units, or both. A section 19B *Crimes Act 1914* order is one where the offence is found proved but no conviction is recorded for example because of the person's prior good record.

45. No fault element is specified for the physical element in each of the above offences when a person is subject to a requirement under subsection 76A(1) or 76A(2), meaning that the default fault element of recklessness will apply. Subsections 76A(4), 76A(6), 76A(8) and 76A(10) provide that strict liability applies to the following physical elements of the offences in section 76A: the person engages in conduct, and the person's conduct breaches a requirement of subsections 76A(1) or 76A(2). This means that it is not necessary for the prosecution to prove an associated fault element—such as intention, knowledge, recklessness or negligence—for these physical elements.

46. The *Guide to Framing Commonwealth Offences* (the Guide) highlights that strict liability should only be used in limited circumstances where there is adequate justification. With reference to the Senate Standing Committee for the Scrutiny of Bills Report 6/2002 and the principles outlined in the Guide, applying strict liability for the above physical elements is considered appropriate to ensure that the integrity of the AML/CTF regulatory regime is maintained when it is extended to include digital currency exchange providers. Requiring these entities to register with AUSTRAC and report actionable financial intelligence is critical to the effective operation of Australia's AML/CTF regime. Requiring proof of fault for the physical elements of the offences would undermine the deterrent effect of these provisions because it would allow for entities to argue that they did not know or were reckless as to whether they had obligations under the Act.

47. Section 9.2 of the Criminal Code provides that a defence of honest and reasonable mistake of fact is available for strict liability physical elements. Under this defence, a defendant must turn his or her mind to the existence of the facts, and be under a mistaken but reasonable belief about those facts. This defence is therefore available for the strict liability elements of the offences in Part 6A.

48. The strict liability provisions in the Bill are therefore consistent with the principles set out in the Guide.

49. The criminal penalties available under 76A(3), 76A(5), 76A(7) and 76A(9) do not align with the standard fine/imprisonment ratio set out in the Guide, but this can be justified on the basis of the need to deter high-risk digital currency exchange providers from operating outside the scope of Australia's AML/CTF regime. These businesses have the potential to generate significant criminal proceeds far exceeding the maximum penalties available under the standard ratio. The Guide contemplates the use of higher penalties to combat corporate or white collar crime to counter the potential financial gains from committing an offence.

50. The registration obligations and procedures, including the offence provisions, in Part 6A mirror the penalty provisions in Part 6 of the AML/CTF Act in relation to the Remittance Sector Register. The use of consistent penalties in relation to the Remittance Sector Register and the Digital Currency Exchange Register is appropriate as the FATF has identified both remitters and digital currency exchange providers to be high-risk businesses for the purposes of AML/CTF regulatory regimes. This is also in accordance with the Guide, which notes that 'a penalty should be formulated in a manner that takes account of penalties applying to

offences of the same nature in other legislation and to penalties for other offences in the legislation in question'.

51. Subsection 76A(11) provides that subsections 76A(1) and 76A(2) are civil penalty provisions. This means that a person may be subject to a civil penalty instead of being charged with a criminal offence for conduct breaching subsections 76A(1) or 76A(2). Civil penalties may be enforced under Division 2 of Part 15 of the AML/CTF Act. The maximum penalty that can be imposed for contravening a civil penalty provision is 100,000 penalty units for a corporation and 20,000 penalty units for persons other than a body corporate. A person cannot be ordered to pay a civil penalty if they have been convicted of an offence in relation to the same conduct. The burden of proof in proceedings for a civil penalty is on the balance of probabilities and there is no requirement to prove any fault elements in relation to the offending conduct.

52. Sections 76B to 76T establish the Digital Currency Exchange Register and provide for:

- the procedures concerning how to make an application for registration as a digital currency exchange provider
- the rights and obligations of registered persons and persons applying for registration
- the rights of applicants for registration and registered persons to seek review of decisions of the AUSTRAC CEO, and
- the AML/CTF Rule-making and other powers of the AUSTRAC CEO.

Part 6A is consistent with the provisions in Part 6 of the AML/CTF Act concerning the Remittance Sector Register, including the amendments to Part 6 made by this Bill, which are discussed below.

53. Section 76B creates a duty for the AUSTRAC CEO to maintain a Digital Currency Exchange Register, which may be done by electronic means. The Digital Currency Exchange Register is not a legislative instrument within the meaning of section 8 of the *Legislation Act 2003* as it is administrative in character and does not determine or alter the content of the law. Accordingly, subsection 76B(3), which states that the register is not a legislative instrument, has been included to assist readers and does not represent a substantive exemption from the requirements of the *Legislation Act 2003*. This means that the Digital Currency Exchange Register does not need to be tabled in Parliament and is not subject to disallowance by either House.

54. Subsection 76B(4) provides that the AUSTRAC CEO may make AML/CTF Rules relating to the correction of the Digital Currency Exchange Register, its publication in whole or in part, and other matters relating to the administration or operation of the Register.

55. Section 76C specifies the information to be included on the Digital Currency Exchange Register if the AUSTRAC CEO decides to register a person.

56. Section 76D establishes the requirements for applying for registration as a digital currency exchange provider. The application must be in the approved form and contain the information required by the AML/CTF Rules.

57. Subsection 76D(4) provides for the deemed refusal of an application if the AUSTRAC CEO has not made a decision within 90 days of the latest of a person:

- making an application;
- providing information in relation to an application requested by the AUSTRAC CEO; or
- making a submission under section 76S of the AML/CTF Act, which provides that a person may make a submission in response to a written notice that the AUSTRAC CEO proposes to refuse registration as a digital currency exchange provider.

58. Subsection 76D(5) gives the AUSTRAC CEO the ability to extend the period by a further 30 days in instances where the application cannot be dealt with properly within the 90 day period either because of its complexity or other special circumstances. The AUSTRAC CEO must give notice of the renewal in writing to the applicant before the end of the initial 90 day period.

59. Section 76E provides that the AUSTRAC CEO must register a person if satisfied that it is appropriate to do so having regard to the ML, TF or other serious crime risk involved and to any additional matters specified in the AML/CTF Rules. Subsection 76E(3) provides a non-exhaustive list of the matters that may be specified in the AML/CTF Rules. Given the ML, TF and other serious crime risks associated with the digital currency sector, it is appropriate that the AUSTRAC CEO be provided with specific information about an applicant which is relevant to determining their suitability as a digital currency exchange provider.

60. A decision by the AUSTRAC CEO not to register a person is a reviewable decision. The AUSTRAC CEO must, as soon as practicable, after deciding to register a person, give written notice to the applicant for registration. A person who is adversely affected by a decision on registration will be entitled to seek review of the decision in accordance with the review provisions in Part 17A of the AML/CTF Act. If the AUSTRAC CEO decides to register a person, subsection 76E(4) requires that a notice be given to the person specifying the matters set out in subsection 76E(5).

61. Section 76F preserves the primacy of the spent convictions regime. Any Rules made by the AUSTRAC CEO under paragraphs 76D(2)(b) or 76E(2)(b) cannot override the spent convictions regime.

62. Section 76G enables the AUSTRAC CEO to impose conditions on the registration of a person as a digital currency exchange provider. These conditions may relate to (without limitation):

- the value of digital currency or money exchanged;
- the volume of digital currency being exchanged (whether by reference to a particular period, a particular kind of digital currency, or otherwise);
- the kinds of digital currencies exchanged; and/or

- requiring notification of exchange of particular kinds of digital currency, changes in circumstances, or other specified events.

63. A decision to impose conditions is a reviewable decision and review of the decision can be sought in accordance with the review provisions in Part 17A of the AML/CTF Act. A note to section 76G highlights that section 76P imposes a general obligation in relation to notification of changes in circumstances.

64. Section 76H specifies when a person's registration as a digital currency exchange provider ceases. The basis for registration ceasing are where:

- registration is cancelled by the AUSTRAC CEO under section 76J
- a person has requested the removal of an entry from the register under section 76M(2)
- at the expiration of three years
- where a person dies, or
- where a body corporate no longer exists.

65. The effect of paragraph 76H(1)(c) is that a person's registration will cease after three years unless it has already ceased for another reason. This ensures that the registration of industry participants in the digital currency exchange sector should be reviewed on a regular basis to consider each person's ongoing suitability for involvement in the sector.

66. There may be circumstances in which it would be unreasonable to require a person whose application ceases under section 76H(1)(c) to undertake a full application process. Accordingly subsection 76H(2) cross-refers to section 76L which enables arrangements for the renewal of registrations to be set out in the AML/CTF Rules.

67. Section 76J provides that the AUSTRAC CEO may cancel registrations on the Digital Currency Exchange Register if the AUSTRAC CEO is satisfied that it is appropriate to do so, having regard to:

- whether the continued registration of the persons involves, or may involve, a significant ML, TF or other serious crime risk, or
- any breaches of a condition of registration by the person, or
- any other matters specified in the AML/CTF Rules.

68. Subsection 76J(2) provides that the AUSTRAC CEO may also cancel the registration if the CEO has grounds to believe that the relevant person no longer carries on a business that involves providing a digital currency exchange service. The cancellation of a registration takes effect on the day specified in a notice provided to the person and it is a reviewable decision in accordance with the review provisions in Part 17A of the AML/CTF Act.

69. Subsection 76J(3) states that cancellation of registration takes effect on the date specified in the notice of cancellation. Subsection 76J(4) empowers the AUSTRAC CEO to

publish a list of the names of persons whose registration has been cancelled and the date of cancellation. This will enhance the transparency of the digital currency exchange sector and enable consumers to access information about cancellation.

70. Section 76K provides that the AML/CTF Rules may make provision for the suspension of registrations on the Digital Currency Exchange Register by the AUSTRAC CEO. Subsection 76K(2) provides a non-exhaustive list of the matters that may be included in the Rules such as:

- the grounds for the suspension of registration
- the effect of the suspension on a person's registration
- the period for which suspensions have effect
- making entries in and removing entries from the Digital Currency Exchange Register in relation to the suspension
- notices of suspension, and/or
- reviews of decisions relating to suspensions

71. Section 76L is related to paragraph 76H(1)(c) which provides that registration ceases after three years. Accordingly, section 76L enables arrangements for the renewal of registrations to be set out in the AML/CTF Rules in circumstances where a complete application process would not be appropriate.

72. Section 76M provides that the AUSTRAC CEO must remove a person's registration from the Digital Currency Exchange Register upon that person's request. Subsection 76M(3) provides that the AUSTRAC CEO may also remove a registration if the registration has ceased under the operation of another provision in Part 6A. The AUSTRAC CEO must notify a person as soon as practicable after taking this action.

73. Section 76N clarifies the relevant Rule-making powers in Part 6A by stating that the Rules may set out different provisions for the registration or proposed registration of a person on the Digital Currency Exchange Register depending on different circumstances.

74. Subsection 76P(1) requires persons registered on the Digital Currency Exchange Register to advise the AUSTRAC CEO of any change in circumstances that could materially affect their registration and of any other matters as required by the AML/CTF Rules. Subsection 76P(2) requires notification to be made within 14 days of the change in circumstances arising in the approved form.

75. Subsection 76P(3) provides that subsection 76P(1) is a civil penalty provision. Under subsection 175(4) and (5) of the AML/CTF Act, the maximum civil penalty that can be imposed by the Court for breaches of these provisions is 100,000 penalty units for a body corporate and 20,000 penalty units for a person other than a body corporate.

76. Section 76Q allows the AUSTRAC CEO to request further information from a person for the purposes of making a decision under Part 6A and makes it clear that the CEO is not required to consider an application until the further information has been provided.

77. Section 76R provides the Commonwealth, AUSTRAC CEO and a member of the staff of AUSTRAC with immunity from an action, suit or proceeding (whether criminal or civil) in relation to the publication of the Digital Currency Exchange Register or a list of persons whose registration has been cancelled under subsection 76J(4).

78. Section 76S sets out the steps the AUSTRAC CEO must take before making a reviewable decision under section 76E, 76G or 76J. Except in cases of urgency, the AUSTRAC CEO must give written notice of a proposed decision setting out the terms of and reasons for the proposed decision. If the proposed decision is to cancel a registration, the AUSTRAC CEO must provide the date on which the cancellation is proposed to take effect. The person will have 28 days to provide a submission in response.

79. Section 76T summarises the grounds on which registration is based, and in particular, makes it clear that registration is defeasible and therefore subject to future modification or extinguishment, by or under later legislation, without compensation.

Item 21 – Paragraph 142(1)(b)

Item 22 – Subsection 142(2)

Item 23 – Paragraph 142(3)(a)

80. Items 21-23 of the Bill are consequential changes related to the separation of the concepts of money and digital currency in the AML/CTF Act. They ensure that the structuring of transactions involving digital currency to avoid any threshold transaction reporting requirements is an offence under the Act.

Item 24 – At the end of subsection 184(1A)

Item 25 – Section 186A (heading)

Item 26 – Subsection 186A(1)

Item 27 – Subsection 186A(2)

Item 28 – Paragraph 186A(3)(a)

Item 29 – Paragraph 186A(4)(a)

Item 30 – Paragraph 186A(4)(b)

Item 31 – Paragraph 186A(4)(b)

81. Items 24-31 are consequential amendments to Part 15 of the AML/CTF Act to extend the infringement notice scheme to cover breaches of new subsections 76A(1) and (2) (which relate to the provision of services without being registered) and 76P(1) (which deals with notifying the AUSTRAC CEO of certain matters).

82. Under proposed amendments to section 186A, the AML/CTF Rules may set out one or more kinds of contraventions of subsections 76A(1), (2) or 76P(1) and specify for each contravention the number of penalty units that will apply.

83. Under section 186A the penalty payable depends on whether or not the contravention is by a body corporate or a person other than a body corporate, and whether it is of a kind specified in the AML/CTF Rules. Subsection 186A(5) of the AML/CTF Act provides that the maximum penalty that may be specified in the Rules must not exceed 120 penalty units for a body corporate and 24 penalty units for a person other than a body corporate.

Item 32 – Subparagraph 189(b)(i)

Item 33 – Subparagraph 189(c)(i)

84. Items 32-33 clarify that the ability to issue infringement notices does not affect the possibility of future criminal and civil proceedings in relation to a failure to register on the Digital Currency Exchange Register.

Item 34 – Section 233B (after table item 3)

Item 35 – Section 233B (at end of the table)

Item 36 – Paragraph 233C(1)(b)

Item 37 – Subsection 233C(2)

85. Items 34-36 provide that decisions under:

- subsection 76D(4) or section 76E to refuse to register a person as a digital currency exchange provider
- section 76G to impose conditions to which a person's registration is subject
- section 76J to cancel a person's registration, and
- paragraphs 75H(2)(g), 75J(2)(f), 76K(2)(f) or 76L(2)(f) that are declared to be reviewable decisions by the AML/CTF Rules

are reviewable decisions for the purposes of the AML/CTF Act. This means that they can be reviewed in accordance with the provisions in Part 17A of the AML/CTF Act.

86. Item 37 provides that the notice provisions under section 233C do not apply to deemed refusals under subsection 76D(4).

Part 3—Remittance activities

87. Part 3 of the Bill gives the AUSTRAC CEO the power to cancel the registration of a person who is registered on the Remittance Sector Register where the AUSTRAC CEO has reasonable grounds to believe that the registered person no longer carries on a service that gives rise to the requirement to be registered on the Remittance Sector Register.

88. Recommendation 11.4 of the Report recommends that the AUSTRAC CEO be given stronger powers to control the registration of registered independent remittance dealers, registered remittance affiliates and registered remittance network providers (remittance providers) in order to assist in addressing some of the ML and TF risks posed by the remittance sector. Recommendation 11.4(a) provides that the AUSTRAC CEO should be allowed to deregister remittance providers that are not conducting remittance activities (as evidenced by a lack of reporting to AUSTRAC or other relevant activity).

89. Under section 75G of the AML/CTF Act, the AUSTRAC CEO currently has the power to cancel a remittance provider's registration if the registration involves, or may involve, a significant ML, TF or people smuggling risk, or if the person has breached one or more conditions of registration. However, the AUSTRAC CEO has no power to cancel a registered entity on the basis that it is inactive.

90. A power to cancel the registration of a remittance provider in circumstances where the provider ceases to carry on a remittance business would ensure that the registration is not passed on to a third party and used to avoid scrutiny by AUSTRAC.

91. Part 3 of the Bill also amends subsection 75E(1) to clarify that the AUSTRAC CEO has the power to renew registrations for remittance providers with conditions. The decision whether to renew a registration with conditions is reviewable in accordance with the provisions in Part 17A of the AML/CTF Act.

92. Part 3 also makes a minor amendment to section 75C of the AML/CTF Act, to expand the matters to which the AUSTRAC CEO should have regard when deciding whether to register a person who has applied for registration on the Remittance Sector Register.

Anti-Money Laundering and Counter-Terrorism Financing Act 2006

Item 38 – Paragraph 75C(2)(a)

93. Subsection 75C(2) of the AML/CTF Act specifies circumstances in which the AUSTRAC CEO must register a person who has applied for registration on the Remittance Sector Register.

94. Paragraph 75C(2)(a) provides that the AUSTRAC CEO must decide to register the person if the AUSTRAC CEO is satisfied that it is appropriate to do so, having regard to 'whether registering the person would involve a significant money laundering, financing of terrorism or people smuggling risk'.

95. Item 38 of the Bill amends paragraph 75C(2)(a) to omit the words 'or people smuggling' and substitute these words with 'people smuggling or other serious crime'. Item 38 seeks to ensure that, in deciding whether to register a person on the

Remittance Sector Register, the AUSTRAC CEO also considers whether registering the person would involve a serious crime risk. This change is consistent with the factors the AUSTRAC CEO will have to take into account when registering entities on the new Digital Currency Exchange Register (see Part 2 of Schedule 1 to this Bill).

Item 39 – Subsection 75E(1)

96. Item 39 amends subsection 75E(1) to omit the words 'under subsection 75C(2)' and substitute these words with 'under this Part'. This change clarifies the AUSTRAC CEO has the power to renew registrations for remittance providers with conditions. The decision whether to renew a provider's registration with conditions is reviewable in accordance with the provisions in Part 17A of the AML/CTF Act.

Item 40 – Paragraph 75G(1)(a)

97. Subsection 75G(1) of the AML/CTF Act specifies the circumstances in which the AUSTRAC CEO may cancel a person's registration on the Remittance Sector Register.

98. Paragraph 75G(1)(a) provides that the AUSTRAC CEO may cancel the registration of a person if the AUSTRAC CEO is satisfied that it is appropriate to do so, having regard to 'whether the continued registration of the person involves, or may involve, a significant money laundering, financing of terrorism or people smuggling risk'.

99. Item 40 of the Bill amends paragraph 75G(1)(a) to omit the words 'or people smuggling' and substitute these words with 'people smuggling or other serious crime'. Item 40 seeks to ensure that, in deciding whether to cancel the registration of a person on the Remittance Sector Register, the AUSTRAC CEO also has regard to whether registering the person would involve a serious crime risk. This change is consistent with the factors the AUSTRAC CEO will have to take into account when cancelling a person's registration on the new Digital Currency Exchange Register (see Part 2 of Schedule 1 to this Bill).

Item 41 – After subsection 75G(1)

100. Item 41 inserts subsection 75G(1A) after subsection 75G(1).

101. Subsection 75G(1A) provides that the AUSTRAC CEO may also cancel the registration of a person if the AUSTRAC CEO has reasonable grounds to believe that the registered person no longer carries on a business that gives rise to the requirement to be registered under this Part.

102. The Item grants the AUSTRAC CEO the power to cancel the registration of a remittance provider if the provider ceases to carry on business as a remittance provider.

Part 4—Regulatory relief to industry

103. Part 4 of the Bill comprises measures that grant regulatory efficiencies to industry, including amendments to:

- clarify due diligence obligations relating to correspondent banking relationships and broaden the scope of these relationships
- de-regulate the cash-in-transit sector, insurance intermediaries and general insurance providers
- qualify the term 'in the course of carrying on a business', and
- allow related bodies corporate to share information.

Broaden the scope of the definition of correspondent banking relationship in section 5 of the AML/CTF Act

104. Section 5 of the AML/CTF Act provides that ***correspondent banking relationship*** means 'a relationship that involves the provision by a financial institution (the ***first financial institution***) of banking services to another financial institution …'

105. This definition of a 'correspondent banking relationship' under the AML/CTF Act is unduly narrow and inconsistent with international banking practice.

106. The narrowness of the relationships captured by this definition stems from the definition of a financial institution under the AML/CTF Act. Section 5 of the AML/CTF Act provides that ***financial institution*** means:

(a) authorised deposit-taking institution; or
(b) a bank; or
(c) a building society; or
(d) a credit union; or
(e) a person specified in the AML/CTF Rules.

107. A consequence of this definition of *financial institution* is that Part 8 of the AML/CTF Act, which deals with matters relating to correspondent banking, does not recognise certain correspondent banking arrangements that financial institutions can enter into with foreign entities, where those foreign entities are not considered to be financial institutions for the purposes of the AML/CTF Act.

108. The current definition of *correspondent banking relationship* has regulatory implications. Financial institutions that enter into correspondent banking relationships with foreign entities that are considered financial institutions for the purposes of the AML/CTF Act must conduct a due diligence assessment of the foreign entity. However, financial institutions that enter into correspondent banking arrangements where the foreign entity is not considered a financial institution for the purposes of the AML/CTF Act must comply with the more stringent customer due diligence obligations in Chapter 4 of the AML/CTF Rules for services provided to each customer under the relationship, instead of only conducting a due diligence assessment of the foreign entity itself.

109. Consultation with the financial sector has revealed strong support for adopting a broader definition of a correspondent banking relationship to acknowledge that Australian financial institutions often enter into correspondent banking relationships with foreign financial services providers which may not be considered a financial institution for the purposes of the AML/CTF Act.

110. Consistent with the views of industry on this matter, recommendation 10.3(a) of the Report provides that the AML/CTF Act should be amended to broaden the definition of correspondent banking in line with international approaches that are consistent with the FATF standards.

Anti-Money Laundering and Counter-Terrorism Financing Act 2006

Item 42 – Section 5

111. Item 42 provides that 'corporate group' has the meaning given by subsection 123(12).

Item 43 – Section 5 (at the end of the definition of *financial institution*)

112. Section 5 of the AML/CTF Act defines a *correspondent banking relationship* as 'a relationship that involves the provision by a financial institution…of banking services to another financial institution…' In order to broaden the definition of *correspondent banking relationship*, Item 43 amends the definition of *financial institution* in section 5 of the AML/CTF Act. Paragraph (e) of the definition of *financial institution* in section 5 of the AML/CTF Act provides that *financial institution* means:

(e) a person specified in the AML/CTF Rules.

113. Item 43 of the Bill amends section 5 of the AML/CTF Act to add text at the end of the definition of *financial institution* providing that the AML/CTF Rules made under paragraph (e) of the definition of *financial institution* may specify different persons to be financial institutions for the purposes of different provisions of the AML/CTF Act. This amendment will enable the AUSTRAC CEO to make AML/CTF Rules to recognise, for the purposes of Part 8 of the AML/CTF Act, a broader range of foreign institutions as 'financial institutions' with which Australian financial institutions may enter into correspondent banking relationships.

De-regulate the cash-in-transit sector under the AML/CTF Act

114. Items 51 and 53 of Table 1 of subsection 6(2) of the AML/CTF Act list collecting physical currency, or holding physical currency collected, from or on behalf of a person (item 51) and delivering physical currency to a person (item 53) as designated services. These services are provided by cash-in-transit operators which are licensed at the state and territory level.

115. The ML and TF risks associated with these services are considered to be low, and as a result recommendation 4.1 of the Report recommends amending the AML/CTF Act to delete items 51 and 53 from Table 1 of subsection 6(2) of the AML/CTF Act.

Anti-Money Laundering and Counter-Terrorism Financing Act 2006

Item 44 – Subsection 6(2) (table items 51 and 53)

116. Item 44 implements this recommendation by repealing items 51 and 53 of Table 1 of subsection 6(2), with the effect being to deregulate businesses that provide the relevant designated services.

Qualify the term 'in the course of carrying on a business'

117. Consultation with industry during the review of the AML/CTF regime revealed widespread concern about the breadth of the phrase 'in the course of carrying on a business' used in section 6 of the AML/CTF Act. Industry considered that the use of the term within the designated services listed under Tables 2 and 3 of subsections 6(3) and 6(4) potentially captured businesses that provide such services incidental to their core function, or on a very occasional basis.

118. The Report recommends amending the designated services under Tables 2 and 3 of subsection 6(3) and 6(4) to better target regulation at businesses that routinely provide the services listed, rather than businesses that may provide these services incidentally or on a very occasional basis. This position is consistent with the Replacement Explanatory Memorandum for the AML/CTF Act which states that:

> as a general proposition, designated services are limited to services provided to a customer in the course of carrying on the core activity of a business and do not capture activities which are peripheral to the core activity of the business […] Some businesses may have more than one core activity and whether an activity is a core activity of the business will be determined by the circumstances of each case.[5]

Anti-Money Laundering and Counter-Terrorism Financing Act 2006

Item 45 – Subsection 6(3) (table items 1 and 2)

Item 46 –Subsection 6(4) (table items 1, 2, 3, 4, 6, 9, 11, 12 and 13)

119. Item 45 amends subsection 6(3), Table 2, items 1 and 2 of the AML/CTF Act to provide that the services specified in these items are only designated services when they are provided in the course of carrying on a bullion-dealing business.

120. Item 46 amends subsection 6(4), Table 3, items 1, 2, 3, 4, 6, 9, 11, 12 and 13 to provide that the services specified in these items are only designated services when they are provided in the course of carrying on a gambling business.

Clarify correspondent banking requirements

121. Correspondent banking is the provision of banking services by one financial institution to another financial institution. There are two types of accounts associated with correspondent banking:

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

- *nostro* account – an account that a bank holds, usually in a foreign currency, in another bank, and

- *vostro* account – an account that other banks have with the bank, usually in the bank's domestic currency.

122. The Report recommends that the due diligence requirements regarding *nostro* accounts be clarified, as industry stakeholders considered that the due diligence requirements appear to apply to both *nostro* and *vostro* accounts.

123. The intention is that the due diligence requirements under Part 8 only apply to *vostro* accounts. This is consistent with the FATF's international standards and international banking practice. Requiring due diligence on *nostro* accounts is unnecessary as transactions within these accounts are originated by and conducted for a bank's own customers.

Anti-Money Laundering and Counter-Terrorism Financing Act 2006

Item 47 – Subsections 97(1) and (2)

Item 48 – Subsections 98(1) and (2)

Item 49 – Subsection 99(1)

Item 50 – Subsection 99(2)

124. Items 47-50 in Part 4 of Schedule 1 to the Bill amend Part 8 of the AML/CTF Act to insert:

- in subsections 97(1), 97(2) and 99(1), after the words 'with another financial institution', the words 'that will involve a *vostro* account', and

- in subsections 98(1), 98(2) and 99(2), after the words 'with another financial institution', the words 'that involves a *vostro* account'.

125. These amendments clarify that the requirement to perform due diligence under Part 8 only applies in relation to *vostro* accounts. The term *vostro* is well understood among the financial sector and is not defined.

Allow related bodies corporate to share information

126. Under section 5 of the AML/CTF Act, 'designated business group' (DBG) is defined as:

> '... a group of 2 or more persons, where:
>
> (a) each member of the group has elected, in writing, to be a member of the group and the election is in force; and
>
> (b) each election was made in accordance with the AML/CTF Rules; and
>
> (c) no member of the group is a member of another designated business group; and
>
> (d) each member of the group satisfies such conditions (if any) as are specified in the AML/CTF Rules; and

(e) the group is not of a kind that, under the AML/CTF Rules, is ineligible to be a designated business group.'

127. The Report concludes that this definition is too restrictive, prohibiting the sharing of information within a corporate group to manage the ML and TF risks associated with a shared customer. In order to rectify this deficiency, and to ensure the group construct under the AML/CTF regime better reflects the reality of business structures, recommendation 7.5 of the Report recommends replacing the concept of a DBG with the concept of a 'corporate group'.

128. Items 51-55 in Part 4 of Schedule 1 to the Bill amend Part 11 of the AML/CTF Act to supplement the concept of a DBG with the concept of a corporate group. The definition of 'corporate group' is defined in accordance with the definition of 'related bodies corporate' under section 50 of the *Corporations Act 2001*. This amendment will allow reporting entities to share information with other reporting entities within a corporate group as well as within a DBG to manage their ML and TF risks associated with common customers without breaching the tipping-off provisions in the AML/CTF Act. Supplementing, rather than replacing, the concept of the DBG will ensure that businesses that fall within the DBG concept, but may not fall within the definition of corporate group (for example, businesses acting under partnership or mixed arrangements) can continue to share information for the purposes of Part 11 of the AML/CTF Act.

Anti-Money Laundering and Counter-Terrorism Financing Act 2006

Item 51 – Paragraph 123(7)(a)

Item 52 – Paragraph 123(7)(b)

Item 53 – Paragraph 123(7)(d)

Item 54 – Paragraph 123(7AA)(a)

Item 55 – At the end of section 123

129. Item 51 of the Bill amends paragraph 123(7)(a) of the AML/CTF Act to insert the words 'or a corporate group' after the words 'designated business group'.

130. Item 52 of the Bill repeals paragraph 123(7)(b) of the AML/CTF Act to remove the requirement that a reporting entity adopt a joint AML/CTF program that applies to that reporting entity and the DBG before information can be shared. This is a consequential amendment related to measures in the Bill which will allow for the sharing of information across a corporate group. Corporate groups are not required to maintain joint AML/CTF programs under the AML/CTF Act.

131. Item 53 of the Bill amends paragraph 123(7)(d) of the AML/CTF Act to insert the words 'or the corporate group (as the case may be)' after the words 'designated business group'.

132. Item 54 of the Bill amends paragraph 123(7AA)(a) of the AML/CTF Act to insert the words 'or the corporate group (as the case may be)' after the words 'designated business group'.

133. Item 55 inserts a definition of 'corporate group' at the end of section 123 of the AML/CTF Act, in a new subsection 123(12). Subsection 123(12) provides that for the purposes of section 123 of the AML/CTF Act, a *corporate group* is constituted by a group of two or more bodies corporate related to each other under section 50 of the *Corporations Act 2001*.

Deregulate insurance intermediaries and general insurance providers

134. Cash dealers are defined in subsection 3(1) of the FTR Act to include a wide range of businesses, including insurance intermediaries and general insurance providers (at paragraph (c) of the definition of *cash dealer*), thereby subjecting these businesses to reporting requirements under the AML/CTF regime.

135. In practice, the only entities which retain reporting obligations under the FTR Act are:

- businesses that sell traveller's cheques, such as Australia Post and travel agents
- insurance intermediaries that are motor vehicle dealers and travel agents
- insurers, and
- solicitors.

Recommendation 18.2 of the Report recommends that insurance intermediaries and general insurance providers, apart from motor vehicle dealers, should be deregulated as the FATF's international standards only require life insurance and investment-related insurance products to be subject to AML/CTF regulation.

Financial Transaction Reports Act 1988

Item 56 – Subsection 3(1) (paragraph (c) of the definition of *cash dealer*)

136. Item 56 of the Bill amends the definition of 'cash dealer' under subsection 3(1) of the FTR Act to remove insurance intermediaries and general insurance providers, and to include motor vehicle dealers acting as insurance intermediaries or insurers.

De-regulate the cash-in-transit sector under the FTR Act

137. As noted above in relation to Item 44 of the Bill, the ML and TF risks associated with cash-in-transit services are broadly considered to be low. Therefore, Item 44 of the Bill de-regulates the cash-in-transit sector under the AML/CTF Act.

138. However, the AML/CTF Act operates alongside the FTR Act. The FTR Act was introduced in 1988 to assist in administering and enforcing taxation laws as well as other Commonwealth, state and territory legislation. With the introduction of the AML/CTF Act in 2006, certain parts of the FTR Act were repealed or became inoperative. However, the FTR Act continues to impose some regulatory requirements for 'cash dealers' and solicitors.

139. Cash dealers are defined in subsection 3(1) of the FTR Act to include a wide range of businesses, including: a person who carries on a business of collecting currency, and holding

currency collected, on behalf of other persons; and a person who carries on a business of delivering currency.

140. The FTR Act reporting obligations do not apply if the same service is captured under the AML/CTF Act as a designated service. Cash-in-transit operators were previously regulated as 'cash dealers' under the FTR Act until the AML/CTF Act commenced in 2006.

141. Due to the de-regulation of cash-in-transit operators under the AML/CTF Act (as set out in Item 44 of this Bill), it is also necessary to amend the FTR Act to ensure that cash-in-transit operators will not once again be regulated as 'cash dealers' under the FTR Act. The intention is to remove all AML/CTF regulation that applies to cash-in-transit operators under the AML/CTF Act or the FTR Act.

Financial Transaction Reports Act 1988

Item 57 – Subsection 3(1) (subparagraphs (k)(i) and (iii) of the definition of *cash dealer*)

142. Item 57 repeals subparagraph (k)(i) of the definition of *cash dealer* under subsection 3(1) of the of the FTR Act, which provides that a cash dealer includes a person (other than a financial institution or a real estate agent acting in the ordinary course of real estate business) who carries on a business of collecting currency, and holding currency collected, on behalf of other persons.

143. Item 57 also repeals subparagraph (k)(iii) of the definition of *cash dealer* under subsection 3(1) of the FTR Act, which provides that a cash dealer includes a person (other than a financial institution or a real estate agent acting in the ordinary course of real estate business) who carries on a business of delivering currency (including payrolls).

144. The effect of Items 44 and 57 of the Bill is that cash-in-transit operators will no longer be regulated under Australia's AML/CTF regime.

Part 5—Investigation and enforcement

Give the AUSTRAC CEO the power to issue infringement notice for a greater range of regulatory offences

145. Infringement notices can only be issued by the AUSTRAC CEO for a narrow range of offences listed under Part 15, Division 3 of the AML/CTF Act. For all other regulatory offences, the AUSTRAC CEO must apply for a civil penalty order through the Federal Court. This process is costly and time consuming and does not always allow AUSTRAC to respond in a timely and proportionate manner to secure reporting entity compliance.

146. Recommendation 15.4 of the Report recommends expanding the infringement notice provisions under subsection 184(1A) of the AML/CTF Act to include a wider range of offences established under the AML/CTF Act that are regulatory in nature. Items 58-62 of the Bill implement this recommendation to give the AUSTRAC CEO more expedient and efficient means for promoting and encouraging compliance with these regulatory requirements.

Anti-Money Laundering and Counter-Terrorism Financing Act 2006

Item 58 – Section 5

Item 59 – Before paragraph 184(1A)(aaa)

Item 60 – After subsection 184(1A)

Item 61 – At the end of section 184

Item 62 – After section 186A

147. Item 58 of the Bill provides that 'designated infringement notice provision' has the meaning given by subsection 184(4).

148. Item 59 of the Bill amends the definition of 'infringement notice provision' under subsection 184(1A) of the AML/CTF Act to include 'a designated infringement notice provision', which is defined in subsection 184(4) inserted by Item 61.

149. Item 60 of the Bill inserts new subsections 184(1B) and 184(1C) into the AML/CTF Act. Subsection 184(1B) provides that despite subsection (1), an infringement notice relating to the contravention of a designated infringement notice provision may only be given to a person by the AUSTRAC CEO. This new power is limited to the AUSTRAC CEO to maintain the integrity of the AML/CTF supervision and enforcement regime and to ensure a consistent regulatory approach is adopted.

150. In order to ensure that the AUSTRAC CEO gives due consideration to relevant matters before issuing an infringement notice, subsection 184(1C) provides that the AUSTRAC CEO must not issue an infringement notice relating to a contravention of subsection 32(1), 41(2), 43(2), 45(2) or 49(2) unless the AUSTRAC CEO considers that issuing such a notice is appropriate in the particular case after taking into account:

(a) the nature and extent of the contravention

(b) the seriousness of the contravention

(c) the circumstances in which the contravention took place, and

(d) any other matter the AUSTRAC CEO considers to be relevant.

151. As these provisions may be triggered by relatively minor contraventions in the context of high-volume transactions, the additional considerations which the AUSTRAC CEO must take into account have been included as a protection against the issue of infringement notices for relatively trivial matters.

152. Item 61 of the Bill inserts a new subsection 184(4) into the AML/CTF Act. Subsection 184(4) provides a list of provisions which fall within the definition of 'designated infringement notice provision'. These provisions are:

(a) subsection 32(1) (which deals with customer identification procedures to be carried out by reporting entities)

(b) subsection 41(2) (which deals with reporting certain suspicious matters)

(c) subsection 43(2) (which deals with reporting a threshold transaction)

(d) subsection 45(2) (which deals with reporting an international funds transfer instruction)

(e) subsection 47(2) (which deals with reporting on compliance with the AML/CTF Act and other instruments)

(f) subsection 49(2) (which deals with providing further information on request), and

(g) subsection 116(2), (3) or (4) (which deal with making and retaining certain records).

153. These provisions have been selected as they relate to conduct that would ordinarily be subject to a civil penalty under existing provisions of the AML/CTF Act. By allowing the AUSTRAC CEO to issue infringement notices for minor contraventions, AUSTRAC will be able to more effectively and efficiently promote compliance with Australia's AML/CTF regime.

154. Item 62 inserts a new section 186B into the AML/CTF Act, which sets the penalty amount for breaches of designated provisions.

155. Subsection 186B(1) provides that the penalty to be specified in an infringement notice for an alleged contravention of a designated infringement notice provision by a body corporate must be a pecuniary penalty equal to 60 penalty units. This penalty is commensurate with the penalty for a breach of a provision identified in an infringement notice issued under paragraph 186A(1)(b), where the breach has been committed by a body corporate.

156. Subsection 186B(2) provides that the penalty to be specified in an infringement notice for an alleged contravention of a designated provision by a person other than a body

corporate must be a pecuniary penalty equal to 12 penalty units. This penalty is commensurate with the penalty for a breach of a provision identified in an infringement notice issued under paragraph 186A(2)(b), where the breach has been committed by a person other than a body corporate.

Allow the AUSTRAC CEO to issue a remedial direction to a reporting entity to retrospectively comply with an obligation that has been breached

157. The AUSTRAC CEO cannot currently issue a remedial direction to require a reporting entity to retrospectively comply with an obligation that has been breached. This deficiency has implications where a reporting entity has failed to submit threshold transaction reports, international funds transfer instructions or compliance reports.

158. The Report recommends that the AUSTRAC CEO be given the power to require a reporting entity to comply with a remedial direction to lodge the required reports to provide a simpler means for AUSTRAC to secure reporting entity compliance and close financial intelligence gaps.

Anti-Money Laundering and Counter-Terrorism Financing Act 2006

Item 63 – Subsection 191(2)

Item 64 – Application of amendment

Item 65 – Subsection 191(3)

Item 66 – After subsection 191(3)

159. Item 63 of the Bill repeals existing subsection 191(2) of the AML/CTF Act and substitutes it with a new subsection 191(2). New subsection 191(2) provides that the AUSTRAC CEO may give the reporting entity a written direction requiring the reporting entity to do one or both of the following:

(a) to take specified action directed towards ensuring that the reporting entity does not contravene the civil penalty provision, or is unlikely to contravene the civil penalty provision, in the future; or

(b) in the case of a contravention of subsection 43(2), 45(2) or 47(2)—to take specified action to remedy the contravention by providing the relevant report to the AUSTRAC CEO within a time specified in the direction.

160. New paragraph 191(2)(a) replicates the substance of existing subsection 191(2) of the AML/CTF Act. Paragraph 191(2)(b) enables the AUSTRAC CEO, in the case of a contravention of subsection 43(2), 45(2) or 47(2), to require the reporting entity to submit the relevant report. This power is limited to the specified provisions as these reports (threshold transaction reports, international funds transfer instructions and compliance reports) should be given to AUSTRAC on the basis of factual information available to the reporting entity. This provides clarity to reporting entities regarding the types of contraventions that will be subject to remedial directions.

161. Item 64 of the Bill provides that paragraph 191(2)(b) of the AML/CTF Act as in force after the commencement of this item applies in relation to a contravention that occurs on or after that commencement. Item 64 is a transitional provision to ensure that the AUSTRAC CEO will not have the ability to issue remedial directions in relation to conduct that occurred before the commencement of the amendments to subsection 191(2) in Item 63.

162. Item 65 amends subsection 191(3) of the AML/CTF Act to omit 'subsection (2)' and substitute 'paragraph (2)(a)'. This amendment reflects that the Bill introduces a new paragraph 191(2)(b) and ensures that subsection 191(3) does not apply to paragraph 191(2)(b).

163. Item 66 of the Bill introduces a new subsection 191(3A) into the AML/CTF Act to provide checks and balances surrounding the remedial directions power granted to the AUSTRAC CEO under paragraph 191(2)(b).

164. Subsection 191(3A) provides that the AUSTRAC CEO:

(a) must not act under paragraph 191(2)(b) if it appears to the AUSTRAC CEO that the contravention occurred more than 24 months before the day on which a direction would be issued, and

(b) must not act under paragraph 191(2)(b) unless the AUSTRAC CEO has:
    (i) assessed the risks that have arisen in view of the contravention, and
    (ii) determined that giving a direction under paragraph 191(2)(b) is an appropriate and proportionate response in the circumstances.

Give police and customs officers broader powers to search and seize physical currency and bearer negotiable instruments and establish civil penalties for failing to comply with questioning and search powers

165. Police and customs officers do not have general search and seizure powers at the border under the AML/CTF Act. Instead, the search and seizure powers under the AML/CTF Act are linked to breaches of the current reporting requirements for physical currency and BNIs.

166. This leaves gaps in the ability of police and customs officers to search and seize physical currency and BNIs under the AML/CTF Act (e.g. in circumstances where a person is carrying physical currency under the $10,000 threshold, or has not been asked to disclose whether they are carrying a BNI).

167. Recommendation 12.4 of the Report recommends removing this gap and broadening the search and seizure powers under sections 199 and 200 of the AML/CTF Act to allow police and customs officers to search and seize physical currency and BNIs where there is:

(a) a suspicion of money laundering, terrorism financing or other serious criminal offences, or

(b) a breach of the cross-border reporting requirements under the AML/CTF Act.

168. The Bill implements these recommendations by broadening the circumstances in which search and seizure powers may be used by police and customs officers at the border.

169. The *Guide to Framing Commonwealth Offences* (the Guide) recommends that seizure should generally only be permitted under a warrant. However, the Guide contemplates a limited range of circumstances where it may be appropriate to allow officers the ability to seize pending issue of warrant, such as situations involving conveyances where it may not be possible or practical to obtain a warrant. The exercise of the new search and seizure powers in the Bill will be time-limited to instances where a person is departing or recently arrived in Australia and can be justified due to the impracticalities of obtaining a warrant in such circumstances.

170. The Guide also contemplates searches without warrants where national security is involved. The movement of physical currency and BNIs across national borders is a recognised ML and TF risk. Criminals exploit the high volume of passenger, cargo and mail movements into and out of Australia and may enlist cash couriers who physically transport cash in person or in their luggage. In many cases it may not be clear until a person is at the border that they are intending to take either legitimately or illegitimately obtained money out of Australia to be used for criminal activities.

171. In its 2014 report, *Terrorism Financing in Australia*, AUSTRAC found that there is a significant risk that the cross-border movement of cash may be used as a channel by Australians travelling overseas to fund terrorist groups and activity. The national security implications of these crime types require police and customs officers to be able to act quickly and effectively to prevent physical currency or BNIs being used for TF purposes.

172. Another limitation in the current provisions is that only criminal penalties are available for the offences under sections 199 and 200 of the AML/CTF Act for failing to comply with questioning and search powers in relation to the cross-border declaration regime for physical currency and BNIs. Recommendation 12.6 of the Report recommends that sections 199 and 200 should also be amended to provide for a civil penalty for a breach of these provisions. The availability of a civil penalty would provide a wider range of options for law enforcement officers to respond to such breaches and assist in ensuring these penalties remain proportionate. The Bill implements this recommendation by amending sections 199 and 200 of the AML/CTF Act.

Anti-Money Laundering and Counter-Terrorism Financing Act 2006

Item 67 – After subsection 199(2)

Item 68 – Subsection 199(3)

Item 69 – Subsection 199(4)

Item 70 – Paragraph 199(4)(d)

Item 71 – Subsection 199(5)

Item 72 – Subsections 199(8), (9) and (10)

Item 73 – At the end of section 199

173. Item 67 of the Bill inserts a new subsection 199(2A) into the AML/CTF Act. Subsection 199(2A) provides that a police officer or customs officer may seize physical

currency produced to the officer in accordance with a lawful request (under paragraphs 199(1)(f) or 199(2)(d)) if:

- the police officer or customs officer has reasonable grounds to suspect that the physical currency may afford evidence as to the commission of an offence against section 53, or

- the police officer or customs officer has reasonable grounds to suspect that the physical currency may be of interest under subsection (14).

174. Section 53 of the AML/CTF Act requires persons departing or arriving in Australia carrying $10,000 or more in physical currency to make a report to authorities. Currently, section 199(2A) only contemplates seizures of physical currency in circumstances where a person has failed to make a section 53 declaration.

175. Subsection 199(14) sets out new, broader grounds of search and seizure for the purposes of subsection 199(2A) and supports the implementation of recommendation 12.4 of the Report (described above). It is also cross-referenced throughout the amendments in Part 5 of the Bill. New subsection 199(14) sets out that physical currency 'may be of interest' if it:

- may be relevant to the investigation of, or prosecution of a person for, an offence against a law of the Commonwealth or of a State or Territory, or

- may be of assistance in the enforcement of the *Proceeds of Crime Act 2002* or regulations under that Act, or

- may be of assistance in the enforcement of a law of a State or Territory that corresponds to the *Proceeds of Crime Act 2002* or regulations under that Act.

176. Item 67 ensures that police and customs officers are now able to seize physical currency produced to them, where the officer has reasonable grounds to suspect that the physical currency may provide evidence of the commission of an offence against section 53 or may be of interest under subsection 199(14).

177. Item 68 of the Bill repeals and replaces subsection 199(3) of the AML/CTF Act. Subsection 199(3) broadens the existing powers of police and customs officers to examine a person's belongings. Currently, officers may only examine an article when seeking to determine if a person has physical currency in respect of which a section 53 report is required. The amendments now allow an officer to examine articles when he or she has reasonable grounds to suspect that the person has any physical currency that may be of interest under subsection 199 (14). This power is time-limited however and may only be exercised in relation to:

- persons who are about to leave Australia, or are about to board or have boarded an aircraft or ship; and

- persons who have arrived in Australia, or are about to leave or have left an aircraft or ship.

178. Item 69 amends the personal search power in subsection 199(4) to remove the requirement that a search only be conducted for the purpose of finding out whether a person has with him or her any physical currency in respect of which a report under section 53 is required. Together with Item 70 of the Bill, which repeals and replaces paragraph 199(4)(d) of the AML/CTF Act, the amendments now allow police and customs officers to search a person so long as the officer has reasonable grounds to suspect that there is on the person, or in clothing being worn by the person:

- physical currency in respect of which a report under section 53 is required, or
- physical currency that may be of interest under subsection (14).

179. This new power is time-limited by the existing provisions in the AML/CTF Act in similar terms to the examination power set out at Item 68.

180. Item 71 of the Bill repeals and replaces subsection 199(5) of the AML/CTF Act which provides police and customs officers with the power to seize physical currency that has been found in the course of an examination or search under subsections 199(3) or (4). In addition to the existing power to seize in relation to section 53 offences, an officer may now seize the currency where there are reasonable grounds to suspect that the currency may be of interest under subsection (14).

181. Item 72 of the Bill repeals and replaces subsections 199(8), (9) and (10) of the AML/CTF Act. Subsection 199(8) currently outlines the powers of police and customs officers to board a ship or aircraft, or examine or search the ship or aircraft and any goods found on board. However, these powers are currently constrained to ascertaining the presence of physical currency in respect of which a report under section 53 would be required. The new subsection 199(8) will allow these powers to be exercised for the purpose of finding out whether there is any physical currency of interest under subsection (14).

182. New subsection 199(9) broadens the search powers of police and customs officers in similar terms to new subsection 199(8), but in relation to 'eligible places'. Eligible places are defined under the AML/CTF Act to include certain warehouses, ports, airports, wharves or boarding stations which are specified under the *Customs Act 1901*.

183. New subsection 199(10) provides police and customs officers with the power to seize currency found in the course of an examination or search under subsections (8) or (9). Currently, officers may only seize currency where they have reasonable grounds to suspect that it may afford evidence of a section 53 offence. The new subsection 199(10) broadens these powers to include circumstances where a police or customs officer has reasonable grounds to suspect that the physical currency may be of interest under subsection (14).

184. Item 73 inserts new subsections 199(12), (13) and (14) into the AML/CTF Act.

185. Subsection 199(12) provides that if a person is subject to a requirement under subsection 199(1) or 199(2), the person must not engage in conduct that breaches the requirement.

186. Subsection 199(13) provides that subsection 199(12) is a civil penalty provision. This Item supports the implementation of recommendation 12.6 of the Report (described above). Under subsection 175(4) and (5) of the AML/CTF Act, the maximum civil penalty that can

be imposed by the Court for breaches of these provisions is 100,000 penalty units for a body corporate and 20,000 penalty units for a person other than a body corporate.

Item 74 – After subsection 200(13)

Item 75 – At the end of section 200

187. Item 74 of the Bill inserts a new subsection 200(13A) into the AML/CTF Act, which broadens the seizure powers of police and customs officers in relation to BNIs (produced under subsection 200(1) or (2) or found in the course of an examination under subsection 200(4)-(9)). A police or customs officer may now seize a BNI when he or she has reasonable grounds to believe that the BNI:

- may be relevant to the investigation of, or prosecution of a person for, an offence against a law of the Commonwealth or of a State or Territory, or
- may be of assistance in the enforcement of the *Proceeds of Crime Act 2002*, or regulations under that Act, or
- may be of assistance in the enforcement of a law of a State or Territory that corresponds to the *Proceeds of Crime Act 2002* or regulations under that Act.

188. These new seizure powers are expressed in similar terms to new subsection 199(14). However, as BNIs are subject to a different reporting regime under the AML/CTF Act (they must be disclosed upon request, rather than declared in amounts over a certain threshold as in the case of physical currency), this Bill only broadens the seizure powers of police and customs officers in relation to BNIs.

189. Item 75 inserts new subsections 200(15) and (16) into the AML/CTF Act.

190. Subsection 200(15) provides that if a person is subject to a requirement under subsection 200(1) or (2), the person must not engage in conduct that breaches the requirement.

191. Subsection 200(16) provides that subsection 200(15) is a civil penalty provision. This Item supports the implementation of recommendation 12.6 of the Report (described above). Under subsection 175(4) and (5) of the AML/CTF Act, the maximum civil penalty that can be imposed by the Court for breaches of these provisions is 100,000 penalty units for a body corporate and 20,000 penalty units for a person other than a body corporate.

Part 6—Revision of definitions

Anti-Money Laundering and Counter-Terrorism Financing Act 2006

Item 76 – Section 5 (paragraph (a) of the definition of *eligible place*)

192. Item 76 corrects a technical drafting error in relation to the definition of 'eligible place'. This provision refers to sufferance wharves appointed under section 17 of the *Customs Act 1901*. Section 17 of the *Customs Act 1901* was repealed in 2015.

Item 77 – Section 5 (at the end of the definition of *investigating officer*)

193. Section 49 of the AML/CTF Act enables an 'investigating officer' or head of a prescribed agency to issue a notice to a reporting entity requiring that entity to provide information or produce a document relevant to a transaction report provided under the AML/CTF Act. The Integrity Commissioner, who is head of the Australian Commission for Law Enforcement Integrity (ACLEI), is one of the agency heads prescribed under section 49.

194. The current definition of 'investigating officer' in section 5 of the AML/CTF Act does not include staff of the ACLEI. This means that the Integrity Commissioner must personally issue a section 49 notice if ACLEI wishes to gather further information.

195. Item 77 amends the definition of 'investigating officer' in section 5 to include a member of the staff of ACLEI, consistent with the approach taken with respect to the Australian Federal Police, the Australian Crime Commission, the Australian Taxation Office and the Australian Border Force.

Item 78 – Section 5 (definition of *signatory*)

196. The current definition of 'signatory' in section 5 of the AML/CTF Act provides:

> ***signatory***, in relation to an account with an account provider, means the person, or one of the persons, on whose instructions (whether required to be in writing or not and whether required to be signed or not) the account provider conducts transactions in relation to the account.

197. This definition has proven to be too broad in practice, giving rise to uncertainty among reporting entities. Under the current definition it could be argued that a store employee can be considered a signatory to the store owner's account if they conduct an EFTPOS transaction through a cash register.

198. Item 78 repeals the definition of 'signatory' in section 5 of the AML/CTF Act and replaces it with a new definition. The new definition focuses on the account holder and persons who have been authorised by the account holder to manage or exercise effective control over an account. This definition excludes persons who may 'instruct' an account provider where this is incidental to a specific transaction or transactions, in circumstances that fall short of management or control of the account.

Item 79 – Section 5 (definition of *stored value card*)

199. Currently, a 'stored value card' (SVC) is defined in section 5 of the AML/CTF Act as follows:

> ***stored value card*** does not include a debit card or credit card but includes a portable device (other than a debit card or credit card) that
>
> (a) is capable of:
>
> (i) storing monetary value in a form other than physical currency; or
>
> (ii) being used to gain access to monetary value stored in such a form; and
>
> (b) is of a kind prescribed by the regulations.

200. Recommendation 19.1(g) of the Report recommends redrafting the definition of SVC to provide industry with greater guidance as to what a SVC can include, while remaining broad, inclusive and sufficiently flexible to cover virtual cards.

201. Item 79 repeals the definition of SVC in section 5 of the AML/CTF Act and replaces it with a new definition, to provide clearer guidance to industry on what is and is not a SVC for the purposes of the AML/CTF Act. The new definition does not alter the existing thresholds applicable to the designated services which relate to SVCs under items 21–24 of Table 1 in subsection 6(2) of the AML/CTF Act. These thresholds ensure that AML/CTF obligations only apply in relation to SVCs where the monetary value stored in connection with the SVC or added to an SVC is not less than $1,000 (for SVCs that permit withdrawal of cash) or $5,000 (for SVCs that do not permit withdrawal in cash). The power to make regulations altering these thresholds is retained.

202. This new definition of SVC encompasses all things, whether real or virtual, that store monetary value in a form other than physical currency, or that give access to value stored in a form other than physical currency. This is substantially similar to paragraph (a) of the previous definition of stored value card, but is technologically neutral and includes SVCs that are entirely virtual and do not exist as a physical card. The requirement to prescribe kinds of SVCs in regulations is removed.

203. The new definition of SVC is broad enough to capture products at risk of misuse for ML or TF. To provide greater clarity, a broader range of exclusions from the definition are also set out in the provision.

204. Credit and debit cards continue to be excluded from the definition of SVC by paragraph (d) of the definition. The exclusion is made technologically neutral by expressly excluding real or virtual credit and debit cards. The exclusion is clarified by specifying that it only applies to credit cards or debit cards linked to an account provided by a financial institution, because services related to these debit and credit cards are regulated under separate provisions of the AML/CTF Act. SVCs such as pre-paid travel cards that make use of credit card networks, but which are not linked to an account provided by a financial institution, do not fall within this exclusion.

205. The new paragraph (e) of the definition expressly excludes specific items from the definition of SVC. However, in each case, the AUSTRAC CEO has the power to declare that things falling within the definition are SVCs under paragraph (c) of the definition, to allow for responsive regulation of new and emerging technologies.

206. The new subparagraph (e)(i) of the definition excludes from the definition of SVCs things that are intended to give access to monetary value in a debit card or credit card account provided by a financial institution, for example, smartphone applications or physical items that may be used to make payments from a debit card or credit card account.

207. The new subparagraph (e)(ii) of the definition expressly excludes gaming chips and tokens from the definition of SVC, because designated services involving gaming chips and tokens are regulated separately under the AML/CTF Act in accordance with Table 3 of subsection 6(4).

208. The new subparagraph (e)(iii) of the definition expressly excludes things that store or give access to digital currency from the definition of SVC, including digital currency 'wallets' and physical media on which digital currency is stored. Digital currencies are separately regulated by the new designated service inserted by the Bill in item 50A of Table 1 (new item 50A of Table 1(financial services) in subsection 6(2)).

209. To ensure the AML/CTF regime is able to capture evolving uses of SVCs and developments in the ML and TF risks associated with SVCs, the new paragraph (f) provides for rule-making powers for the AUSTRAC CEO to prescribe additional products as SVCs or to exclude products from being SVCs. These powers also empower the AUSTRAC CEO to give greater guidance to industry regarding what is and what is not a SVC for the purposes of Australia's AML/CTF regime.

Part 7—Other regulatory matters

Provide a legislative basis for work performed by the AUSTRAC CEO that is incidental or conducive to the performance of his or her functions

210. Recommendation 16.1 of the Report recommends that Division 3 of Part 16 of the AML/CTF Act be amended to:

(a) expand the powers of the AUSTRAC CEO relating to:

(i) retaining, compiling and analysing AUSTRAC information, and

(ii) facilitating access to, and the sharing of, AUSTRAC information to support domestic and international efforts to combat ML, TF and other serious crimes

(b) give the AUSTRAC CEO a standard power to perform tasks that are necessary or convenient to his or her functions.

211. The expansion of the AUSTRAC CEO's powers in these ways would better reflect the full range of work performed by the AUSTRAC CEO. It would also provide a legislative basis for AUSTRAC's role in supporting international and collaborative efforts to combat ML, TF and other serious crimes.

Anti-Money Laundering and Counter-Terrorism Financing Act 2006

Item 80 – Paragraph 212(1)(a)

Item 81 – After paragraph 212(1)(a)

Item 82 – After paragraph 212(1)(d)

Item 83 – At the end of paragraph 212(1)(f)

212. Item 80 of the Bill amends paragraph 212(1)(a) of the AML/CTF Act to insert the words 'or AUSTRAC information' after the words 'eligible collected information'. The amendment ensures that the functions of the AUSTRAC CEO include retaining, compiling, analysing and disseminating AUSTRAC information. The amendment recognises that the AUSTRAC CEO's functions extend to information that has been analysed and compiled by AUSTRAC, such as financial intelligence reports, which may be updated in light of new information or further compiled and analysed to identify broader trends.

213. Item 81 of the Bill also amends subsection 212(1) of the AML/CTF Act to insert a new paragraph 212(1)(aa), which provides that the functions of the AUSTRAC CEO include providing access to, and the sharing of, AUSTRAC information to support domestic and international efforts to combat ML, TF and other serious crimes. The amendment ensures that the AUSTRAC CEO has the power to provide access to and share AUSTRAC information for the purposes stipulated.

214. Item 82 of the Bill amends paragraph 212(1)(d) of the AML/CTF Act to insert a new paragraph 212(1)(da), which provides that it is a function of the AUSTRAC CEO to facilitate gaining access on a timely basis to the financial, administrative and law

enforcement information that the AUSTRAC CEO requires to properly undertake the AUSTRAC CEO's financial intelligence functions.

215. Item 83 of the Bill inserts a new paragraph 212(1)(g) into the AML/CTF Act to give the AUSTRAC CEO the power to do anything that is incidental or conductive to the performance of a function referred to in a preceding paragraph. Following public consultations, the term 'incidental or conducive' was determined to be appropriate given the nature of the AUSTRAC CEO's powers.

Clarify weighting given to ML and TF risk in certain decisions made by the AUSTRAC CEO

216. Under section 212 of the AML/CTF Act, the AUSTRAC CEO must consider a range of factors when making Rules or granting exemptions or modifications as part of his or her functions under the AML/CTF Act. This includes the level of ML and TF risks. As part of Australia's 2015 Mutual Evaluation by the FATF, this requirement was assessed to be insufficient to meet the FATF's international standards, which require exemptions from AML/CTF obligations to be granted solely on the basis of a demonstrated low ML and TF risk.

217. Recommendation 17.1 of the Report recommends that the AML/CTF Act should be amended to set out the specific matters that the AUSTRAC CEO must take into account when determining exemptions, with the level of ML and TF risk posed being the prime consideration.

Anti-Money Laundering and Counter-Terrorism Financing Act 2006

Item 84 – After subsection 212(3)

Item 85 – Subsection 212(5)

218. Item 84 inserts a new subsection 212(3A) after subsection 212(3) of the AML/CTF Act. Subsection 212(3A) provides that in considering an exemption or modification under or in relation to the operation of the AML/CTF Act that could reasonably be expected to have an impact on ML or TF risk, the AUSTRAC CEO must be satisfied that the risk associated with the proposed exemption or modification is low. This formulation envisages two broad categories of exemptions or modifications: those exemptions or modifications that have no impact on ML or TF risk, and those that could be expected to have an impact on ML or TF risk.

219. Examples of exemptions or modifications that have no impact on ML or TF risk include purely procedural or administrative exemptions or modifications; for example, amending the content or format of reports required to be submitted to AUSTRAC to reflect the unique circumstances of a reporting entity.

220. New subsection 212(3A) clarifies that any exemption or modification that could be reasonably expected to have an impact on ML or TF risk may only be given effect where the AUSTRAC CEO is satisfied that the ML or TF risk associated with the exemption or modification is low. In accordance with administrative law principles, the AUSTRAC CEO must take into account all relevant considerations in determining ML or TF risk. The

considerations relevant to risk will differ from case to case and will depend on the specific circumstances of the proposed exemption or modification.

221. Item 85 amends subsection 212(5) of the AML/CTF Act by inserting a reference to new subsection 212(3A) to ensure that any failure by the AUSTRAC CEO to comply with the requirements of subsection 212(3A) does not affect the validity of the AUSTRAC CEO's performance of the function.

Annex A

Australian Government
Attorney-General's Department

May 2017

Final Assessment Regulation Impact Statement

Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2017

Table of contents

EXECUTIVE SUMMARY

Background

This regulatory impact statement (RIS) examines proposed reforms to the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act). The proposed reforms will strengthen and streamline Australia's anti-money laundering and counter-terrorism financing (AML/CTF) regime by removing regulatory gaps, providing regulatory relief and enhancing Australia's compliance with international obligations.

Money laundering and terrorism financing are major global problems. They threaten Australia's national security and the integrity of Australia's financial system. To combat these threats, Australia has established an AML/CTF regime, based on the Financial Action Task Force's (FATF) international standards, that provides for the collection of valuable information from the private sector about the movement of money and other assets.[1]

The Australian Transaction Reports and Analysis Centre (AUSTRAC) analyses the information it receives from the private sector and transforms the information into actionable financial intelligence that is disseminated to its partner agencies, including domestic law enforcement, national security, human services and revenue protection agencies. AUSTRAC information is also shared with its international counterparts for law enforcement, regulatory and counter-terrorism purposes.

The Anti-Money Laundering and Counter-Terrorism Financing Bill 2017 introduces reforms that aim to reduce the risk of money laundering, terrorism financing and other serious crimes, achieve better regulatory outcomes for industry, and build a stronger culture of compliance across regulated business.

The statutory review

The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) was developed in consultation with industry to establish a strong and modern regulatory regime for combating money laundering and terrorism financing (ML/TF), as well as other serious crimes. Broadly, the primary components of this regime require regulated businesses to:

- establish, implement and maintain an AML/CTF compliance program
- conduct customer due diligence (CDD), and
- lodge specified transaction and suspicious matter reports with AUSTRAC.

Section 251 of the AML/CTF Act required a review of the operation of the regulatory regime – that is, the AML/CTF Act, AML/CTF Regulations and AML/CTF Rules – 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.

While section 251 of the AML/CTF Act limits the review to the operation of the AML/CTF regime, issues concerning the operation of the *Financial Transaction Reports Act 1988* (FTR Act), which operates in parallel to the AML/CTF Act, were also considered.

On 29 April 2016, the Minister for Justice tabled in the Australian Parliament the report of the statutory review. The report makes 84 recommendations to strengthen, modernise, streamline and simplify Australia's AML/CTF

[1] The FATF 40 Recommendations can be accessed at the following link: http://www.fatf-gafi.org/topics/fatfrecommendations/documents/internationalstandardsoncombatingmoneylaunderingandthefinancingofterrorismproliferation-thefatfrecommendations.html

regime, and enhance Australia's compliance with the international standards for combating ML/TF set by the FATF, an inter-governmental policy-making body.[2]

As a foundation member of the FATF, Australia periodically undergoes a mutual evaluation to assess its compliance with the FATF Recommendations and the effectiveness of its AML/CTF measures. The 2015 mutual evaluation of Australia identified a number of deficiencies and made a number of recommendations to strengthen compliance and effectiveness.[3] These recommendations were taken into account as part of the statutory review.

Implementation of review recommendations

The review recommendations are being implemented in phases. The Anti-Money Laundering and Counter-Terrorism Financing Bill 2017 (the Bill) will implement the first phase of priority legislative reforms.

Phase 1 includes initiatives that have been identified as priority projects for introduction in 2017.

Future phases will progress significant reforms, the detail of which need to be developed in close consultation with Government agencies and industry. These include measures to simplify, streamline and clarify AML/CTF obligations, and strengthen compliance with the FATF standards.

Major decision points

The tabling of the report on the review represented a major decision point. An early regulatory impact statement was prepared in relation to the recommendations in the report.

The introduction of the Bill to implement the first phase of recommendations also represents a major decision point. This RIS is the final assessment for these first phase recommendations.

Industry contribution

AUSTRAC is Australia's AML/CTF regulator and financial intelligence unit. The industry contribution is a levy on businesses regulated under the AML/CTF regime to meet the costs of AUSTRAC's functions. Any increase (or decrease) in AUSTRAC's regulated population will have an impact on how the industry contribution is calculated.

Policy options for preventing the misuse of digital currency exchange service providers for MT/TF purposes

The majority of measures in the Bill are deregulatory or will have a neutral regulatory impact.

The Bill will impose the full suite of obligations under the AML/CTF regime (apart from International Fund Transfer Instruction reporting obligations) on digital currency exchange service providers.

The use of digital currencies pose significant ML/TF risks as it can occur anonymously and largely outside of the regulated financial system. Consultation with the digital currency exchange sector indicates a good awareness of the ML/TF risks posed by the services they provide and general support for the introduction of regulatory measures to mitigate these risks. While a significant portion of the sector comply with a voluntary Code of Conduct, the sector generally did not consider that a voluntary framework was sufficient to mitigate the risks and bolster public confidence in the sector. Regulatory options were explored with the sector.

[2]The report on the review is available at:
https://www.ag.gov.au/Consultations/Pages/StatReviewAntiMoneyLaunderingCounterTerrorismFinActCth2006.aspx

[3] Financial Action Task Force, *Anti-money laundering and counter-terrorist financing measures, Australia: Mutual Evaluation Report, April 2015*: http://www.fatf-gafi.org/documents/documents/mer-australia-2015.html.

1. What is the policy problem?

The Bill will implement the first phase of reforms arising from the statutory review of the AML/CTF regime.

The review explored, in consultation with industry and government agencies, the continuing relevance of the AML/CTF regime. More specifically, the review examined:

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

Review recommendations address policy and operational issues, and identify opportunities to deliver a more modern and efficient regulatory framework for industry and government.

The Bill progresses prioritised initiatives arising from the review recommendations and include a number of proposals that will have a deregulatory impact. These are:

- clarifying correspondent banking requirements
- expanding the definition of correspondent banking
- deregulating the cash-in-transit sector
- improving the utility of the designated business group concept
- regulating digital currency exchange providers under the AML/CTF regime, and
- deregulating insurance intermediaries and general insurance providers (under the *Financial Transaction Reports Act 1988*)

All of the above measures are deregulatory, except for the proposal to regulate digital currency exchange providers. While the RIS considers the regulatory impact of all the proposals, the proposal to regulate this sector is a key focus.

Clarifying correspondent banking requirements

The application of correspondent banking requirements under the AML/CTF Act to *nostro* and *vostro* accounts is unclear and out-of-step with international banking standards and practices. This lack of clarity leads some regulated businesses to unnecessarily apply AML/CTF measures to both types of accounts, when the AML/CTF measures should only apply to *vostro* accounts.

Expand the definition of correspondent banking

The definition of correspondent banking under the AML/CTF Act is unduly narrow and fails to capture some banking relationships that are recognised as correspondent banking relationships under international banking practice. This means that Australian banks are operating at a competitive disadvantage by having to apply more stringent CDD measures compared with their international counterparts to certain banking relationships.

Deregulating the cash-in-transit sector

Cash-in-transit (CIT) operators are currently subject to AML/CTF compliance and reporting obligations because they provide designated services associated with the secure collection and delivery of physical currency.[4]

[4] Items 51 and 53, table 1, section 6 of the AML/CTF Act.

The AML/CTF regulation of CIT operators in Australia predates the founding of the FATF. CIT operators were first subjected to regulatory obligations under the *Cash Transactions Reports Act 1988* as cash dealers on the basis that they collect and deliver currency. CIT operators continued to be subjected to AML/CTF regulation under the FTR Act and more recently under the AML/CTF Act.

It is generally considered that there are low or negligible inherent ML/TF risks associated with the *domestic* transportation of cash from one place to another by a contractor such as a CIT operator. Securely moving cash using a licensed third party operator within Australia is not, in itself, a money laundering typology and the FATF standards do not require countries to apply AML/CTF regulation to CIT operators. The physical movement of cash *internationally* across borders is, however, an established money laundering typology and the risks associated with such movements of cash are monitored as part of the cross-border reporting regime under the AML/CTF Act.

It is considered that the removal of the AML/CTF obligations will produce regulatory efficiencies because CIT operators and their staff are subject to licensing obligations by the States and Territories.

Improving the utility of the designated business group concept

Some businesses or persons regulated under the AML/CTF regime have an association through ownership which enables them to join together as a 'designated business group' (DBG) and share certain obligations under the AML/CTF Act, allowing these businesses to minimise regulatory burden across the group.

The current definition of a DBG under the AML/CTF Act does not align with how businesses currently structure themselves into 'corporate groups', particularly businesses that are part of multi-national corporate groups, which can lead to duplicate reporting of suspicious matters. A particular concern is that related bodies corporate are unable to share information about joint customers, thereby impeding the ability to effectively and efficiently manage the ML/TF risk associated with a joint customer across the corporate group.

Regulating digital currencies under the AML/CTF regime

Digital currencies, which largely operate outside the scope of the regulated financial system, are increasingly being used as a method for the payment of goods and services and transferring value in the Australian economy.

While digital currencies offer the potential for cheaper, more efficient and faster payments, the associated ML/TF risks are well-documented. Key risks include:

- greater anonymity compared with traditional non-cash payment methods
- limited transparency because transactions are made on a peer-to-peer basis, generally outside the regulated financial system,[5] and
- different components of a digital currency system may be located in many countries and subject to varying degrees of AML/CTF oversight.[6]

The regulatory regime under the AML/CTF Act currently only applies to an 'e-currency' which is backed by a physical thing and excludes convertible digital currencies, such as Bitcoin which are backed by a cryptographic algorithm.

[5] To use bitcoin as an example of 'pseudonymity', every bitcoin transaction is linked to a corresponding public key, which is then stored and made publicly available to view in the block chain. If a person's identity were linked to a public key, then it would be possible to look through the recorded transactions in the block chain and see the transactions associated with that key. In other words, while bitcoin offers users the ability to transact under the concealed identity of their bitcoin address/public key, transactions are available for public viewing and therefore potentially for law enforcement scrutiny.

[6] Financial Action Task Force, *FATF Report: Virtual Currencies – Key Definitions and Potential AML/CFT Risks*, 2014, pp. 9-10, Virtual currency key definitions and potential AML/CTF risks (accessed 11/10/2016).

This regulatory gap is also having an impact on the standing and public perception of the legitimacy of the digital currency sector, which may impede developments or use of these currencies in the future. It is also recognised that many existing businesses are concerned about the risks associated with dealing with digital currency and are choosing not to use or accept this payment method. Banks are also concerned about the risks associated with providing services to digital currency businesses, which can limit access to traditional banking services for the digital currency sector.

Deregulating insurance intermediaries and general insurance providers under the FTR Act

The AML/CTF Act operates alongside the *Financial Transaction Reports Act 1988* (FTR Act). The FTR Act was introduced in 1988 to assist in administering and enforcing taxation laws as well as other Commonwealth, State and Territory legislation. With the introduction of the AML/CTF Act in 2006, certain parts of the FTR Act were repealed or became inoperative but the FTR Act continues to impose some regulatory requirements for 'cash dealers' and solicitors. A cash dealer must submit significant cash transaction reports (SCTRs) and suspect transaction reports (SUSTRs) to AUSTRAC, while solicitors must report SCTRs.

The definition of a cash dealer under the FTR Act currently includes:

- insurance intermediaries, such as motor vehicle dealers and travel agents, and
- general insurance providers, such as motor vehicle dealers.

The FATF's international standards for combating ML/TF only require life insurance and investment-related insurance products to be regulated and not general insurance.[7] Services provided by travel agents acting as insurance intermediaries pose a low ML/TF risk, as do general insurance providers (other than motor vehicle dealers). In view of this outcome, the Bill proposes that these service providers be deregulated.

[7] See the FATF Recommendations: available at http://www.fatf-gafi.org/publications/fatfrecommendations/?hf=10&b=0&s=desc(fatf_releasedate).

2. Why is government action needed?

Money laundering is a key enabler of serious and organised crime. Every year, criminals generate huge amounts of funds from illicit activities including among other things drug trafficking, tax evasion, people smuggling, theft, fraud and corruption. The pursuit of these illicit profits affects the Australian community in many ways and comes at a significant cost to the economy. The Australian Crime and Intelligence Commission estimates that serious and organised crime cost Australia $36 billion in the two year period from 2013 to 2014.[8]

To benefit from the profits of their illicit activity without raising suspicion, criminals must find ways to cloak and place these funds into the legitimate financial system in order to obscure their illicit origins.

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.

Australia's AML/CTF regime needs to keep pace with international trends and developments in order to combat and disrupt money laundering and terrorism financing. By their nature, money laundering and terrorism financing methods evolve to exploit opportunities and avoid detection. Measures introduced under the regime since 2006 can be expected to have influenced ML/TF behaviour and caused criminals to find new ways to circumvent controls. Technological advances, market developments and the emergence of new products and services, in particular new payment systems and methods, may have created new and emerging risks that fall outside the scope of the regime, as well as opportunities for more efficient and effective regulatory outcomes.

The primary objectives in updating Australia's AML/CTF system are better prevention, disruption and detection of ML/TF in Australia, complemented by increased regulatory efficiencies and enhancing compliance with the FATF's international standards.

Digital currencies largely operate outside the scope of the regulated financial system and are becoming an increasingly popular method of paying for goods and services, and transferring value in the Australian economy. In its March 2016 FinTech statement, *Backing Australian FinTech*, the Government noted that '[t]he frictionless operation of FinTech innovations such as Blockchain and digital currencies are generating new value streams not just in financial services but across the economy'.[9] As noted above, there is a range of ML/TF risks associated with the continued proliferation of these new payment methods.

In June 2015, the FATF released guidance on how countries can apply a risk-based approach to address the ML/TF risks associated with virtual currency payment products and services.[10] [11] The guidance suggests that countries should consider applying the FATF standards to convertible virtual currency exchanges, and any other types of institution that act as nodes where convertible virtual currency activities intersect with the regulated financial system. This includes:

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

[8] Available online at https://www.acic.gov.au/sites/g/files/net1491/f/2016/06/the_costs_of_serious_and_organised_crime_in_australia_2013-14.pdf?v=1467258021

[9] The Treasury, *Backing Australian FinTech*, Backing Australian Fintech (accessed 16/11/2016).

[10] The FATF uses the term 'virtual currencies' to refer to 'digital currencies'.

[11] Financial Action Task Force, *Guidance for a risk-based approach to virtual currencies*, June 2015, FATF Guidance for a RBA to Virtual Currencies.

- subjecting domestic entities providing convertible virtual currency exchange services to adequate supervision and regulation.

The FATF acknowledged in its guidance that international approaches to AML/CTF regulation of digital currencies vary across jurisdictions. Some countries consider that digital currencies already fall within their AML/CTF regimes or are seeking to include digital currencies within their AML/CTF regimes.[12] Others have sought to ban digital currencies altogether.[13]

Based on this FATF guidance and broader international developments, the statutory review of Australia's AML/CTF regime recommended that new regulation should focus on digital currency exchanges, as this is the point of intersection between digital currencies and the regulated financial system.

The broader regulation of digital currencies in Australia under the AML/CTF Act is also consistent with:

- a recommendation made by the Productivity Commission as part of its 2015 report, *Business Set-up, Transfer and Closure*
- a recommendation made by the Senate Economic References Committee in its 2015 report *Digital currency – game changer or bit player*, and
- the *Australian Government's FinTech statement*, which noted that applying AML/CTF regulation to digital currencies may facilitate future developments or use of these currencies in the future.

The AML/CTF regulation of this sector will assist the legitimate use of digital currencies by businesses concerned about the risks associated in dealing with digital currency businesses and allow for the collection of financial intelligence about transactions involving digital currencies for use by law enforcement, intelligence and national security agencies. This will restrict opportunities for criminals to exploit digital currencies to move illicit funds and avoid detection.

Providing regulatory relief through simplifying and streamlining regulatory requirements is consistent with the Government's agenda to reduce unnecessary regulatory burden, cut red tape, and reduce the costs incurred in complying with Commonwealth regulation.

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

[13] See the FATF's *Guidance for a risk-based approach to virtual currencies* for further information on how jurisdictions around the world have approached virtual currencies. Financial Action Task Force, *Guidance for a risk-based approach to virtual currencies*, June 2015, FATF Guidance for a RBA to Virtual Currencies.

3. Options to achieve the objective

Regulating digital currencies under the AML/CTF regime

This RIS proposes three policy options to address the ML/TF risks arising from the non-regulation of digital currency exchange providers under the AML/CTF regime.

- **Option 1: Maintain the status quo.** This option would involve no change to the current regulatory requirements under the AML/CTF Act and digital currency exchange providers would continue to operate outside of the AML/CTF regulatory framework.
- **Option 2: Light touch regulation under the AML/CTF regime.** This option would involve applying some of the AML/CTF obligations to digital currency exchange providers.
- **Option 3: Full regulation under the AML/CTF regime.** This option would involve imposing all obligations under the AML/CTF regime on digital currency exchange providers.

Impacts

Option 1 – Maintain the status quo

Option 1 would not assist with mitigating the ML/TF risks associated with the activities performed by digital currency exchange providers.

The Australian Digital Currency Commerce Association (ADCCA) is an industry body representing those in the digital currency industry and has established a mandatory Code of Conduct for its members that includes, among other things, guidance on measures for protecting their services from misuse for ML/TF purposes. It also includes a certification process for compliance with the Code of Conduct and members are subject to regular independent reviews.

Membership of ADCCA is voluntary and the Code of Conduct does not provide for the reporting of suspicious matters and threshold transactions to AUSTRAC.

Option 1 would allow criminal interests to establish or control a digital currency exchange business and/or continue to exchange digital currencies for fiat currencies (currency established as money by government regulation or law) anonymously, and launder illicit funds quickly with minimal barriers. Financial intelligence on the movements of illicit funds using convertible digital currencies would not be tracked resulting in a significant intelligence gap.

The comprehensive consultation processes conducted during the course of the review and in the development of Phase 1 revealed that digital currency exchange providers generally did not support this option. These businesses considered that maintaining the status quo would fail to sufficiently mitigate the ML/TF risks associated with the sector, undermining the standing and reputation of, and public confidence in, the sector.

Option 2 - Light touch regulation under the AML/CTF regime

Option 2 focuses on activities performed by digital currency exchange providers and imposes light touch regulation.

Light touch AML/CTF regulation could involve imposing the following obligations:

- enrol with AUSTRAC
- customer due diligence
- suspicious matter reporting, and
- record-keeping.

Option 2 would have a regulatory impact on approximately 16 Australian digital currency exchange businesses. These businesses would have to enrol with AUSTRAC before providing a designated service and implement customer identification and verification processes that comply with the requirements of the AML/CTF Act and Rules. The businesses would also have an obligation to lodge suspicious matter reports with AUSTRAC in accordance with the requirements of the AML/CTF Act and Rules and comply with the Australian Privacy Principles in relation to any personal information collected under the AML/CTF regime.

The obligation to keep records of customer due diligence procedures and transactions is likely to have a modest regulatory impact and would be consistent with similar obligations under corporations and taxation laws.

The majority of digital currency exchange businesses operate a fully digital model and already conduct CDD using e-verification processes to support know your customer (KYC), which significantly reduces the impost on these businesses. The minimal imposition of customer due diligence requirements on the sector would act as a deterrent for criminals seeking to launder illicit funds using digital currencies. The reporting of suspicious matters by the sector would provide AUSTRAC with valuable information and form the basis of actionable financial intelligence for partner agencies.

The nature of the operations of digital currency exchange providers means that there is no utility or benefits from imposing an obligation to report international funds transfer instructions (IFTIs) to AUSTRAC. Under the AML/CTF Act, the 'sender' of an IFTI transmitted out of Australia, or the 'recipient' of an IFTI transmitted into Australia, must report the instruction to AUSTRAC within 10 business days after the day the instruction was sent or received. These reports allow AUSTRAC to track movements of funds in and out of Australia.

It would be impractical to apply IFTI reporting obligations to digital currency exchange providers because they have no visibility of the location to where digital currencies are sent, resulting in an intelligence gap. For example, digital currency exchange providers will not know the location of the bitcoin address to which a customer's bitcoin is sent because there is no geographical data attached to a bitcoin address (which is an identifier of 26-35 alphanumeric characters). In the instance in which a digital currency exchange provider will be expected to transfer fiat currency to a nominated bank account overseas, this IFTI will be reported by the digital currency exchange provider's bank.

A disadvantage of Option 2 is that it would also not require digital currency exchange providers to report threshold transactions. There are also a number of other disadvantages associated with the light touch regulatory approach under Option 2. These relate to digital currency exchange providers not having obligations to:

- register with AUSTRAC, and
- develop, implement and maintain an AML/CTF program.

Under the FATF international standards, the AML/CTF program is a cornerstone obligation which establishes the operational framework and toolkit for the business to meet its ongoing compliance and risk-management obligations. Under the AML/CTF Act, an AML/CTF program must provide for:

- an ML/TF risk assessment, which should be reviewed and updated periodically
- approval and ongoing oversight by boards (where appropriate) and senior management
- appointment of an AML/CTF compliance officer
- regular independent review
- an employee due diligence program
- an AML/CTF risk awareness training program for employees
- policies and procedures for the reporting entity to respond to and apply AUSTRAC feedback

- systems and controls to ensure the entity complies with its AML/CTF reporting obligations
- a framework for identifying customers and beneficial owners of customers so the regulated business can be reasonably satisfied a customer is who they claim to be
- ongoing customer due diligence procedures, which provide for the ongoing monitoring of existing customers to identify, mitigate and manage any ML/TF risks (including a transaction monitoring program and an enhanced customer due diligence program), and
- collecting and verifying customer and beneficial owner information.

The requirement for an AML/CTF program is also important for building and embedding a culture of compliance within regulated businesses at all levels of the organisation. It requires regulated businesses to identify and understand the ML/TF risk they face and have internal controls and systems in place to mitigate and manage those risks.

Light touch regulation and international best practice

In view of the ML/TF risks associated with digital currency exchange providers, light touch regulation of the sector is inconsistent with international best practice. The FATF considered the potential AML/CTF risks of virtual currencies such as digital currencies in 2014 and concluded that digital currencies 'provide a powerful new tool for criminals, terrorist financiers and other sanctions evaders to move and store illicit funds, out of the reach of law enforcement'.[14] At a global level, more and more countries are recognising and understanding the ML/TF risks associated with digital currencies and taking steps to fully regulate the sector under AML/CTF regimes.

In March 2013, the US Financial Crime Enforcement Network (FinCEN) released interpretive guidance stating that all virtual currency exchanges and administrators are money service businesses and are therefore subject to its AML/CTF registration, reporting, and recordkeeping requirements.[15] The US has already taken enforcement action against virtual currency firms for breaching these obligations.[16]

In August 2015, the State of New York's 'BitLicense' regime for New York-based digital currency businesses came into effect.[17] This regulatory framework contains fundamental AML/CTF obligations including the requirement to obtain a license and to have an AML/CTF program, CDD procedures and to observe suspicious transaction reporting requirements.

In June 2014, Canada also amended its AML/CTF law to treat dealers in digital currencies as money service businesses.[18] The amendments mean dealers in digital currency will be subject to requirements relating to AML/CTF programs, record keeping, verification procedures, PEPs, suspicious transaction reporting and registration.

As a general rule, the FATF standards only permit exemptions from the suite of AML/CTF obligations for situations which have been formally assessed as posing a demonstrated low or negligible ML/TF risk. As activities involving digital currencies do not pose a low ML/TF risk, light touch regulation is unlikely to sufficiently mitigate the ML/TF risks, or bolster business and consumer confidence in the sector.

Option 3 - Full regulation under the AML/CTF regime

Option 3 provides for a full suite of obligations commensurate with the recognised ML/TF risks posed by digital currencies and in accordance with global best practice. This is the preferred option.

[14] FATF Report - Virtual Currency - Key Definitions and Potential AML/CTF risks; at 5.
[15] Financial Crimes Enforcement Network*, Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies, FIN-2013-G001*, 18 March 2013, http://fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf.
[16] See for example, Financial Crimes Enforcement Network, 5 May 2015, *FinCEN fines Ripple Labs Inc. in first civil enforcement action against a virtual currency exchanger,* FinCEN fines Ripple Labs Inc., (accessed 15 January 2016).
[17] New York State Department of Financial Service, 3 June 2015 *NYDFS announces final BitLicense framework for regulating digital currency firms*, NYDFS announces final BitLicense framework, (accessed 15 January 2016).
[18] Division 19 (Money laundering and terrorist financing) of *Economic Action Plan 2014 Act, No. 1*, EAP - Division 19 (ML/TF).

Under this option, the regulation of digital currency exchanges adopts the following obligations for the regulation of remittance service providers:

- enrolment with AUSTRAC
- registration with AUSTRAC (a scheme which requires a person seeking registration to provide the AUSTRAC CEO with information relevant to their suitability for registration)
- establish, implement and maintain an AML/CTF program including customer due diligence
- report threshold transaction and suspicious matter reports, and
- record keeping.

The full suite of obligations to be imposed under Option 3 is likely to encourage and embed a culture of compliance within the sector and establish robust controls to mitigate the ML/TF risks. Further, this option aligns with the current obligations for the majority of reporting entities under the AML/CTF framework

The registration process allows the AUSTRAC CEO to assess the suitability of a person, and their key personnel, to operate a digital currency exchange. Applicants must provide information about their criminal history and the details of any beneficial owners of the business, allowing the AUSTRAC CEO to ensure that persons who pose significant ML/TF risks are not permitted to provide digital currency exchange services. The process also ensures that AUSTRAC has sufficient knowledge about who is operating in the sector so that it can better carry out its regulatory functions and provide assistance to reporting entities.

The registration scheme will give the AUSTRAC CEO the power to refuse, cancel or suspend the registration of a digital currency exchange in response to serious non-compliance or in circumstances where there is an unacceptable ML/TF risk.

While it was not possible to quantitatively estimate the benefits of Option 3, robust AML/CTF regulation is likely to bolster community safety, national security and the reputation of Australian businesses in highly competitive overseas markets. It will provide a strong deterrent for criminals seeking to launder illicit funds using convertible digital currencies. Criminals seeking the services of these businesses would be subject to customer due diligence procedures and have their transactions monitored on an ongoing basis. Valuable information about transactions that are suspicious and transactions involving cash that equal or exceed $10,000 would be reported to AUSTRAC and used to produce actionable intelligence to enable law enforcement, national security and intelligence agencies to track and seize illicit funds moved from place to place as digital currency. Seizure of these illicit funds disrupts criminal activity, taking the profit out of crime and preventing the reinvestment of these illicit funds in additional criminal activity.

Consultation with industry indicates that the sector generally supports Option 3 because robust AML/CTF regulation will bolster public and consumer confidence in the sector.

In terms of costs, the AML/CTF obligations to be imposed under Option 3 broadly correspond to requirements in the digital currency sector's Code of Conduct introduced by the industry association, the Australian Digital Currency Commerce Association (ADCCA). This Code of Conduct states that "ADCCA Certified Digital Currency Businesses must comply with the Sanctions Law and applicable AML/CTF Law, or to the extent that AML/CTF Law does not apply to them, must voluntarily comply with so much of the AML/CTF Law as would be applicable if the AML/CTF Law applied to Digital Currency Businesses."[19] The ADCCA Code of Conduct requires certified businesses to conduct ongoing customer due diligence procedures, to collect and verify customer and beneficial ownership information, to appoint an AML/CTF compliance officer and to make employees aware of the ML/TF risks of the business.

[19] The Australian Digital Currency Commerce Association, *Australian Digital Currency Industry Code of Conduct*, November 2016 ADCCA Code of Conduct (accessed 05/05/2017).

Option 3 would have a regulatory impact on approximately 16 Australian digital currency exchange businesses although this is minimised as the majority of digital currency exchange businesses operate a fully digital model and already conduct CDD using e-verification processes to support KYC. Approximately half of the 16 businesses are ADCCA members. Separating the estimated costs for the proposed reforms from 'business as usual' costs (that is, the costs that businesses incur as a result of voluntarily complying with the Code of Conduct) has been challenging. Quantifying costs is also difficult because regulated businesses are permitted to adopt a risk-based approach to compliance under the AML/CTF regime. This enables regulated businesses to individually tailor their AML/CTF programs in proportion to the ML/TF risks they face.

In view of industry's support for AML/CTF regulation of the sector, and the willingness of the industry to meet fundamental AML/CTF obligations without regulation (through the ADCCA Code of Conduct or otherwise), it is unlikely that the regulatory cost of AML/CTF regulation will result in the closure of digital currency exchange providers. Moreover, the impacts on consumers are likely to be modest if the majority of digital currency exchange providers already have AML/CTF practices in place.

4. Impact of the options

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

- digital currency exchange providers (approximately 16 entities)
- AUSTRAC, and
- consumers.

The impact of Option 1 is not addressed in detail in this RIS because it does not impose any regulatory obligations on the sector.

Compliance costs

There are compliance costs for industry including consumers under Options 2 and 3. These compliance and consumer costs are outlined in detail in the table at **Attachment B.**

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 will pass part of these costs to consumers.

5. Regulatory costs and offsets estimate table

The following table provides a summary of the estimated overall annualised cost and savings over 10 years of the regulatory impacts/offsets identified in the previous section. The assumptions used to estimate the cost/offsets are outlined in **Attachment B**.

Option 2[20]

Average annual regulatory costs (from business as usual)				
Change in costs	Business	Community Organisations	Individuals	Total change in cost
Total, by sector	$ 565,746	$61,008	$ Nil	$626,754
Cost offset ($ million)	Business	Community organisations	Individuals	Total, by source
Deregulation of CIT sector[21]	$(32,641,401)	$ ($41,850)	$ Nil	$(32,683,251)
Correspondent banking[22]	$(9,028)	Neutral	$ Nil	$(9,028)
DBG concept change[23]	$(3,987,549)	Neutral	$ Nil	$(3,987,549)
Deregulation of insurance intermediaries under FTR Act[24]	$(55,588)	$(13,198)	$ Nil	$(68,786)
Are all new costs offset? **X Yes, costs are offset ☐ No, costs are not offset ☐ Deregulatory—no offsets required**				
Total (Change in costs – Cost offset) ($million) = $(36,121,860)				

[20] The source of the data for digital currencies has been collated from research and also engagement with the Australian Digital Currency and Commerce Association including a number of ADCCA members who currently operate digital currency businesses.
[21] The source of data was developed from engagement with CIT sector representatives (reporting entities) as well as AUSTRAC data.
[22] The source of data is based on feedback received from industry during consultations on the Review of the AML/CTF Act and AUSTRAC data.
[23] The source of data is from transaction reports submitted to AUSTRAC from reporting entities and feedback from industry.
[24] The source of data is from transaction reports submitted to AUSTRAC from cash dealers who provide insurance services excluding motor vehicle dealers.

Option 3[25]

Average annual regulatory costs (from business as usual)				
Change in costs	Business	Community Organisations	Individuals	Total change in cost
Total, by sector	$601,213	$61,008	Nil	$662,221
Cost offset ($ million)	Business	Community organisations	Individuals	Total, by source
Deregulation of CIT sector[26]	$(32,641,401)	$(41,850)	Nil	$(32,683,251)
Correspondent banking[27]	$(9,028)	Neutral	Nil	$(9,028)
DBG concept change[28]	$(3,987,549)	Neutral	Nil	$(3,987,549)
Deregulation of insurance intermediaries under the FTR Act[29]	$(55,588)	$(13,198)	Nil	$(68,786)
Are all new costs offset? **x Yes, costs are offset □ No, costs are not offset □ Deregulatory—no offsets required**				
Total (Change in costs – Cost offset) ($million) = $(36,086,393)				

[25] The source of the data for digital currencies has been collated from research and also engagement with the Australian Digital Currency and Commerce Association including a number of ADCCA members who currently operate digital currency businesses.
[26] The source of data was developed from engagement with CIT sector representatives (reporting entities) as well as AUSTRAC data.
[27] The source of data is based on feedback received from industry during consultations on the Review of the AML/CTF Act and AUSTRAC data.
[28] The source of data is from transaction reports submitted to AUSTRAC from reporting entities and feedback from industry.
[29] The source of data is from transaction reports submitted to AUSTRAC from cash dealers who provide insurance services excluding motor vehicle dealers.

6. Who will you consult about the options and how will you consult WITH them?

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 D** 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 E**.

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

Consultation on the detail of the review recommendations prioritised for implementation under Phase 1 commenced in December 2016 with the release of separate consultation papers for industry and government. Eleven submissions were received from industry and six submissions from government agencies. The submission process was followed by meetings with industry bodies representing the banking (Australian Bankers Association), financial (Australian Financial Markets Authority), financial planning (Financial Planners Association of Australia), casino (Australian casinos legal representative) and digital currency (ADCCA and FinTech Australia) sectors to discuss issues and concerns raised about the detail of reform proposals. The Attorney-General's Department also met with representatives from MoneyGram and RIA (remitters).

Meetings were also held with government agencies.

Discussions with the digital currency exchange service providers and representative industry bodies explored regulatory options for the sector. Industry's initial preference was to codify the ADCCA Code of Conduct in legislation to give it the force of law, and for ADCCA to co-regulate the sector for AML/CTF purposes with AUSTRAC. This regulatory option was proposed to avoid regulatory lag to ensure this rapidly-evolving industry's compliance obligations were efficiently designed and could be flexibly adapted in the face of technological progress. However, this proposal was not pursued as a viable option as all digital currency exchange providers are not members of ADCCA. In addition, this option was unlikely to instil the same level of public confidence in the sector as regulation under the AML/CTF Act. It was also noted and accepted by many digital currency providers that the use and application of binding AML/CTF Rules in the regulation of this sector will provide the desired level of flexibility to avoid regulatory lag.

The suite of obligations under the AML/CTF regime, and their applicability to the digital currency exchange sector, were also discussed during consultations. For instance, following consultation with industry, it became clear that digital currency exchange providers have no visibility of the location to which certain digital currencies (e.g. Bitcoin) are sent. For this reason, the regulatory options for the sector do not include imposing an IFTI reporting obligation, as it would be impractical for the sector to comply.

In discussing regulatory options with the sector, a key concern for digital currency exchange providers was that the imposition AML/CTF regulation should mitigate the ML/TF risks and bolster public confidence without unduly impeding the progress of the fledgling sector.

If the Bill is passed by Parliament, the Attorney-General's Department, in partnership with AUSTRAC, will continue to engage with industry and government on implementation issues.

Newly regulated digital currency exchange providers would not have to comply with AML/CTF obligations until at least six months after the assent of the Bill. This will allow AUSTRAC to develop, in consultation with the

sector, industry specific guidance and Rules that set out the details of the obligations to assist digital currency exchange providers to understand and comply with their obligations.

The Attorney-General's Department will consult with industry about an appropriate implementation period. If the initial six months period from the date of Royal Assent to the commencement of the amendments is insufficient, the Attorney-General's Department will consider requesting that the Minister make a 'policy principle period' for a further 12 months. This 'policy principle period' will provide digital currency exchange providers with a period of time in which they can meet their compliance obligations under the AML/CTF Act without the possibility of criminal sanction by the AUSTRAC CEO. However, in this time, the AUSTRAC CEO would be empowered to pursue a civil penalty for breaches of AML/CTF obligations by digital currency providers only where the service provider has manifestly failed to take steps towards compliance. This will reassure digital currency exchange providers that they can work with the regulator to meet their compliance obligations in good faith, without being penalised.

The commencement of other measures will be staggered to allow AUSTRAC to develop the appropriate AML/CTF Rules and guidance to support industry compliance with new requirements. AML/CTF Rules are developed by AUSTRAC and subject to a public consultation process. This includes the public release of new draft Rules for comment.

The Attorney-General's Department will continue to engage with industry and government agencies through the consultative forums that support the implementation of the review recommendations. These are the AML/CTF Industry Consultation Council and the AML/CTF Co-ordinating Committee.

7. Implementation and review

Delayed commencement

It is proposed that the Bill would commence six months from the date of Royal Assent to enable the digital currency exchange sector to implement systems and controls to comply with AML/CTF obligations.

Policy principle to govern transition period

Under section 213 of the AML/CTF Act, the Minister may give written policy principles to the AUSTRAC CEO about the performance of the CEO's functions. Sub-section 213(2) provides that the Minister must table a copy of the policy principles in each House of Parliament within 15 sitting days of providing them to the AUSTRAC CEO.

Policy principles are not legislative instruments.

It is proposed that the Minister for Justice approve a policy principle that will apply to newly regulated digital currency exchange providers. This policy principle would apply for the 12 month period following commencement of the Bill.

The policy principle would outline a transition period for the newly regulated businesses, setting out obligations and expectations for newly regulated businesses. The transition period will enable the businesses to implement a plan to meet their compliance and reporting obligations, and achieve full compliance, by the end of the 12 month policy principle period.

AUSTRAC support and guidance

AUSTRAC will consult closely with the digital currency exchange sector to develop AML/CTF Rules for the sector and industry specific guidance.

Attachment A: Options

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

REGULATION OF THE DIGITAL CURRENCY EXCHANGE SECTOR			
	OPTION 1: MAINTAIN THE STATUS QUO	**OPTION 2:**	**OPTION 3:**
SUMMARY	No change to current background checking arrangements	• Light touch regulation under the AML/CTF Act • Enrolment with AUSTRAC • CDD obligations • Suspicious matter report (SMR) obligations • Record keeping	• Enrolment with AUSTRAC • Register with AUSTRAC • AML/CTF program • CDD obligations • SMR and threshold transaction report (TTR) obligations • Record keeping
RESOURCE IMPLICATIONS	No resource implications	Compliance costs for the sector	Compliance costs for the sector
ADVANTAGES	No advantages No regulatory cost for sector	AUSTRAC receives vital intelligence via the submission of SMRs. The sector is required to identify and verify their customers and assess the risks posed by its customers. Enhanced customer due diligence will ensure that the sector undertakes further investigations of high risk customers.	The sector identifies, understands and manages the risks associated with the exchange of digital currency. Australia is compliant with the FATF recommendations. Potential trust advantages AUSTRAC receives SMRs and TTRs to disseminate as financial intelligence to its partner agencies.
DISADVANTAGES	No improved standing The sector does not have a good understanding of its ML/TF risks. AUSTRAC does not receive information regarding cash transactions equal to or over AUD10,000. Australia is out of step with regulation in other jurisdictions and the FATF recommendations. Cost	The sector does not have a good understanding of its ML/TF risks. AUSTRAC does not receive information regarding cash transactions equal to or over AUD10,000. Australia is out of step with regulation in other jurisdictions and the FATF recommendations. Cost	Most costly (marginal) Potential disadvantage to unregulated jurisdictions

Attachment B: Regulatory costs and offsets

OPTION 2 **TOTAL $5,657,463**				
Item	**Cost**	**Number of affected entities**	**Total**	**Justification**
CAPITAL COSTS				
Understand AML/CTF Obligations	2 hours	7	14 hours	The code of conduct mirrors the AML/CTF obligations. It is assumed that 2 hours will be sufficient to review the new obligations and assess whether their existing processes are compliant with the AML/CTF obligations.
	7 hours	9	63 hours	It is assumed that 7 hours will be required to understand the AML/CTF obligations for those businesses that are not ADCCA members. Current AUSTRAC guidance material will assist with their understanding.
Enrol	1 hour	16	16 hours	Enrolment is conducted via an online form on the AUSTRAC website which takes most businesses up to 1 hour to complete.
Program development	-	-	-	
IT Upgrades	$3,000	12	$36,000	It is assumed that the 12 businesses operating with e-verification would require minimal IT updates/upgrades.
	$10,000	4	$40,000	Allows for integration of e-verification costs, TMP and reporting for those businesses not currently operating a fully digital model.

OPTION 2 **TOTAL $5,657,463**				
External advice/consultants	$2,000	12	$24,000	
	$4,000	4	$16,000	
ONGOING COSTS				
Threshold transaction reports	-	-	-	
Submit the suspicious matter report (SMR) to AUSTRAC	2 hours per SMR x 60 SMRs per entity per annum (TOTAL = 120 hours)	16	1920 hours per annum	Industry has indicated that they would report approximately 60 SMRs per annum. Completing the SMR process would take a maximum of 0.5 hours.
Compliance Report and updates to AML/CTF program	-	-	-	
AUSTRAC Compliance Audit	5 hours per entity per annum	2	10 hours per annum	Based on the size of the sector, AUSTRAC would conduct compliance assessments of no more than 2 providers per annum.
CDD obligations: e-verification	6000 new customers per annum per entity x $3.50 per individual search using e-verification providers (TOTAL = $21,000)	4	$84, 000 per annum	There are currently 12 businesses operating as a digital currency exchange and identifying their customers using e-verification processes. These businesses have chosen to adopt these measures as part of their fraud prevention, readiness for AML/CTF compliance and also to provide assurance to the banks that the providers are adopting appropriate measures to mitigate fraud, sanctions and other risks. Confirmed 12 digital currency businesses operate a fully digital model and already conduct CDD using e-verification processes. This RIS allows for another 4 digital

OPTION 2 **TOTAL $5,657,463**				
				currency providers for which we could not confirm that they have adopted any CDD measures. E-verification rates for an individual customer vary. We have assumed that an average cost of $3.50 per search would apply for this industry.
Enhanced CDD Obligations – including mismatches/follow up	15% percent of all new customers (900 customers) per annum per entity x 0.50 hours per customer (TOTAL = 450 hours)	4	1,800 hours per annum	These costings allow for any manual intervention to identify the customers, for example mismatching via e-verification, follow up communication with customers for those deemed higher risk.
Identity verification service annual subscription	No cost	12	No cost	Confirmed 12 digital currency businesses operate a fully digital model and already conduct CDD using e-verification processes.
	$5,000 per entity per annum	4	$20,000	This is an average cost sourced from industry.
CUSTOMER COSTS				
Costs to the customer to provide CDD information	24,000 new customers affected per annum x 0.05 hours (3 mins) per customer. (TOTAL: 1200 hours) 20% of all new customers (4,800 new customers) x 0.16 (10 minutes) (TOTAL: 768 hours)		E-verification: $37,200 Follow up processes: $23,808 TOTAL: $61,008 per annum	Based on figures provided above, it is assumed there are 6000 new customers per the 4 digital currency entities that do not currently require this information. It is assumed that it would take 3 mins to provide the necessary information for e-verification per customer. It is assumed that 20% of new customers may require follow up via a phone call or request for further information via email and that this would take an average of 10 minutes to complete per customer.

OPTION 3 **TOTAL: $6,012,137**				
Item	**Cost**	**Number of affected entities**	**Total**	**Justification**
CAPITAL COSTS				
Understand AML/CTF Obligations	4 hours	7	28 hours	As per option 2 the code of conduct mirrors the AML/CTF obligations. However, additional hours have been included to cover off the additional obligations proposed in this option.
	8 hours	9	72 hours	As per option 2.
Enrol/Register	3 hours	16	48 hours	Enrolment and registration is completed in one form. AUSTRAC estimates that it takes most businesses no more than 3 hours to complete.
Program development	4 hours	7	28 hours	ADCCA members hours reduced due to the obligations which mirror the Code of Conduct.
	10 hours	9	90 hours	Allows for additional time for non-ADCCA members to understand their obligations and develop an AML/CTF program. AUSTRAC guidance will assist.
IT Upgrades	$3,000	12	$36,000	ADCCA members have systems in place but we have allowed for additional IT upgrades.
	$10,000	4	$40,000	Non-ADCCA members – although the sector's business model is based on digital commerce we have allowed for additional IT upgrades to comply with the AML/CTF obligations.

OPTION 3 **TOTAL: $6,012,137**				
External advice/consultants	$2,000	12	$24,000	ADCCA members
	$5,000	4	$20,000	Non-ADCCA members
ONGOING COSTS				
Submit the threshold transaction report to AUSTRAC	0.25 hours per transaction x 15 TTR reports per entity per annum (TOTAL = 3.75 hours)	16	60 hours per annum	99% of cash transactions (which would only be 5% of all transactions) would be below the $10,000 threshold. Majority of providers don't accept cash at all.
Submit the suspicious matter report to AUSTRAC	2 hours per transaction x 60 SMR reports per entity per annum (TOTAL = 120 hours)	16	1,920 hours per annum	As per option 2
Compliance Report and updates to AML/CTF program	4 hours per entity per annum	16	64 hours per annum	A compliance report is required to be completed and submitted to AUSTRAC annually. This estimation is based on existing processes. Updates to AML/CTF programs are only required where there are amendments to the Rules, guidance issued by AUSTRAC or deficiencies identified through compliance visits.
AUSTRAC Compliance Audit	80 hours per entity per annum	2	160 hours per annum	As per option 2 however additional hours are required to assess the entities compliance with its obligations.

OPTION 3 **TOTAL: $6,012,137**				
CDD obligations: e-verification	6000 new customers per annum per entity x $3.50 per individual search (TOTAL = $21,000)	4	$84,000 per annum	As per option 2
Enhanced CDD Obligations – including mismatches/follow up	15% percent of all new customers (900 customers) per annum per entity x 0.50 hours per customer (TOTAL = 450 hours)	4	1,800 hours per annum	As per option 2
Identity verification service annual subscription	No cost	12	No cost	ADCCA members have existing IDV services in place and undertake this process as part of their digital business model.
	$5,000 per entity per annum	4	$20,000	Non-ADCCA members may need to subscribe to these services although it is likely that these businesses already have this process in place given their digital business model.

OPTION 3 **TOTAL: $6,012,137**				
CUSTOMER COSTS				
Costs to the customer to provide CDD information	24,000 new customers affected per annum x 0.05 hours (3 mins) per customer. (TOTAL: 1200 hours) 10% of all new customers (4,800 new customers) x 0.16 (10 minutes) (TOTAL: 768 hours)		E-verification: $37,200 Follow up processes: $23,808 TOTAL: $61,008	As per option 2.

DEREGULATION OF THE CIT SECTOR – OFFSET **TOTAL: (326,414,010)**				
Item	**Savings**	**Number of affected entities**	**Total**	**Justification**
CAPITAL SAVINGS				
Understand AML/CTF Obligations	-	-	-	
Enrol	-	-	-	
Register	-	-	-	
Program development	-	-	-	
IT Upgrades	-	-	-	
External Legal Advice	-	-	-	
ONGOING SAVINGS				
Submit the threshold transaction report to AUSTRAC	0.17 hours per transaction x 1,299,596 transaction reports per annum (TOTAL = 220,931.32 hours per annum) 0.25 hours per transaction x 164,257 transaction reports per annum submitted by the remaining 100 entities (TOTAL = 41064.25 hours per annum)	submitted by the 2 major CIT operators per annum submitted by the 110 smaller CIT operators per annum	(261, 995.57 hours per annum in total for the whole CIT sector)	This calculation is based on the number of reports submitted to AUSTRAC by the whole sector in 2016 and the number of CIT entities enrolled with AUSTRAC. 2 of the major CIT operators submit approximately 89% of all TTRs to AUSTRAC. These TTRs are submitted online and manually (with data to be pulled from a range of different sources for discrete pieces of information). It is assumed that it takes on average 10 minutes to gather the information, enter the information and submit the report to AUSTRAC for both of these

DEREGULATION OF THE CIT SECTOR – OFFSET **TOTAL: (326,414,010)**				
				processes. The other CIT operators are smaller entities and rely on less automated processes to submit TTRs to AUSTRAC. It is assumed that this process takes on average 15 minutes to complete.
Submit the suspicious matter report to AUSTRAC	2 hours per transaction x 40 suspicious matter reports (sector wide) per annum (based on 2016 figures) (TOTAL = 80 hours)	The average number of REs that have submitted SMRs (4 entities)	(320 hours per annum)	This calculation is based on the number of reports submitted to AUSTRAC by the whole sector in 2016 and the number of CIT entities. Industry feedback verified that it takes on average 2 hours to complete an SMR (pulling the information together regarding their corporate customers and undertaking the investigations across the CIT business).
Compliance Report and updates to AML/CTF program	7 hours per entity per annum for 110 entities 150 hours per annum submitted by the two major entities	110 2	(770 hours per annum) (300 hours per annum)	As per digital currency costings for the smaller CIT businesses with a substantial increase for two major entities(based on the size of their operation)
AUSTRAC Compliance Audit	80 hours per entity per annum 14 hours per entity per annum	10 5	(800 hours per annum) (70 hours per annum)	Behavioural reviews are usually conducted for a number of smaller CIT providers.
CDD obligations	0.25 hours per new customer for 150 new customers per annum (TOTAL = 37.5 hours) 2 hours per new customer for 3 new customers per annum (TOTAL = 6 hours)	12 100	(450 hours per annum) (600 hours per annum)	E-verification and manual processes for larger entities. The average number of new customers sourced from AUSTRAC reporting. All manual processes for smaller entities.

DEREGULATION OF THE CIT SECTOR – OFFSET **TOTAL: (326,414,010)**				
Enhanced CDD Obligations (90% of customers requiring beneficial ownership checks, further verification)	2 hour per customer for 95% of all new customers (142.5 customers) (TOTAL = 285 hours) 5 hours per customer for 95% of all new customers (2.85 customers) (TOTAL = 14.25 hours)	12 100	(3,420 hours per annum) (1,425 hours per annum)	All customers would be subject to beneficial ownership requirements. E-verification would be used by larger entities with some manual work. All manual identification of beneficial owners by smaller entities.
Identity verification service (annual subscription and cost to IDV)	$10,000 per entity per annum	12	($120,000 per annum)	E-verification only costed for the larger businesses including costs to identify and verify customers.
CUSTOMER SAVINGS				
Customer savings	A total of 2700 new customers per year x 0.5 hours (TOTAL: 1,350 hours)		($41,850 per annum)	Based on the figures provided above, it is assumed that 2700 new customers will be on-boarded per annum by the CIT sector. The customer base for the CIT sector is predominantly non-individuals which requires additional CDD to be conducted to identify the beneficial owners of the company, trust etc. This RIS allows for 0.5 hours for the customer to provide the necessary information requested by the CIT operators during the on-boarding process.

CORRESPONDENT BANKING - OFFSET				
Item	**Savings**	**Number of affected entities**	**Total**	**Justification**
ONGOING SAVINGS				
Clarification of obligations	5 hours per entity per annum	15	(75 hours per annum)	This assumption is based on feedback received from industry during consultations on the Review of the AML/CTF Act.
CUSTOMER SAVINGS				
Neutral				

DESIGNATED BUSINESS GROUPS - OFFSET (39,875,499)				
Item	**Savings**	**Number of affected entities**	**Total**	**Justification**
ONGOING SAVINGS				
Cost saving for identifying and analysing a suspicious matters & submitting an SMR to AUSTRAC	2,366 SMRs submitted by REs within an existing DBG x 14 hours (TOTAL: 33,124 hours)	Reporting entities that formed more than one DBG (banking and finance sector)	33,124 hours per annum	78,876 suspicious matter reports were submitted to AUSTRAC in 2015-16. It is assumed that 3% of these SMRs were submitted by reporting entities that formed more than one DBG and therefore submitted duplicate reports for the same customer. It is assumed that forming a suspicion either manually or via an alert and also the process of investigating an SMR may take on average 14 hours to complete.
CUSTOMER SAVINGS				
Neutral				

Deregulating insurance intermediaries and general insurance providers under the FTR Act – OFFSET **TOTAL:** $**555,886**				
Item	**Cost**	**Number of affected entities**	**Total**	**Justification**
ONGOING COSTS				
Transaction reports submitted under the FTR Act	0.25 hours per transaction x 1,703 transaction reports (sector wide) per annum (based on 2016 figures) (TOTAL = 425.75 hours)	9 entities	(425.75) hours	This estimation is based on financial transaction reports submitted by 9 entities in this sector in 2016.
Maintaining compliance with obligations	2 hours per annum x per entity	9 entities	18 hours per annum	It is assumed that 2 hours is required per annum per entity to consider their ongoing compliance obligations under the FTR Act.
CUSTOMER SAVINGS				
Customer savings – 100 point check	1,703 customers per annum would require 100 point check under the FTR Act x 0.25 hours. (TOTAL:425.75 hours)		($13,198.25)	

Attachment C: Assumptions

The assumptions used to estimate the regulatory impact are set out in **Attachment B**.

Attachment D: List of submissions to AML/CTF Review

Accounting

Australian Auditing and Accounting Public Policy Committee

AML compliance

AML Master

GRC Institute

Banking

Australian Bankers Association

Australian Finance Conference

Australian Financial Markets Association

Customer Owned Banking Association

HSBC Australia Limited

1 confidential submission

Cash-in-transit

Australian Security Industry Association Limited

Mr Rick & Ms Anna Biela

Security Specialists Australia

2 confidential submissions

SNP Security

Financial planners

Mr Ashok Sherwal

Financial Planning Association of Australia

Gaming services industry

Australian Bookmakers' Association Pty Ltd

Australian Hotel Association

Australian Wagering Council

Casinos and Resorts Australasia

ClubsNSW/ClubsAustralia

Mercury Group Victoria Inc

Peter Shepherd

One confidential submission

Government (confidential)

Australian Crime Commission (two submissions)

Australian Customs and Border Protection Service

Australian Federal Police

Australian Security intelligence Organisation

Australian Taxation Office (two submissions)

Cyber & Identity Security Policy Branch, Attorney-General's Department

Department of Foreign Affairs and Trade

Department of Human Services

Inspector General of Intelligence and Security

NSW Crime Commission

NSW Police Integrity Commission

Office of the Australian information Commissioner

Treasury

Individuals and academia

Ms Anne Imobersteg Harvey

One confidential submission

Mr Douglas Allen

Faculty of Law, University of New South Wales

Mr Michael Robson

Professor Louis de Koker and Mr Kayne Harwood

Legal

Financial Services Committee, Law Council of Australia

One confidential submission

Law Council of Australia

Lenders

Capricorn Society Limited

Mortgage & Finance Association of Australia

National Financial Services Federation Ltd

SP AusNET

Managed investment schemes

Fawkner Property Pty Ltd

Fundhost Limited

New payment methods

Mr Kevin Beck (three submissions)

PayPal Australia Pty Ltd (appendices confidential)

Universal Gift Cards Pty Ltd

NGOs

Australian Privacy Foundation and Privacy International

Transparency International Australia

Uniting Church in Australia Synod of Victoria and Tasmania

Remitters

Capital Money Exchange Pty Ltd (confidential)

Eastern & Allied Pty Ltd/Hai Ha Money Transfer

Kapruka Pty Ltd

MoneyGram Payment Systems Inc.

Western Union

Salary packaging

McMillan Shakespeare Group

Superannuation

Association of Superannuation Funds of Australia Limited

Australian Institute of Superannuation Trustees

Financial Services Council

Technology providers

iSignthis Ltd (White Paper confidential)

One confidential submission

Attachment E: Stakeholder Engagement

STATUTORY REVIEW OF THE AML/CTF ACT

ENGAGEMENT WITH STAKEHOLDERS

ROUNDTABLE DATE	PARTICIPANTS
19 September 2015	
NGO sector	Uniting Church in Australia, Synod of Victoria and Tasmania Transparency International Australia Australian Council for International Development OXFAM
24 September 2015	
Gaming sector: Gaming machines	Australian Hotels Association ClubsNSW Mercury Group Victoria Inc ALH Group Pty Ltd
Gaming sector: Casinos	Casinos and Resorts Australasia
Gaming sector: Wagering	Australian Wagering Council Australian Bookmakers Association Limited TattsGroup
Cash-in-transit sector	Australian Security Industry Association Limited Linfox Armaguard Prosegur
25 September 2015	
Remittance sector: Large remitters	Western Union
Remittance sector: Small/medium remitters	UAE Exchange Hai Ha MoneyGram OzForex Group RIA
26 September 2015	
AML compliance sector	AML Master
2 October 2015	
AML compliance sector	Yarra Valley Associates
25 November 2015	
Banking sector: Australian Finance Conference	Australian Finance Conference Toyota Finance Australia Limited Pepper Group Marubeni Equipment Finance

ROUNDTABLE DATE	PARTICIPANTS
Banking sector: Australian Banking Association	Australian Bankers' Association Commonwealth Bank of Australia Macquarie Westpac ANZ ING Direct HSBC
19 November 2014	
Banking sector: Australian Financial Markets Association	Australian Financial Markets Association Western Union Bank of America Merrill Lynch Westpac 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

ROUNDTABLE DATE	PARTICIPANTS
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