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 currency providers for which we could not

OPTION 2 **TOTAL $5,657,463**				
				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