Australian Government

AUSTRAC

Privacy Impact Assessment

Amendments to Chapter 4 of the AML/CTF Rules

A FINANCIAL SYSTEM **FREE** FROM CRIMINAL ABUSE

Contents

1. Background

1.1 Purpose of this document

1.1.1 The Australian Transaction Reports and Analysis Centre (AUSTRAC) is undertaking a Privacy Impact Assessment (PIA) to assess the privacy impact of the proposed amendments to Chapter 4 of the Anti-Money Laundering and Counter-Terrorism Financing Rules (AML/CTF Rules), which will allow reporting entities to collect Know-Your-Customer (KYC) information from sources other than the customer. Currently, the AML/CTF Rules require reporting entities to collect KYC information directly from customers.

1.1.2 The PIA also seeks to identify mitigating privacy protections and processes in relation to the protection, use, storage and disclosure of this type of personal information. Industry may need to implement these to manage, minimise or eliminate material privacy impacts which are likely to occur if the proposed amendments are implemented.

1.1.3 The PIA has arisen from a request from the Office of the Australian Information Commissioner (OAIC), recommending that an Assessment be undertaken due to the concerns of the Commissioner that the proposed amendments will have a privacy impact on individuals and, therefore, should incorporate appropriate privacy protections.

1.1.4 Stakeholders have been consulted on the privacy implications of the proposed amendments. All industry submissions confirmed their awareness of privacy obligations in relation to the collection, use and disclosure of personal information. The proposed amendments will be progressed after the PIA process has been completed.

1.2 AUSTRAC

1.2.1 AUSTRAC is Australia's anti-money laundering and counter-terrorism financing (AML/CTF) regulator and specialist financial intelligence unit (FIU). In its role as AML/CTF regulator, AUSTRAC oversees compliance of Australian businesses with their obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) and *Financial Transactions Report Act 1988* (FTR Act). These businesses span financial services providers, the gambling industry and bullion dealers, under the AML/CTF Act, and 'cash dealers' under the FTR Act. The proposed amendments which are the subject of this PIA relate only to the AML/CTF Act regime, rather than the FTR Act.

1.2.2 In its role as Australia's FIU, AUSTRAC collects and analyses information provided by regulated entities and disseminates the resulting financial intelligence to law enforcement, national security, human services and revenue raising agencies, and certain international counterparts. This assists them in investigating and prosecuting

serious criminal activity including money laundering, terrorism financing, people smuggling, organised crime and tax evasion.

1.3 AML/CTF legislative regime

1.3.1 The AML/CTF Act was enacted to deter money laundering and terrorism financing. It covers financial, gaming and bullion services provided to customers by businesses (called 'reporting entities' in the AML/CTF Act).

1.3.2 Before providing these services ('designated services'), reporting entities must carry out a procedure (the applicable customer identification procedure (ACIP)) in order to verify a customer's identity.

1.3.3 The AML/CTF Act is supplemented by the AML/CTF Rules which may be made by the AUSTRAC CEO. Under section 229 of the AML/CTF Act, AML/CTF Rules are legally binding legislative instruments and prescribe in further detail matters allowed for under the Act.

1.4 Financial Action Task Force (FATF)

1.4.1 FATF is an independent inter-governmental body, established in 1989, which focuses on fighting money laundering, terrorism financing and other related threats to the integrity of the global financial system, by ensuring the effective implementation of legal, regulatory and operational measures. FATF develops and promotes international best practice standards (the FATF Recommendations) to combat global money laundering and terrorism financing and the financing of the proliferation of weapons of mass destruction. The AML/CTF Act and AML/CTF Rules are based upon the FATF Recommendations.

1.4.2 In February 2012, FATF released revised Recommendations that included those relating to Customer Due Diligence (CDD) upon which the customer identification requirements in the AML/CTF Rules are based.

1.4.3 AUSTRAC subsequently published draft amendments to the AML/CTF Rules based upon the revised Recommendations (the CDD amendments). After a consultative process which took place in 2013 and 2014 (including a Privacy Impact Assessment)[1], the AML/CTF Rules were amended and took effect on 1 June 2014.

1.5 Background to the proposed amendments to AML/CTF rules

1.5.1 Although the 2014 CDD amendments to the AML/CTF Rules related directly to the updated FATF Recommendations, industry submitted during the course of consultation that other amendments to Chapter 4 should be made that would

[1] *Enhanced Customer Due Diligence (CDD) Requirements – Privacy Impact Assessment (PIA)*. January 2015. Available at: http://www.austrac.gov.au/sites/default/files/documents/cdd_pia_may2014.pdf

enhance the AML/CTF regime while reducing regulatory burden. The Regulation Impact Statement (RIS) undertaken for those proposed amendments identified savings of $15.1 million per annum.[2]

1.5.2 One of these proposed amendments (and the subject of this PIA), relates to allowing reporting entities the discretion to collect identification information 'about' a customer rather than 'from' a customer, as is currently the case.

1.5.3 FATF Recommendation 10 (Customer Due Diligence) states that financial institutions (reporting entities) must undertake measures 'identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information'.[3] It is noted that FATF does not require that the 'reliable, independent source documents, data or information' be sourced only from the customer.

1.5.4 The obligation to identify and verify customers has been in operation since 12 December 2007, when Part 2 of the AML/CTF Act (Identification procedures) commenced operation. Part 2 prescribes the ACIP requirements in relation to customer identification and verification.[4] The ACIP comprises:

- identification of the customer, by collecting certain KYC information; and
- verification of the collected KYC information using 'reliable and independent documentation' or 'reliable and independent electronic data' or both.

1.5.5 Chapter 1 of the AML/CTF Rules contains an inclusive definition of 'reliable and independent documentation':

> ***reliable and independent documentation*** includes but is not limited to:
>
> (1) an original primary photographic identification document;
>
> (2) an original primary non-photographic identification document; and
>
> (3) an original secondary identification document.
>
> ***Note:*** *This is not an exhaustive definition. A reporting entity may rely upon other documents not listed in paragraphs (1) to (3) above as reliable and independent documents, where that is appropriate having regard to ML/TF risk.*

Each of these three types of documents are also separately defined in Chapter 1.

1.5.6 Chapter 4 of the AML/CTF Rules prescribes the ACIP that should be undertaken in relation to the following customer types, including a requirement that minimum KYC information must be collected and verified:

- individuals, including those operating as sole traders
- companies
- trustees of trusts

---

[2] *Regulation Impact Statement – Proposed Reform to Strengthen Customer Due Diligence*, May 2014, page ix. Available at: http://www.austrac.gov.au/sites/default/files/documents/cdd_ris_may2014.pdf

[3] *The FATF Recommendations* February 2012, page 14. Available at: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

[4] Section 32 (Carrying out the applicable customer identification procedure before the commencement of the provision of a designated service) of the AML/CTF Act.

- partners of a partnership
- incorporated or unincorporated associations
- registered co-operatives
- government bodies
- agents of customers
- beneficial owners of customers
- politically exposed persons

1.5.7 In response to the industry submissions made during public consultation on the CDD amendments, AUSTRAC developed and published draft amendments to Chapter 4. These were published on the AUSTRAC website for public consultation from 10 June 2015 to 8 July 2015 and are available on the Draft rules web page (http://www.austrac.gov.au/draft-aml-ctf-rules)

1.5.8 The draft amendments covered three issues:

- a further version of the amendments relating to the electronic safe harbour procedures for customers;
- allowing for the collection of KYC information from sources other than the customer; and
- extending current exemptions in relation to the carrying out of an applicable customer identification procedure to beneficial owners and politically exposed persons.

1.5.9 This PIA assesses the second issue relating to the collection of KYC information from sources other than the customer.

1.6 The privacy legislative regime

1.6.1 Section 6 of the *Privacy Act 1988* (Privacy Act) defines 'personal information' as follows:

> ***personal information*** means information or an opinion about an identified individual, or an individual who is reasonably identifiable:
>
> (a) whether the information or opinion is true or not; and
>
> (b) whether the information or opinion is recorded in a material form or not.

1.6.2 Common examples are an individual's name, signature, address, telephone number, date of birth, medical records, bank account details and commentary or opinion about a person.

1.6.3 The Privacy Act includes thirteen legally binding Australian Privacy Principles (APPs) which apply to 'APP entities'. An APP entity is either an 'agency' created by the Commonwealth government or an 'organisation' which covers individuals, body corporates, partnerships, unincorporated associations or trusts.

1.6.4 Subsection 6E(1A) of the Privacy Act imposes the requirements of that Act on all reporting entities in relation to AML/CTF Act related activities regardless of whether or not the Privacy Act would otherwise apply to the reporting entity. This means that all reporting entities need to comply with the APPs in their dealings with personal information, regardless of whether the personal information is sourced from a customer directly or from other sources.

1.6.5 The APPs are principles-based law. Each APP entity needs to apply the principles to its own situation. The APPs cover:

- the open and transparent management of personal information including having a privacy policy
- an individual having the option of transacting anonymously or using a pseudonym where practicable
- the collection of solicited personal information and dealing with unsolicited personal information including giving notice about collection
- how personal information can be used (including for direct marketing) and disclosed (including overseas)
- adopting, using and disclosing government related identifiers
- maintaining the quality of personal information
- keeping personal information secure
- right for individuals to access and correct their personal information

1.6.6 The APPs place more stringent obligations on APP entities when they handle 'sensitive information'. Sensitive information is a type of personal information and includes information about an individual's:

- health (including predictive genetic information)
- racial or ethnic origin
- political opinions
- membership of a political association, professional or trade association or trade union
- religious beliefs or affiliations
- philosophical beliefs
- sexual orientation or practices
- criminal record
- biometric information that is to be used for certain purposes
- biometric templates.

1.6.7 The AML/CTF Rules recognise and promote compliance with privacy obligations, including those relevant to the *Human Rights (Parliamentary Scrutiny) Act 2011.* For example, the following note appears at the end of every chapter of the AML/CTF Rules:

Reporting entities should note that in relation to activities they undertake to comply with the AML/CTF Act, they will have obligations under the Privacy Act 1988, including the requirement to comply with the Australian Privacy Principles, even if they would otherwise be exempt from the Privacy Act. For further information about these obligations, please go to OAIC website or call 1300 363 992.

1.6.8 In respect to Chapter 4, there are additional notes that address or highlight specific privacy issues and obligations. For example, in relation to beneficial owners and politically exposed persons, the following note was inserted as a result of the CDD amendments in 2014:

> ***Note**: Reporting entities should consider the requirements in the Privacy Act 1988 relating to the collection and handling of information about beneficial owners or politically exposed persons.*

1.7 Public consultation on the PIA

1.7.1 AUSTRAC released a draft PIA for public consultation for a 2 week consultation period, which closed on Wednesday 9 December 2015. While a total of four submissions were received in relation to the draft PIA, all industry submissions contained similar comments and observations. These comments and observations have been incorporated into this final PIA.

1.7.2 The final PIA was forwarded to the OAIC for consideration prior to publication.

1.8 Industry feedback on information to be collected from sources other than the customer

1.8.1 Industry submissions indicated that the regulatory benefit arising from being able to collect information from other sources about the customer, primarily arises with respect to non-individual customers, particularly in light of the increased obligations to verify the identity of the beneficial owners of such customers and politically-exposed persons. Non-individual entities include companies, associations, trusts and registered charities. Industry noted that the proposed amendments would enable them to simplify and streamline their data collection processes and save their customers time and money. Industry also noted that there were no significant opportunities to collect information about individuals, as there were limited reliable and independent sources for such information.

1.8.2 The industry submissions identified the following currently available potential sources of information about non-individual customers:

- Corporate registries (ASIC or overseas equivalent);
- Annual reports and other public documents issued by the company;
- Corporate websites;
- Australian Business Register (ABR);

- Foreign registration bodies;
- Professional association databases (where publicly available);
- Electoral rolls;
- Related group entities of the reporting entity;
- Third party KYC or credit check service providers, such as VEDA, Bloomberg, Thomson Reuters, etc.

One industry submission indicated that information could also be collected from an officer of a business customer (for example, the financial controller or asset procurement officer) about directors, shareholders and other officers as part of the customer identification and verification process.

1.8.3 For corporate entity customers, industry submitted that the following information could be obtained from sources other than the customer (for example, from the above sources or from an officer of these corporate entity customers):

- Full legal name;
- Date of incorporation;
- Registered and principal place of business address details;
- ACN, ABN or other identification number;
- Business or trading names;
- Current shareholding/beneficial ownership details;
- Director and office-bearer information; and
- Listing information (where applicable).

2. Assessment of the privacy impact

2.1 The proposed amendments to Chapter 4 will allow for the collection by reporting entities of KYC information about customers from sources other than the customer.

2.2 The RIS details how this would be undertaken in some circumstances:

> *... the reporting entity would have flexibility in its approach to collection and verification of customer information including obtaining initial information from an independent source, pre-fill parts of the customer application form and then check the information with the customer for verification purposes.*[5]

2.3 The proposed amendments will have impacts on the handling of personal information by, and privacy procedures of, reporting entities and on the privacy of affected individuals (about whom personal information will be collected by the reporting entity for the purposes of carrying out an ACIP).

2.4 It is noted that Chapter 4 requires the collection of information about individuals who are customers, but also individuals who are not customers. For example, in regard to non-individual customers (such as trusts, companies and partnerships), reporting entities are required to collect and verify information about directors and trustees.

2.5 The proposed amendments will not have privacy impacts on AUSTRAC's handling of personal information, as AUSTRAC is not responsible for collecting personal information to identify and verify customers of reporting entities under the AML/CTF Act.

2.6 AUSTRAC considers that all Australian Privacy Principles are relevant to the privacy assessment, although APP 3 (Collection of solicited personal information) is particularly relevant to the privacy assessment. The Table below at paragraph 2.32 provides an overview of each APP and the potential impact. Actual privacy impacts on individuals as a result of these amendments are largely dependent on whether, and how, a reporting entity implements the proposed amendments into its customer identification procedures.

2.7 APP 3 enables individuals to exercise greater control over their personal information and decide how much personal information will be shared or revealed to others. The proposed amendments may impact on the control individuals currently have over their personal information as it may not be collected directly from the individual by the reporting entity, especially where they are associated with non-individual entities which are customers of a reporting entity.

2.8 In relation to non-agency APP entities (such as reporting entities), APP3 provides that personal information about an individual (in this case, information held by third parties):

- may only be collected where it is reasonably necessary for the organisation's functions or activities; and

[5] *Regulation Impact Statement – Proposed Reform to Strengthen Customer Due Diligence*, May 2014, page ix. Available at: http://www.austrac.gov.au/sites/default/files/documents/cdd_ris_may2014.pdf

- must only be collected from the individual concerned unless it is unreasonable or impracticable to do so.

2.9 AUSTRAC considers that the exceptions in APP3.6(b) may apply to collections of personal information made under the proposed amendments in certain circumstances.

2.10 Paragraph 3.65 of the APP guidelines[6] clarifies the phrase 'unreasonable or impracticable to collect directly from the individual':

> 3.65 Whether it is 'unreasonable or impracticable' to collect personal information only from the individual concerned will depend on the circumstances of the particular case. Considerations that may be relevant include:
>
> - whether the individual would reasonably expect personal information about them to be collected directly from them or from another source
> - the sensitivity of the personal information being collected
> - whether direct collection would jeopardise the purpose of collection or the integrity of the personal information collected
> - any privacy risk if the information is collected from another source
> - the time and cost involved of collecting directly from the individual. However, an APP entity is not excused from collecting from the individual rather than another source by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable or impracticable will depend on whether the burden is excessive in all the circumstances.

2.11 Industry submissions indicated that information will be collected from sources other than the customer in circumstances where it is unreasonable or impracticable to collect information directly from the customer. Examples provided included:

- When it would be unreasonable to expect the reporting entity to approach the individual themselves, rather than collecting information from an officer of a non-individual entity in relation to which that individual is associated;
- When the individual becomes a customer of an entity within the same group of related entities and another entity in that group already holds that individual's personal information and appropriate privacy consents. (Further discussion about 'consent' is included in paragraphs 2.17 – 2.20 below).

2.12 The information will generally be collected at the time of 'on-boarding', and periodically as part of customer due diligence. This generally appears to be consistent and in accordance with the requirements of APP3.

2.13 Collecting the personal information about non-customers (for example, individuals associated with non-individual customers) from other sources may pose some new

[6] Available at: http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-3-app-3-collection-of-solicited-personal-information#_Toc381351272

privacy risks, which reporting entities should consider when assessing whether it is 'unreasonable or impracticable' to collect directly from the relevant individual. In some cases, it is unlikely that an individual who is not a customer of a reporting entity (and does not otherwise have a direct business relationship with the reporting entity) would reasonably expect the reporting entity to collect their personal information, let alone from a third party. Reporting entities will need to have appropriate privacy systems, policies and procedures in place to ensure that personal information about these non-customer individuals is collected from third parties only in appropriate circumstances and, where applicable, with appropriate notifications to, or consents from, affected individuals.

2.14 It is noted that only 'adequately informed, voluntary and current and specific consent by a person with capacity' is acceptable for the exception in APP3.6(b) to apply. This is discussed below in paragraphs 2.17 – 2.20.

2.15 OAIC considers that where information, including personal information, is contained in a public register (such as an ASIC registry), generally individuals would reasonably expect their information to be collected from such third parties. Therefore, where information is collected from these sources, the exception in APP 3.6(b) would likely apply (provided the collection otherwise complies with APP 3).

2.16 One industry submission indicated that a person who is a director, shareholder or office-holder of a business would have an expectation that their details may be provided to, and collected by, third party suppliers of goods, equipment, financial and other services to enable the business to enter into contracts and carry on its day-to-day operations. However, even where an individual has consented to indirect collection, reporting entities should still assess the overall privacy impact on the individual when considering whether the exceptions in APP 3.6(b) apply.

2.17 While APP 3.6 includes an exception that allows a customer to consent to the collection of personal information from a source other than the individual, this only applies to government agencies, not private sector entities (such as reporting entities)[7]. Ultimately, for private sector entities, collection of personal information from other sources can only occur where collection of personal information directly from an individual is unreasonable or impracticable. Where an individual has consented to collection of their information by a third party, this may be relevant in assessing whether the individual reasonably expects their information to be collected from another source, and therefore, whether the exception in APP3.6(b) applies, that is, whether or not the individual reasonably expects that their information will be collected from another source.

2.18 The OAIC's APP Guidelines[8] contain further information about "Consent" for the purpose of the exception in APP3.6(b). In particular, paragraph B.35 of the APP Guidelines states that:

> Consent means 'express consent or implied consent' (s6(1) [of the Privacy Act]). The four key elements of consent are:

[7] See paragraph APP 3.6(a)(i)).

[8] Chapter B – Key Concepts of the APP Guidelines which are available at: https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific [to the proposed use or disclosure, and not be broad or 'bundled' consent], and
- the individual has the capacity to understand and communicate their consent.

2.19 More importantly, paragraphs B.39, B.40 and B.42 state that:

> B.39 ...An APP entity cannot infer consent simply because it provided an individual with notice of a proposed collection, use or disclosure of personal information.
>
> B.40 Use of an opt-out mechanism to infer an individual's consent will only be appropriate in limited circumstances, as the individual's intention in failing to opt-out may be ambiguous. An APP entity will be in a better position to establish the individual's implied consent the more that the following factors, where relevant, are met:
>
> - the opt out option was clearly and prominently presented
> - it is likely that the individual received and read the information about the proposed collection, use or disclosure, and the option to opt out
> - the individual was given information on the implications of not opting out
> - the opt out option was freely available and not bundled with other purposes
> - it was easy for the individual to exercise the option to opt out, for example, there was little or no financial cost or effort required by the individual
> - the consequences of failing to opt out are not serious
> - an individual who opts out at a later time will, as far as practicable, be placed in the position as if they had opted out earlier.
>
> B.42 An APP entity should as far as practicable implement procedures and systems to obtain and record consent. This may resolve any doubt about whether consent was given (either on the basis of express or implied consent).

2.20 The APP Guidelines also discusses "bundled consent":

> B.45 Bundled consent refers to the practice of an APP entity 'bundling' together multiple requests for an individual's consent to a wide range of collections, uses and disclosures of personal information, without giving the individual the opportunity to choose which collections, uses and disclosures they agree to and which they do not.

B.46 This practice has the potential to undermine the voluntary nature of the consent. If a bundled consent is contemplated, an APP entity could consider whether:

- it is practicable and reasonable to give the individual the opportunity to refuse consent to one or more proposed collections, use and/or disclosures
- the individual will be sufficiently informed about each of the proposed collections, uses and/or disclosures
- the individual will be advised of the consequences (if any) of failing to consent to one or more of the proposed collections, uses and/or disclosures…

2.21 AUSTRAC notes that the existing AML/CTF requirements in relation to customer identification and verification (which have generally been in place since 2007) will remain unchanged and are merely being supplemented by this proposed amendment. The requirements currently in place in Chapter 4 to verify information by the use of reliable and independent documentation or reliable and independent electronic data or both, effectively narrows the collection of information to reputable sources. This will continue with the proposed amendments as the sources must be reliable and independent.

2.22 It is not the intent of these amendments to increase the amount or type of personal information collected about a customer by a reporting entity as generally reporting entities are currently only required to collect a minimum amount of information about a customer. Obtaining minimum KYC information about a customer from other sources will not be a mandated requirement, but an optional procedure which reporting entities may wish to adopt in carrying out the ACIP.

2.23 Furthermore, the changes are not introducing a new requirement to collect any 'sensitive information' about individuals. However, under the current risk-based approach prescribed in Chapter 4, reporting entities may collect additional information:

- to satisfy themselves that a person is who they say they are;
- if there is an increased ML/TF risk involved and more detailed customer due diligence is required; and
- which is reasonably necessary by the reporting entity to carry out one or more of its functions or activities.

2.24 In addition, and as previously noted, the amendments relate to the section 32 requirement under the AML/CTF Act that an ACIP be carried out by reporting entities in regard to their customers. As a result, the proposed amendments are relevant to the legitimate objective under the AML/CTF Act that customer identities be verified in order to identify, mitigate and manage ML/TF risk.

2.25 A further legitimate objective is the requirement under the AML/CTF Act that AUSTRAC must consider whether an obligation imposes 'unnecessary financial and

administrative burdens on reporting entities'.[9] As previously noted, it is anticipated that substantial regulatory savings will result from the proposed amendments.

2.26 Overall, industry submissions have indicated that if the proposed amendments are finalised, reporting entities will undertake an assessment and review of their privacy policies and the privacy regulatory framework to determine whether changes are necessary, including identifying all instances where personal information would be collected from sources other than the customer in order to ensure that any privacy concerns are mitigated prior to collection from another source. For example, some changes that industry may need to make include revising prior privacy notices and consents, requiring the person from whom information is collected to notify the individual that their information will be collected, or reporting entities themselves telling the individual as soon as possible after the information has been collected.

2.27 Some industry submissions indicated that their privacy policies already provided for the collection of information about their customers from third parties such as service providers, agents, advisers, brokers, employers and family members, as well as from sources that are publicly available, for example from public registers or social media or from other third parties.

2.28 However, it is important to note that while privacy policies outline how personal information is collected (as required by APP1.4(b)), including notifications in a privacy policy, this does not necessarily make the collection of the information about an individual from third parties lawful. This is particularly so for private sector entities, which are not covered by the 'consent exception' in APP3.6(a)(i).

2.29 While notification/consent may be relevant to assessing whether the collection is "unreasonable" or "impracticable", an assessment of other factors as listed in paragraph 2.10 of this PIA should also be undertaken to determine whether the exception applies.

2.30 Furthermore, reporting entities should be mindful about "bundled consents" and actively seek the informed and specific consent from individuals about whom information is collected from other sources.

2.31 It was noted in one industry submission that many reporting entities may not have sufficient details in the privacy policies to indicate where information is being collected from. In such cases, it is expected that reporting entities would amend their policies, as appropriate, to ensure that they correctly articulate their information collection and handling procedures, including those of individuals who are not customers of reporting entities. Such information is required to be included in a privacy policy by APP1.

2.32 The following table provides an overview of each APP and summarises AUSTRAC's assessment of the privacy impacts on individuals and the information handling practices of reporting entities as a result of the proposed amendments to Chapter 4:

[9] Paragraph 212(3)(c) of the AML/CTF Act.

Privacy impacts

Australian Privacy Principle (APP)	Potential relevant exception	Privacy impact on individuals from proposed amendments	Mitigation of privacy impact
APP 1 – Open and transparent management of personal information	N/A	There will be privacy impacts on individuals if reporting entities do not: • implement adequate or updated ongoing practices, procedures and systems to ensure compliance with the APPs; • have up to date and accessible APP Privacy Policies which address how they each collect and manage personal information about individuals (including non-customers, if applicable). A failure to have a lawful and current APP privacy policy and ongoing/adequate policies and procedures in relation to the collection and management of personal information for sources other than a customer could have a privacy impact on the following: • Existing individual customers of reporting entities (from whom personal information has historically been collected, but now may be collected from other sources); • Individuals who are not customers of reporting entities, but are associated with a customer (whether another individual or a non-individual entity) of a reporting entity. The privacy impact will occur when personal information about these individuals is not collected directly from that individual, but from other sources.	All reporting entities are subject to the requirements of the *Privacy Act 1988* and APPs by virtue of subsection 6E(1A). Reporting entities may have to implement revised practices, procedures and systems, including a revised APP privacy policy and new processes for collecting and managing personal information about customers and non-customers, as a result of these amendments.

Australian Privacy Principle (APP)	Potential relevant exception	Privacy impact on individuals from proposed amendments	Mitigation of privacy impact
APP 2 – Anonymity and pseudonymity	APP 2.2(a)	Individuals who are not customers of a reporting entity, but about whom personal information is collected (for example, individuals associated with a non-individual customer), will not necessarily have the option of being able to deal with the reporting entity anonymously or using a pseudonym, because of the exception in APP 2.2(a). Reporting entities are required under the AML/CTF regime to identify and verify customers prior to providing designated services (refer to sections 139 and 140 of the AML/CTF Act). The amendments will be subject to these requirements.	N/A, due to the exception in APP2.2(a).
APP 3 – Collection of solicited personal information	APP 3.6(b)	There could be a privacy impact on individuals if a reporting entity collects personal information which is not reasonably necessary for, or directly related to, one or more of the reporting entity's functions or activities. For non-agency APP entities, APP 3.6(b) provides that personal information must be collected from the individual unless it is unreasonable or impracticable to do so. Where it is unreasonable or impracticable to collect personal information directly from an individual, and the reporting entity collects this information from other sources, there could be a privacy impact on the following individuals, as they may have less control over the use of their personal information: • Existing individual customers of reporting entities (from whom personal information has historically been collected, but	Reporting entities may have to implement revised practices, procedures and systems as a result of these amendments to ensure that: • only personal information which is ***reasonably necessary*** for one or more of the reporting entity's functions or activities is collected; and • personal information is collected from third parties only when it is unreasonable or impracticable to collect it directly from an individual. Reporting entities should consider the factors listed in paragraph 3.65 of the OAIC's APP Guidelines (reproduced in paragraph 2.10 of this PIAand any other

Australian Privacy Principle (APP)	Potential relevant exception	Privacy impact on individuals from proposed amendments	Mitigation of privacy impact
		now may be collected from other sources); • Individuals who are not customers of reporting entities, but are associated with a customer (whether another individual or a non-individual entity) of a reporting entity. The privacy impact will occur when personal information about these individuals is not collected directly from, or with the consent of, that individual, but from other sources. Under the ACIP requirements, reporting entities are required to collect and verify certain personal information about beneficial owners of non-individual customers and politically-exposed persons. Reporting entities may not necessarily collect personal information about such individuals directly from them, or with their consent.	relevant factors) when making this assessment. Any consent provided by an individual to a reporting entity to collect their personal information from other sources will also be relevant to assessing whether the collection is "unreasonable" or "impracticable". However, any consent provided by an individual to their information being collected from another source should be fully-informed and specific (see paragraphs 2.17 – 2.20 above for further details). It should be noted that the ACIP requirements do not include any minimum requirement to collect 'sensitive information', especially in regard to politically-exposed persons, although some information may be collected in certain circumstances. The 'Note' as currently published to Part 4.13 (Collection and Verification of Politically Exposed Person information) of Chapter 4, alerts reporting entities to this possibility: 'Reporting entities should consider the requirements in the *Privacy Act 1988* relating to the collection and handling of sensitive information about politically exposed persons.' The ACIP requirements require reporting entities to verify some information collected about customers and, where applicable, beneficial owners from reliable and independent sources. It can

Australian Privacy Principle (APP)	Potential relevant exception	Privacy impact on individuals from proposed amendments	Mitigation of privacy impact
			be difficult to meet this requirement if the reporting entity is not able to collect information from third party sources. Where personal information is contained in a public register (such as an ASIC registry), generally individuals would reasonably expect their information to be collected from such third parties. The exception in APP3.6(b) would likely apply providing the collection otherwise complies with APP3.
APP 4 – Dealing with unsolicited personal information	N/A	This APP is not relevant to the proposed amendments, as they do not relate to the collection of unsolicited personal information. The amendments to Chapter 4 relate to personal information directly sourced by the reporting entity about the customer from sources other than the customer.	N/A
APP 5 – Notification of the collection of personal information	N/A	APP5 requires reporting entities to provide notification of the collection of personal information before, or at the time, it collects that information from an individual. If this is not practicable, notification should be provided to the individual as soon as practicable after collection. Individuals who are not customers of reporting entities may have personal information collected about them without prior notification from reporting entities or having consented to such collection, for example, officers of a company. Alternatively, such individuals may be provided with notification of collection of personal information after the collection has already occurred.	Reporting entities should have current and accurate privacy policies, notices or other notifications to customers outlining how their personal information is collected, including the collection of such information from sources other than a customer. While notification/consent may be relevant to the assessing whether the collection is “unreasonable” or “impracticable”, an assessment of other factors listed in paragraph 2.10 of this PIA should also be undertaken to determine whether the exception applies. Furthermore, reporting entities should be mindful about “bundled consents” and actively seek the informed and specific consent

Australian Privacy Principle (APP)	Potential relevant exception	Privacy impact on individuals from proposed amendments	Mitigation of privacy impact
			from individuals about whom information is collected from other sources (see paragraphs 2.17 – 2.20 above for further details). Reporting entities may have to implement revised practices, procedures and systems as a result of these amendments, particularly in relation to the collection of personal information about non-customer-individuals who are associated with customers of the reporting entity (whether these customers are individuals or non-individual entities) to satisfy ACIP requirements. It is expected that the amendments will not cause significant change to existing industry practices. Reporting entities should already be making their customers aware that personal information may be collected about them and verified before they receive designated services. The main issue will be for reporting entities to deal with, and handle personal information about, non-customers of reporting entities – particularly those in relation to non-individual customers – in accordance with APP5 requirements. Where personal information is contained in a public register (such as an ASIC registry), generally individuals would reasonably expect their information to be collected from such third parties. The exception in APP3.6(b) would likely apply provided the collection otherwise complies with APP3.

Australian Privacy Principle (APP)	Potential relevant exception	Privacy impact on individuals from proposed amendments	Mitigation of privacy impact
APP 6 – Use or disclosure of personal information	APP 6.1(a), APP 6.2(b), APP 6.2(c)	APP6 requires reporting entities to only use or disclose personal information for the particular purpose for which it was collected ("primary purpose"), or for a secondary purpose if an exception applies (such as where the individual has consented). The main privacy impact will be where personal information about an individual is collected by a reporting entity for one primary purpose but is used or disclosed for a secondary purpose, unless prior consent has been obtained from the individual, or another exception applies. There could be a privacy impact on: • Existing individual customers of reporting entities (from whom personal information has historically been collected, but now may be collected from other sources); • Individuals who are not customers of reporting entities, but are associated with a customer (whether another individual or a non-individual entity) of a reporting entity. The privacy impact will occur when personal information about these individuals is not collected directly from, or with the consent of, that individual, but from other sources.	Reporting entities should have current and accurate privacy policies, notices or other notifications to customers outlining how their personal information (including information collected from other sources) will be used or disclosed. It is expected that the amendments will not cause significant change to existing industry practices. Reporting entities will either seek prior customer consent to such use or disclosure, or inform customers of required or possible lawful disclosures or use of personal information they collect from other sources about the customer. The main issue will be for reporting entities to deal with, and handle personal information about individuals who are not customers of reporting entities – particularly those individuals associated with non-individual customers of a reporting entity. Reporting entities may have to implement revised practices, procedures and systems as a result of these amendments, particularly in relation to how it will use or disclose personal information collected about individuals who are associated with customers of the reporting entity (whether these customers are individuals or non-individual entities).
APP 7 – Direct marketing	APP 7.3	APP7 prohibits reporting entities from using personal information for direct marketing, except where the individual would reasonably expect the information to be used for the purpose of direct marketing; and	It is expected that the amendments will result in changes to existing industry practices in relation to the collection of personal information about customers of reporting

Australian Privacy Principle (APP)	Potential relevant exception	Privacy impact on individuals from proposed amendments	Mitigation of privacy impact
		where the reporting entity includes a simple means to opt out of the direct marketing communications. Additional restrictions apply if the personal information was collected from a third party, in which case consent is required unless it is impracticable to obtain that consent. Where a reporting entity engages in direct marketing and decides to collect personal information about individuals from other sources, there could be future privacy impacts on: • Existing individual customers of reporting entities (from whom personal information has historically been collected, but now may be collected from other sources); • Individuals who are not customers of reporting entities, but are associated with a customer (whether another individual or a non-individual entity) of a reporting entity. The privacy impact will occur when personal information about these individuals is not collected directly from, or with the consent of, that individual, but from other sources.	entities for reporting entities who engage, or intend to engage in direct marketing using information collected from third parties. In these circumstances reporting entities are required to: • seek prior customer consent to allow for the use or disclosure of personal information for direct marketing; and • inform customers of 'opt out' procedures whereby customers may request not to receive direct marketing communications or request the reporting entity's source of an individual's personal information. Accordingly, reporting entities may have to implement revised practices, procedures and systems as a result of these amendments. This is relevant to personal information collected about non-customer individuals who are associated with customers of the reporting entity (whether the customers are individuals or non-individual entities) when reporting entities engage in direct marketing activities.
APP 8 – Cross-border disclosure of personal information	APP 8.2(b), APP 8.2(c), APP 8.2(d), APP 8.2(e)	APP 8 requires reporting entities to take reasonable steps to ensure the protection of personal information when it is disclosed overseas, unless a relevant exception applies. Where a reporting entity collects personal information about an individual customer (or an individual associated with a non-individual	It is expected that the amendments will not cause significant change to existing industry practices relating to the handling of personal information collected from or about customers of reporting entities. It is expected that reporting entities will:

Australian Privacy Principle (APP)	Potential relevant exception	Privacy impact on individuals from proposed amendments	Mitigation of privacy impact
		customer) from other sources and this personal information is disclosed to an overseas recipient, there could be a privacy impact on: • the existing individual customer of the reporting entity (from whom personal information has historically been collected, but now may be collected from other sources); • individuals who are not customers of reporting entities, but are associated with a customer (whether another individual or a non-individual entity) of a reporting entity. The privacy impact will occur when personal information about these individuals is not collected directly from, or with the consent of, that individual, but from other sources. The privacy impact could occur where a reporting entity discloses this personal information to overseas or global organisations and third parties, for example, as part of the ACIP verification process.	• seek prior customer fully-informed and specific consent (see paragraphs 2.17 – 2.20 above for further details) to allow for the cross-border disclosure of personal information in line with the requirements of APP 8.2(b), where required; and/or • inform customers that personal information may need to be disclosed for certain domestic and international lawful purposes, for example, the disclosure is required or authorised by or under an Australian law or a court/tribunal order. Reporting entities may have to implement revised practices, procedures and systems as a result of these amendments, particularly in relation to how personal information collected about non-customer-individuals who are associated with customers of the reporting entity (whether these customers are individuals or non-individual entities) is disclosed overseas. This may include reviewing existing or implementing new enforceable contractual arrangements with overseas recipients of personal information. Such contractual arrangements must require, amongst other matters, the recipient to handle the personal information in accordance with the APPs.

Australian Privacy Principle (APP)	Potential relevant exception	Privacy impact on individuals from proposed amendments	Mitigation of privacy impact
APP 9 – Adoption, use or disclosure of government related identifiers	N/A	APP9 prohibits reporting entities from using and disclosing government-related identifiers, except in certain circumstances such as: • the identifier is reasonably necessary to verify an individual's identity for the purposes of the reporting entity's activities or functions; • the identifier is reasonably necessary for the reporting entity to fulfil its obligations to an agency or a State/Territory authority; • the identifier is required or authorised by or under an Australian law or court/tribunal order; • the identifier is reasonably necessary for one or more enforcement related activities conduct by or on behalf of an enforcement body. Where a reporting entity collects personal information about an individual customer (or an individual associated with a non-individual customer) which constitutes a government related identifier from other sources, there could be a privacy impact on: • the existing individual customer of the reporting entity (from whom personal information has historically been collected, but now may be collected from other sources); • individuals who are not customers of reporting entities, but are associated	It is expected that the amendments will not cause significant change to existing industry practices in relation to the types of personal information about a customer a reporting entity collects, then adopts, uses or discloses. Reporting entities may have to implement revised practices, procedures and systems as a result of these amendments, particularly in relation to the personal information collected about non-customer-individuals who are associated with customers of the reporting entity (whether these customers are individuals or non-individual entities).

Australian Privacy Principle (APP)	Potential relevant exception	Privacy impact on individuals from proposed amendments	Mitigation of privacy impact
		with a customer (whether another individual or a non-individual entity) of a reporting entity. The privacy impact will occur when personal information about these individuals is not collected directly from, or with the consent of, that individual, but from other sources.	
APP 10 – Quality of personal information	N/A	APP10 requires a reporting entity to take reasonable steps to ensure the personal information it collects, uses and discloses is accurate, up to date and complete. Where a reporting entity collects personal information about an individual customer (or an individual associated with a non-individual customer) from other sources, there could be a privacy impact on: • the existing individual customer of the reporting entity (from whom personal information has historically been collected, but now may be collected from other sources); • individuals who are not customers of reporting entities, but are associated with a customer (whether another individual or a non-individual entity) of a reporting entity. The privacy impact will occur when personal information about these individuals is not collected directly from, or with the consent of, that individual, but from other sources; where that personal information has not been reviewed for accuracy, currency and completeness by the	It is expected that the amendments will not cause significant change to existing industry practices. Under the AML/CTF requirements, a reporting entity needs to be satisfied about the customer's identity (and, if applicable, any beneficial owners and politically exposed persons). This includes the need to verify personal information collected using 'reliable and independent documentation', 'reliable and independent electronic data', or both. Furthermore, there are additional requirements under Chapter 15 of the AML/CTF Rules for reporting entities to review and update customer information in order to ensure that it is accurate, up to date and complete. This will apply in relation to personal information collected about a customer from sources other than the customer. Reporting entities may have to implement revised practices, procedures and systems as a result of these amendments, particularly in relation to the personal information collected about non-customer-individuals who are associated with

Australian Privacy Principle (APP)	Potential relevant exception	Privacy impact on individuals from proposed amendments	Mitigation of privacy impact
		reporting entity prior to its subsequent use or disclosure.	customers of the reporting entity (whether these customers are individuals or non-individual entities).
APP 11 – Security of personal information	N/A	APP11 requires a reporting entity to take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. A reporting entity has obligations to destroy or de-identify personal information in certain circumstances (for example, if it no longer needs that information, or if it is not legally required to retain the information). Where a reporting entity collects personal information about an individual customer (or an individual associated with a non-individual customer) from other sources, there could be a privacy impact on: • the existing individual customer of the reporting entity from whom personal information has historically been collected, but now may be collected from other sources; • individuals who are not customers of reporting entities, but are associated with a customer (whether another individual or a non-individual entity) of a reporting entity. The privacy impact will occur when personal information about these individuals is not collected directly from, or with the consent of, that individual, but from other sources;	It is expected that the amendments will not cause significant change to existing industry practices in relation to personal information collected about customers of reporting entities. Reporting entities may have to implement revised practices, procedures and systems as a result of these amendments, particularly in relation to the personal information collected about non-customer-individuals who are associated with customers of the reporting entity (whether these customers are individuals or non-individual entities).

Australian Privacy Principle (APP)	Potential relevant exception	Privacy impact on individuals from proposed amendments	Mitigation of privacy impact
		• where such personal information is used or disclosed without adequate restrictions and security being implemented in relation to its use or disclosure. • where a reporting entity chooses to retain the information about an individual who is associated with a customer of the reporting entity, once the customer ceases its relationship with the reporting entity. This will be subject to the record-keeping requirements under Part 10 (Record-keeping requirements) of the AML/CTF Act.	
APP 12 – Access to personal information	N/A	APP12 generally requires that a reporting entity must, upon request, give an individual access to any personal information that the reporting entity holds about them. For reporting entities, relevant exceptions are prescribed in paragraph APP12.3. Where a reporting entity collects personal information about an individual customer (or an individual associated with a non-individual customer) from other sources, there could be a privacy impact on: • the existing individual customer of the reporting entity (from whom personal information has historically been collected, but now may be collected from other sources);	It is expected that the amendments will not cause significant change to existing industry practices in relation to personal information collected about customers of reporting entities. Reporting entities may have to implement revised practices, procedures and systems as a result of these amendments, particularly in relation to the personal information collected about non-customer-individuals who are associated with customers of the reporting entity (whether these customers are individuals or non-individual entities). This may include a reporting entity:

Australian Privacy Principle (APP)	Potential relevant exception	Privacy impact on individuals from proposed amendments	Mitigation of privacy impact
		• individuals who are not customers of reporting entities, but are associated with a customer (whether another individual or a non-individual entity) of a reporting entity. The privacy impact will occur when personal information about these individuals is not collected directly from, or with the consent of, that individual, but from other sources; especially where such individuals have not been informed that personal information about them has been collected by the reporting entity. In these cases, such individuals may not be aware of their ability to access the personal information that a reporting entity holds about them.	• updating its "information-accessibility processes" so that it complies with APP 12; and/or • denying or refusing access to the information if any of the exceptions in APP 12.3 apply.
APP 13 – Correction of personal information	N/A	APP13 requires a reporting entity to take reasonable steps to correct any personal information it holds if it is satisfied that the information is out of date, inaccurate, incomplete, irrelevant or misleading, or an individual requests the correction of the information. Where a reporting entity collects personal information about an individual customer (or an individual associated with a non-individual customer) from other sources, there could be a privacy impact on: • the existing individual customer of the reporting entity (from whom personal information has historically been collected, but now may be collected from other sources);	It is expected that the amendments will not cause significant change to existing industry practices in relation to personal information collected about customers of reporting entities. Reporting entities may have to implement revised practices, procedures and systems as a result of these amendments, particularly in relation to the personal information collected about non-customer-individuals who are associated with customers of the reporting entity (whether these customers are individuals or non-individual entities).

Australian Privacy Principle (APP)	Potential relevant exception	Privacy impact on individuals from proposed amendments	Mitigation of privacy impact
		• individuals who are not customers of reporting entities, but are associated with a customer (whether another individual or a non-individual entity) of a reporting entity. The privacy impact will occur when personal information about these individuals is not collected directly from, or with the consent of, that individual, but from other sources.	

3. Conclusion and recommendations

3.1 AUSTRAC notes that the proposed amendments to Chapter 4 do not:

- impose a new mandatory requirement on reporting entities to use a particular source when collecting KYC information about a customer (including those individuals who are not customers). Reporting entities will still have the option of collecting personal KYC information about individuals directly from a customer;
- expand the type of personal information a reporting entity must collect when carrying out an ACIP; or
- significantly amend the existing AML/CTF regime for customer identification and verification.

3.2 On the basis of industry submissions, AUSTRAC anticipates that "information collected from other sources" will generally be managed under the existing privacy practices, procedures and systems of reporting entities, subject to reporting entities making any necessary adjustments, especially in relation to the collection of personal information about individuals (who are not customers of a reporting entity) who may be associated with a non-individual customer.

3.3 AUSTRAC also considers that the activity allowed by the amendments may be covered by the exceptions in APP 3.6(b). The first exception allows organisations to collect information from third parties where it would be unreasonable or impracticable to collect the information from the individual, in particular those circumstances where the individual would reasonably expect personal information about them to be collected directly from them or from another source. The second exception relates to the legislative requirement that reporting entities have an obligation to identify customers under the AML/CTF Act and AML/CTF Rules.

3.4 Accordingly, while the proposed amendments will have privacy impacts, AUSTRAC considers that these impacts can be managed appropriately by:

(a) Reporting entities implementing any necessary adjustments to their privacy practices, procedures or systems to ensure continued compliance with the APPs. This is important in relation to non-individual customers who have associated individuals who may not normally be notified about collection of their personal information by the reporting entity, nor have the opportunity to consent to such collection;

(b) the inclusion of the following note in Chapter 4 which highlights the relevant privacy obligations:

> ***Note**: Reporting entities that collect information about a customer from a third party will need to consider their obligation under subclause 3.6 of the Australian Privacy Principles, which requires that personal information about an individual must be collected only from the individual unless it is unreasonable or impractical to do so and where it is reasonably necessary for the reporting entity's functions or activities;*

(c) AUSTRAC issuing guidance to industry which discusses the amendments to Chapter 4, explains the interaction with APP3 (and other APPs generally) and highlights the importance of complying with APP 3.6 when collecting information from sources other than the individual concerned;

(d) noting the above recommendations in the 'Statement of Compatibility with Human Rights' as required by Part 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*, when the proposed amendments are finalised.