EXPLANATORY STATEMENT

Issued by authority of the Acting AUSTRAC CEO

Anti-Money Laundering and Counter-Terrorism Financing Act 2006

Anti-Money Laundering and Counter-Terrorism Financing Rules 2025

Anti-Money Laundering and Counter-Terrorism Financing Rules Amendment (Consequential Amendments) Instrument 2025

AUTHORITY

Section 229 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (**the Act**) provides that the AUSTRAC CEO may, by legislative instrument, make Anti-Money Laundering and Counter-Terrorism Financing Rules (**AML/CTF Rules**). The AML/CTF Rules are set out in the *Anti-Money Laundering and Counter-Terrorism Financing Rules 2025* (**the Rules**) and the *Anti-Money Laundering and Counter-Terrorism Financing (Class Exemptions and Other Matters) Rules 2007* (the **Class Exemption Rules**).

Under subsection 33(3) of the *Acts Interpretation Act 1901*, where an Act confers a power to make, grant or issue any instrument of a legislative or administrative character (including rules, regulations or by-laws), the power shall be construed as including a power exercisable in the like manner and subject to the like conditions (if any) to repeal, rescind, revoke, amend, or vary any such instrument

The Rules also rely on section 4 of the *Acts Interpretation Act 1901*, as they are made in contemplation of commencement of amendments to the Act made by the *Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2024*. The Rules commence at the same time as Schedules 1, 2, 3, item 1 and Part 1 Division 2 of Schedule 5, Schedule 6, Schedule 8 and Schedule 10 of that Act.

PURPOSE AND OPERATION OF THE INSTRUMENT

The *Anti-Money Laundering and Counter-Terrorism Financing Rules 2025* and *Anti-Money Laundering and Counter-Terrorism Financing Rules Amendment (Consequential Amendments) Instrument 2025* (the **Rules Instruments**) are legislative instruments for the purposes of the *Legislation Act 2003*.

Details of the Instruments are set out in Attachment A and Attachment B.

A Statement of Compatibility with Human Rights (the **Statement**) is at Attachment C. The Statement was completed in accordance with the *Human Rights (Parliamentary Scrutiny) Act 2011.* The Instruments are compatible with human rights, and to the extent that they may limit human rights, those limitations are reasonable, necessary and proportionate.

Legislative background

Overview of the AML/CTF Regime

1. Australia's anti-money laundering and counter-terrorism financing terrorism regime (**AML/CTF regime**) comprises of the AML/CTF Act, the AML/CTF Rules and any Anti-Money Laundering and Counter-Terrorism Financing Regulations made under the AML/CTF Act. The AML/CTF regime establishes a regulatory framework for combatting money laundering, the financing of terrorism, and other serious financial crimes. At its core, the AML/CTF regime is a partnership between the Australian Government and industry. Through the regulatory framework, reporting entities play a vital role in effectively detecting and preventing the misuse of their sector for money laundering, terrorism or the proliferation of weapons of mass destruction.

Reforms to the AML/CTF Act

2. In November 2024, the Australian Parliament passed the *Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2024* which amended the AML/CTF Act. The amendments extended the AML/CTF regime to certain higher-risk services provided by real estate professionals, professional service providers including lawyers, accountants and trust and company service providers, and dealers in precious stones and metals—also known as 'tranche two' entities. The amendments to the AML/CTF Act shift the AML/CTF regime to an outcomes-based framework to make it simpler and clearer for businesses to be able to comply with their obligations, and modernise the regime to reflect changing business structures, technologies and illicit financing methodologies.

Reforms to the AML/CTF Rules

3. To operationalise, and supplement, the amended AML/CTF Act, a new AML/CTF Rules framework has been developed, and created, by the AUSTRAC CEO. The new AML/CTF Rules framework includes:

    (a) the making of the *Anti-Money Laundering and Counter-Terrorism Financing Rules 2025*, which replaces many of the provisions in the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007* and operationalises the amended AML/CTF Act; and

    (b) the *Anti-Money Laundering and Counter-Terrorism Financing Rules (Class Exemption and Other Matters)* 2007 (the Class Exemption Rules) formerly titled the, *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007*– which has historically supplemented the AML/CTF Act—has been amended and renamed. The only chapters preserved are Chapters 1, 21, 22, 31, 39, 42, 43, 45, 47, 48, 49, and 67.

4. The AML/CTF Rules 2025 is set out in in a topically-structured format that reflects the order of engagement a reporting entity will have with the AML/CTF regime. It supports the amended AML/CTF Act by:

- providing reporting entities with finer detail on fundamental AML/CTF obligations set out in the AML/CTF Act, for example, reporting groups, AML/CTF programs and customer due diligence obligations.

- specifying information required to meet specific obligations—particularly for enrolment, registration, suspicious matter reporting, threshold transaction reporting, keep open notices, and the transfer of value.

- re-writing in simpler terms, existing measures that have not substantively changed such as correspondent banking relationships and AML/CTF compliance reporting requirements.

5. The reforms to the AML/CTF regime ensure that Australia's AML/CTF regime continues to effectively deter, detect and disrupt illicit financing, and protect Australian businesses from criminal exploitation. Moreover, the reforms ensure that Australia's AML/CTF regime meets international standards set by the FATF. The FATF Standards (comprising the FATF Recommendations and their Interpretive Notes and Glossary accessible at https://www.fatf-gafi.org/en/topics/fatf-recommendations.html) are a comprehensive framework of measures to combat money laundering, the financing of terrorism, and proliferation financing. These standards set an international benchmark for countries to implement and adapt to their legal, administrative and operational frameworks and financial systems.

6. The FATF promotes compliance and effective implementation of the standards through peer assessment mechanisms—known as mutual evaluations—and public listing of jurisdictions found to have weak AML/CTF systems. In 2015, the FATF identified deficiencies in Australia's compliance with the FATF Standards and highlighted areas for improvement. Since then, the FATF Standards have continued to be strengthened, particularly in relation to the regulation of virtual assets.

CONSULTATION

7. Paragraph 212(2)(a) of the Act sets out whom the AUSTRAC CEO must consult with in performing the AUSTRAC CEO's functions. AUSTRAC has worked closely with industry and the statutory office holders listed in Paragraph 212(2)(a) in developing the Rules, meeting at senior executive and officer levels with the office holders, industry representatives, reporting entities, undertaking two rounds of public consultation on two separate exposure drafts of the Rules and facilitating various working groups.

8. AUSTRAC established 9 sector based Rules & Guidance Working Groups. The purpose of the working groups was to work with industry on the development of the Rules through focusing on sector specific issues. The sectors represented were the:
    - Legal sector
    - Conveyancing sector
    - Dealers in precious metals and stones sector

- Financing services sector
- Gambling sector
- Accounting sector
- Virtual asset sector
- Remittance sector
- Real estate sector.

9. The initial round of public consultation on the First Exposure Draft AML/CTF Rules (ED1 Rules) took place between 11 December 2024 and 14 February 2025. One hundred and three long-form submissions were received by AUSTRAC.

10. AUSTRAC considered all written submissions and feedback received during the first round of consultation and, in response, developed and released the Second Exposure Draft AML/CTF Rules (ED2 Rules) together with a table of feedback from the submissions made on the ED1 Rules which included AUSTRAC's responses to the principal issues raised.

11. The second round of public consultation on the ED2 Rules took place from 19 May 2025 to 27 June 2025. One hundred and twenty six submissions were received by AUSTRAC. The feedback from the second round of public consultation resulted in further amendments which are incorporated in the Rules. Similar to its response to issues raised on the ED1 Rules, AUSTRAC has developed a table of feedback, setting out common topics of feedback from the submissions made on the ED2 Rules. Within the feedback table, AUSTRAC has responded to industry queries and feedback. This table of feedback will be made publicly available shortly after publication of the Rules. AUSTRAC's responses will include:
    - clarification on the policy intent or operational scope of the Rules
    - examples of how the section is intended to operate in practice
    - an explanation of any amendments to the relevant sections which addressed a query raised in the submissions.

12. AUSTRAC facilitated three working groups for each sector—one in November, the second in January/ February 2025, and the third in July 2025, twenty six in total—all of which covered AML/CTF Rules development. In addition there were 8 Industry Forums and 5 workshops held through the consultation on the AML/CTF Rules.

13. The working groups allowed AUSTRAC to explain the ED1 Rules and ED2 Rules to each sector, and answer questions from each sector on sector-specific issues that pertained to the proposed AML/CTF Rules. Feedback received from industry on the working groups was positive, and members communicated that participating in the working groups assisted with their submissions on both the ED1 and ED2 Rules.

SUNSETTING

14. Under item 6 of regulation 12 of the *Legislation (Exemptions and Other Matters) Regulation 2015* the Instruments are not subject to sunsetting.

15. The AML/CTF Rules are designed to be enduring because they:
    - complement and provide the detail required for the broader obligations set out in the AML/CTF Act, aid in meeting Australia's international obligations and matters of international concern, and support the combatting of money laundering and terrorism financing
    - assist industry in fulfilling their compliance with the AML/CTF Act, and provide commercial and regulatory certainty for industry, and
    - are subject to an ongoing process of development, refinement and review, involving scrutiny and feedback from a wide range of stakeholders including industry, the Financial Action Task Force, Australian Government agencies, law enforcement agencies, and other interested parties.

16. The exemptions remaining in the Class Exemption Rules are time-limited and automatically repeal on 31 March 2031.

IMPACT ANALYSIS

17. The Office of Impact Analysis (OIA) has been consulted in relation to the Rules Instruments and an Impact Analysis **is not required** as they do not create any additional impact other than what has already been assessed in the Impact Analysis for the Anti-Money Laundering and Counter-Terrorism Financing Regime (AML-CTF) Reforms (OIA reference number: OBPR22036-47) completed in September 2024. The Executive Summary of that Impact Analysis is set out below.

18. Each year billions of dollars of illicit funds are generated from illegal and harmful activities such as drug trafficking, tax evasion, human trafficking, cybercrime and scams, arms trafficking and other illegal and corrupt practices. Illicit financing is also used to fund activities that harm Australia's national security and efforts to maintain an international rules-based order. The Australian Institute of Criminology (AIC) estimated serious and organised crime to cost the Australian community $60.1 billion in 2020-21. The true total cost of crime is likely much greater, given the illicit nature of the activities and the second order effects on the community and economy. While money laundering is a criminal activity in its own right, illicit financing is a key enabler of these serious crimes with profit being the primary motivation. Criminals must launder their proceeds of crime to enjoy the proceeds of their illegal activities or to reinvest illicit funds in further criminal activity without detection. The amount of money laundered in Australia has been indicatively estimated at up to 2.3 per cent of GDP.

19. Australia's anti-money laundering and counter-terrorism financing (AML/CTF) regime establishes a regulatory framework for combatting money laundering, terrorism financing and other serious financial crimes. At its core, the AML/CTF regime is a

partnership between the Australian Government and industry. Through the regulatory framework established by the AML/CTF regime, businesses play a vital role in effectively detecting and preventing misuse of their sectors and products by criminals seeking to launder money and fund terrorism.

20. There are a number of inefficiencies throughout Australia's AML/CTF regime that limit the effectiveness of Australia's response to transnational crime at large. Industry and government stakeholders have consistently called for reforms to key obligations of the AML/CTF regime due to unnecessary complexity.

21. Currently, businesses internationally recognised as providing high-risk services (including lawyers, accountants, trust and company service providers, real estate agents, and dealers in precious metals and stones) are not regulated as part of the AML/CTF regime. These sectors are known internationally as Designated Non-Financial Businesses and Professions (DNFBPs) or tranche two in the Australian context. Gaps in the regulated population leave legitimate businesses vulnerable to exploitation by opportunistic criminals seeking to obfuscate the origins of their illicit wealth from law enforcement.

22. These problems impact the quality and breadth of financial intelligence generated to support national security and law enforcement operations, inflate regulatory burden for currently regulated entities and do not adequately harden businesses most at risk of criminal exploitation.

23. Without reform to address these problems, the AML/CTF regime will become increasingly less effective and more wasteful over time. The costs of inaction are significant, and would likely increase over time with Australia falling further behind continually strengthened international standards set by the Financial Action Taskforce (FATF), heightening the risk of substantial reputational and economic damage and increasing criminal threats to Australia's financial systems and professional services. Without hardening Australia's AML/CTF regime in line with the FATF standards, criminals would continue to exploit legitimate Australian businesses left exposed. Further, currently regulated entities will continue to be subject to an overly complex regime that inflates regulatory costs, ultimately diminishing the extent to which they are able to holistically comply with the AML/CTF regime.

24. To address these challenges, the proposed reforms have three objectives:
    - combatting crime
    - improving FATF compliance
    - minimising regulatory burden.

25. In line with the requirements set out in the Australian Government Guide to Policy Impact Analysis, administered by the Office of Impact Analysis (OIA), the Attorney-General's Department (the department) has conducted an impact analysis to assess and accompany proposed reforms to Australia's AML/CTF regime.

26. The department (with support from Nous Group) has provided a best effort at conducting a robust net benefit analysis. In accordance with OIA guidance, a multi-criteria analysis (MCA) was used as the preferred analytical tool to assess the available information and quantifiable data along with the unquantifiable but equally tangible benefits of the proposed reforms.

27. The department has identified and analysed four viable policy options to respond to the problems identified, including:
    - Option 1: Maintain the status quo
    - Option 2: Simplify, clarify and modernise existing legislation
    - Option 3: Expand the reporting population to DNFPBs
    - Option 4: Both simplify, clarify and modernise legislation, and expand the reporting population to DNFBPs

28. Under the analysis, Option 1 does not address the key challenges facing the regime or achieve the reform objectives. Option 2 provides some benefit to crime prevention outcomes and producing higher quality financial intelligence from assisting existing regulated entities to better comply with the regime. However, it does not reduce the risk of 'grey-listing' by the FATF as it does not address the regulation of tranche two sectors. Option 3 does address this issue, as well as supporting crime prevention outcomes and increasing the amount of financial intelligence by covering a larger proportion of the economic activity at risk of exploitation. The quantifiable benefits of this are estimated to be up to $13.1 billion over ten years. However, Option 3 also comes with largest estimated regulatory impact of $15.8 billion to business, as it does not include simplifying and clarifying measures.

29. Option 4 is assessed to best meet the objectives and showed the highest net benefit through the MCA, by providing the same quantifiable benefits as Option 3 while imposing a lower regulatory burden. Implementing Option 4 is expected to deliver the significant law enforcement benefits and reduction in community harm from the expansion of the regime to tranche two entities, with the additional benefit of improved compliance across regulated entities and tranche two entities due to the reforms to simplify the regime. This is estimated to provide benefits of up to $2.4 billion over ten years. Option 4 will also be most effective in minimising the likelihood of grey-listing and any associated economic and reputational damage, which may be up to $10.7 billion over 10 years. Implementing Option 4 is estimated to result in an additional regulatory burden to businesses of $13.9 billion over 10 years, which is lower than Option 3.

30. The department notes that there are inherent limitations to the impact analysis, including:
    - Difficulty quantifying the value of money laundering globally and in Australia and the financial and societal impacts arising from money laundering. Estimates of benefits therefore reflect the best efforts and understanding of the department

and portfolio agencies, supplemented with academic sources and international experience where possible.

- A lack of evidence in the Australian context of the likely impact these reforms will have on the amount of money laundered per year.
- The details of the reforms are not yet finalised as the AML/CTF Rules will build on the principles in the Act and provide further detail on how such obligations may be achieved. As such, the operational impact of the reforms is difficult to quantify, particularly for tranche two entities who have no experience with the AML/CTF regime. Estimates of regulatory burden therefore reflect the best efforts and understanding of the affected stakeholders.
    - The department notes there will be an additional public consultation process on the Rules to ensure the reforms are fit-for-purpose. This will provide a further opportunity to reduce regulatory burden through further refinement of the obligations and simplification of the regime.

31. The full Impact Analysis for the AML/CTF reforms is contained in the Explanatory Memorandum for the Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2024 (now an Act), which is available on the Parliament of Australia website at https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r724

ATTACHMENT A

Explanation of the provisions in the *Anti-Money Laundering and Counter Terrorism Financing Rules 2025*

ACRONYMS AND ABBREVIATIONS

AML/CTF	Anti-money laundering and counter-terrorism financing
Act	*Anti-Money Laundering and Counter-Terrorism Financing Act 2006*
APRA	Australian Prudential Regulation Authority
ASIC	Australian Securities and Investments Commission
AUSTRAC	Australian Transaction Reports and Analysis Centre
CDD	Customer due diligence
CEO	Chief Executive Officer
FATF	Financial Action Task Force
FATF recommendation	Financial Action Task Force Recommendations (2012-2025): International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation June 2025 (accessible at www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html)
FATF methodology	Methodology for assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT/CPF Systems June 2025 (accessible at www.fatf-gafi.org/en/publications/Mutualevaluations/Assessment-Methodology-2022.html)
IVTS	International value transfer services
ML NRA	2024 Money Laundering National Risk Assessment of Australia (accessible at https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/money-laundering-australia-national-risk-assessment-2024)

ML/TF	Money laundering and terrorism financing
PEP	Politically exposed person
RNP	Remittance network provider
RSP	Remittance service provider
RSR	Remittance Sector Register
SMR	Suspicious matter report given to the AUSTRAC CEO under section 41 of the AML/CTF Act
TF NRA	2024 Terrorism Financing National Risk Assessment of Australia (accessible at https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/terrorism-financing-australia-national-risk-assessment-2024)
TTR	Threshold transaction report given to the AUSTRAC CEO under section 43 of the AML/CTF Act
VASP	Virtual asset service provider

Part 1—Preliminary

1-1—Name

1. This section provides that the name of the instrument is the *Anti-Money Laundering and Counter-Terrorism Financing Rules 2025* (the Rules).

1-2—Commencement

2. This section provides that the Rules commence on 31 March 2026.

1-3—Authority

3. This section provides that the Instrument is made under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006.*

1-4—Definitions

4. Section 1-4 is an interpretative provision which contains definitions of the terms and expressions used in the Rules. A note at the beginning of the provision makes it clear that a number of expressions used in the Rules are defined in the Act and provides

non-exhaustive examples. Paragraph 13(1)(b) of the *Legislation Act 2003* operates so that expressions used in the Rules have the same meaning as in the AML/CTF Act.

5. The definition of ***ABN*** provides that the meaning of the term given by section 41 of the *A New Tax System (Australian Business Number) Act 1999* applies. Under that Act, an ABN (Australian Business Number) means the entity's ABN as shown on the Australian Business Register which is established under the same Act.

6. The definition of ***ACN*** provides that the meaning of the term given by section 9 of the *Corporations Act 2001* applies. Under that Act, an ACN (Australian Company Number) is the number given by ASIC to a company on registration.

7. The definition of ***Act*** in this instrument is *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.

8. The definition of ***ARBN*** provides that the meaning of the term given by section 9 of the *Corporations Act 2001* applies. Under that Act, ABRN (Australian Registered Body Number) is the number given by ASIC to a registrable body on registration under Part 5B.2.

9. The definition of ***ARSN*** provides that the meaning of the term given by section 9 of the *Corporations Act 2001* applies. Under that Act, ARSN (Australian Registered Scheme Number) is the number given by ASIC to a registered scheme on registration.

10. ***BECS*** means the Bulk Electronic Clearing System administered by the Australian Payments Network. BECS co-ordinates and facilitates the exchange and settlement of bulk electronic transactions between participants. The essential characteristic of BECS is that the payment instructions are exchanges electronically in bulk. In addition, BECS is intended to facilitate multilateral settlement of amounts owing to or by participants as a consequence of participating in any other Clearing System operated on a net deferred settlement basis (including but not limited to the High Value Clearing System) if that system is settled on a net deferred basis in fall back mode because settlements cannot occur in real time as a result of some contingency. BECS participants are bound to comply with the Australian Payments Network Constitution and agreed regulations and procedures (accessible at https://www.auspaynet.com.au/resources#rules-regs) to maintain status as a participant.

11. ***BPAY*** means the electronic bill payment system known as BPAY. BPAY is a widely used electronic bill payment system that enables individuals and businesses to pay billers through their internet banking, it also allows merchants to offer an alternative payment method to customers by becoming a BPAY Biller through their financial institution. As a BPAY Biller, they provide BPAY payment details on bills issues to customers. Payments are then made by the customer through the payer's financial institution via phone or internet banking. The payer institution debits the account, collates information and transmits to BPAY. Payments are then batched and sent to

financial institutions. The biller's institution then sends the information and payment to the biller. BPAY also allows payments to be made in batches via APIs. To process BPAY transactions linked to an underlying bank account, financial institution participants require an authorised deposit-taking institution license and/or an Australian Financial Services Licence. The definition is restricted to the bill payment system and does not extend to Osko by BPAY.

12. The definition of ***card number*** includes a tokenised reference that allows the issuer of a credit card, debit card or stored value card to trace a payment to the payer's card. This recognises and facilitates the financial sector's increasing use of payment tokenisation as a fraud reduction measure, while still permitting payments to be traced back to the card holder and merchant if required.

13. The definition of ***corporate group*** means a group of 2 or more bodies corporate, where each member of the group is a related body corporate of each other member of the group. 'Related body corporate' is also defined in this section and is explained below.

14. The definition of ***co-operative*** provides that any body registered as a co-operative under a law of the Commonwealth, a State, a Territory or a foreign country is a co-operative. Every state and territory in Australia has adopted Co-operatives National Law (CNL) or legislation consistent with it, with registrars in each jurisdiction overseeing incorporation and registration of co-operatives.

15. ***Defence Department*** means the Department administered by the Minister responsible for administering the *Defence Act 1903*. The Administrative Arrangements Orders is a document made by the Governor-General which sets out the matters and Acts dealt with by each Department of State and its Minister(s).

16. **DEFT** (short for Direct Electronic Funds Transfer) means the electronic bill payment system known as DEFT. DEFT is owned and operated by Macquarie Bank Limited, who acts as a payment facilitator between a biller and their payer. Billers issue DEFT reference numbers which allow payers to make payments directly into the billers' bank account.

17. The definition of ***director identification number*** provides that the meaning of the term given by section 9 of the *Corporations Act 2001* applies. Under that Act, a director identification number means a director identification number given under section 1272 of that Act; or section 308—5 of the *Corporations (Aboriginal and Torres Strait Islander) Act 2006*.

18. The definition of ***domestic transfer of value*** refers to the transfer of value within Australia where the value to be transferred starts in Australia and the value will be made available in Australia. Some domestic transfers of money are subject to different value transfer obligations with respect to collecting, verifying and/or passing on information between institutions in a value transfer chain.

19. The definition of ***earnings*** provides that the term is defined in subsection 3-4(1) of the Rules.

20. The definition of ***eligible officer*** provides that the meaning of the term given by section 1272B of the *Corporations Act 2001* applies. Under that Act, an eligible officer is:

- a director of a company, or of a body corporate that is a registered Australian body, or registered foreign company, who:
    - is appointed to the position of a director; or
    - is appointed to the position of an alternate director and is acting in that capacity;

  regardless of the name that is given to that position; or
- any other officer of a company, or of a body corporate that is a registered Australian body or registered foreign company, who is an officer of a kind prescribed by the regulations;

but does not include a person covered by a determination under subsections 1272B(2) or (3).

21. ***Foreign Affairs Department*** means the Department administered by the Minister responsible for administering the *Diplomatic Privileges and Immunities Act 1967*. The Administrative Arrangements Orders is a document made by the Governor-General which sets out the matters and Acts dealt with by each Department of State and its Minister(s).

22. The definition of ***foreign company*** provides that the meaning of the term given by section 9 of the *Corporations Act 2001* applies:

"foreign company" means:

(a) a body corporate that is incorporated in an external Territory, or outside Australia and the external Territories, and is not:

(i) a corporation sole; or

(ii) an exempt public authority; or

(b) an unincorporated body that:

(i) is formed in an external Territory or outside Australia and the external Territories; and

(ii) under the law of its place of formation, may sue or be sued, or may hold property in the name of its secretary or of an officer of the body duly appointed for that purpose; and

(iii) does not have its head office or principal place of business in Australia.

23. ***Home Affairs Department*** means the Department administered by the Minister responsible for administering the *Australian Border Force Act 2015*. The

Administrative Arrangements Orders is a document made by the Governor-General which sets out the matters and Acts dealt with by each Department of State and its Minister(s).

24. The definition of ***independent evaluation report*** is given by paragraph 5-10(2)(e) of the Rules, and is a written report containing findings from an independent evaluator's:
    - evaluation of the steps taken by the reporting entity when undertaking or reviewing the reporting entity's ML/TF risk assessment, against the requirements of the Act, the regulations and the Rules;
    - evaluation of the design of the reporting entity's AML/CTF policies, against the requirements of the Act, the regulations and the Rules; and
    - testing and evaluation of the compliance of the reporting entity with the reporting entity's AML/CTF policies.

25. The definition of ***key personnel*** is relevant to reporting entities that are required to apply for registration under the Act. Key personnel comprise individuals who would be the governing body or senior manager of the reporting entity once registered, the beneficial owner of the person, and the AML/CTF compliance officer of the person.

26. The definition of ***leviable entity*** provides that the term has the same meaning as in the *Australian Transaction Reports and Analysis Centre Industry Contribution Act 2011*. Under that Act, a leviable entity, in relation to a financial year (the current year), means a person who:
    - is a reporting entity (within the meaning of section 5 of the Act) at any time in the previous financial year; and
    - on the census day for the current year:
        - is entered on the Reporting Entities Roll under Part 3A of the Act; or
        - is required, under section 51B of the Act, to apply to be entered on the Reporting Entities Roll; and
    - is not an exempt entity for the current year.

27. The definition of ***merchant payment*** covers credit card, debit card, and stored value card transfers of value from the card holder to a merchant, where the transfer is initiated or 'pulled' by the merchant's financial institution (the beneficiary institution that will make the transferred value available to the merchant). Typically this is done by the card holder presenting their card to a merchant terminal or entering their payment details on the merchant's web site or software application. The merchant acquirer conveys the request for payment to the card issuer which determines whether to accept the instruction (as the ordering institution) and authorise the payment. The term does not extend to 'push payments' in which the card issuer initiates the transfer of value as a result of a direct instruction from the card holder, unless the push payment is refund of a merchant payment.

28. The definition of passport has the same meaning as in section 5 of the Migration Act 1958. Under that Act, a passport includes a document of identity issued from official sources, whether in or outside of Australia, and having the characteristics of a passport, but does not include a document, which may be a document called or purporting to be a passport, that the Migration Regulations declare is not to be taken to be a passport. In most circumstances, passengers will be travelling into Australia on an Australian passport, within the meaning of the *Australian Passports Act 2005*; or a passport or a similar document issued for the purpose of international travel that contains a photograph and the signature of the person whose name the document is issued; and issued by a foreign government, the United Nations or an agency or an agency of the United Nations. The Rules adopt the *Migration Act 1958* definition to encompass these circumstances as well as accommodate the small number of passengers who might have other types of travel documents which are also acceptable for travel into Australia. Holders of these documents will in most cases also require a visa. The types of other acceptable travels documents that the Australian Border Force accepts is accessible at: https://www.abf.gov.au/entering-and-leaving-australia/crossing-the-border/at-the-border/travel-documents. The definition of passport is intended to capture the other acceptable travel documents as prescribed by the Australian Border Force.

29. The definition of ***payable-through accounts*** refers to paragraph 7-1(3)(g) of the AML/CTF Rules, which requires particular correspondent banking due diligence measures where a financial institution maintains an account for another financial institution, where that other financial institution's customers can directly access the account.

30. The definition of ***payer information***, sets out information about the payer in a transfer of value which is ordinarily required to be collected and verified by the ordering institution, and passed on from one institution to another in a value transfer chain, unless specified otherwise. This definition is intended to reflect the concept of 'required and accurate originator information' in FATF recommendation 16.

31. ***Registered financial sector entity*** means an entity that is a registered entity within the meaning of the *Financial Sector (Collection of Data) Act 2001.* A registered entity within the meaning of that Act is a corporation whose name is entered in the Register of Entities kept by APRA under section 8 of that Act comprising non-ADI lenders such as non-ADI lenders such as automotive financiers, mortgage securitisers and asset financing companies where certain thresholds are met.

32. ***Registrable services*** is a collective term used for the designated services that require a person to register with AUSTRAC prior to commencing to provide such services. ***Registrable services*** are:

- in relation to registration or proposed registration of a person under Part 6 of the Act as a RNP—registrable remittance network services, or

- in relation to registration or proposed registration of a person under Part 6 of the Act as an independent remittance dealer or a remittance affiliate of a RNP—registrable remittance services, or
- in relation to registration or proposed registration of a person under Part 6A of the Act as a virtual asset service provider—registrable virtual asset services.

33. The definition of ***related body corporate*** has the same meaning as in the *Corporations Act 2001*. Section 50 of the *Corporations Act 2001* specifies that a *related bodies corporate* is where a body corporate is a holding company of another body corporate; or a subsidiary of another body corporate; or a subsidiary of a holding company of another body corporate; the first-mentioned body and the other body are related to each other.

34. The definition of ***super agent*** is given by subsection 4-13(2) of the Rules, and is a person who, in the course of carrying on a business provides administrative services to a registered RNP to assist with the control or management of the remittance network operated by the provider; and as part of providing those services, represents the interests of remittance affiliates of the provider in their dealings with the provider. Assistance provided by the super agent can include compliance training, affiliate on-boarding, managing contractual arrangements, optimising the use of an RNP's proprietary remittance platform, and ensuring affiliates are implementing the RNP's AML/CTF program effectively.

35. The definition of ***tracing information*** sets out a range of information which allows a transfer of value to be traced back to the payer or the payee. It reflects the minimum information as indicated by FATF recommendation 16 that should be included with domestic transfers of value in certain circumstances.

36. The definition of ***ultimate parent*** of a remitter, virtual asset service provider or financial institution means a body corporate that controls directly, or indirectly, the remitter, virtual asset service provider or financial institution; and is not itself controlled by another body corporate. An ultimate parent is the ultimate controlling body corporate in a corporate hierarchy structure.

37. The definition of ***unique identifier*** applies to all individuals and legal forms, to cover any alphanumeric identifier given to a person to distinguish them from all others by the issuing government body or foreign country. Examples include passport numbers, drivers licence numbers or national identity card numbers, ABNs, ABRNs, and registered co-operative identifiers. Foreign equivalent identifiers are included in recognition that customers of reporting entities may not have Australian government body issued identifiers if obtaining designated services while resident, incorporated etc. in a foreign country.

38. A legal entity identifier given to the person by an organisation accredited by the Global Legal Entity Identification Foundation (accessible at

https://www.gleif.org/en), known as the Legal Entity Identifier (**LEI**) is a 20-character, alpha-numeric code based on the ISO 17442 standard developed by the International Organization for Standardization. A LEI connects to key reference information that enables clear and unique identification of legal entities participating in financial transactions and other official interactions. Each LEI contains information about an entity's ownership structure and the LEI data pool includes information to answer the question of 'who owns whom'. Specifically, legal entities that have or acquire an LEI report their 'direct accounting consolidating parent' as well as their 'ultimate accounting consolidating parent'. The child legal entity is obliged to provide the LEI, respectively, of its direct and ultimate parent to the LEI issuing organisation. The publicly available LEI data pool is a global directory, which enhances transparency in the global marketplace. In the context of the AML/CTF regime assists reporting entities applying CDD to know and verify customer relationships (beneficial owners, subsidiaries, ultimate parents and control relationships. LEIs also simplifies international regulatory supervision cooperation for AUSTRAC and its foreign equivalent regulators.

39. Similarly, connected business identifier codes issued by the Society for Worldwide Interbank Financial Telecommunication (also known as SWIFT/BIC codes) is an alpha-numeric code that is between 8 and 11 characters long. It is an international standard used to identify banks and other financial institutions in international transactions to ensure that such payments are routed correctly.

40. The term unique identifier is used throughout the Rules in relation to applications for enrolment and registration of reporting entities, TTR and SMR reportable details, and the transfer of value under Part 8 of the Rules.

41. Tax file numbers within the meaning of section 202A of the *Income Tax Assessment Act 1936*, being a number issued to a person by the Commissioner of Taxation, are not a unique identifier under the Rules due to the protections under the *Taxation Administration Act 1953* which provide offences for unauthorised requirements or requests that a person's tax file number be quoted, and the unauthorised recording, maintaining a record of, use or disclosure of an individual's TFN respectively, unless an exception applies. Similarly, the *Privacy (Tax File Number) Rule 2015* prohibits collection, use or disclosure of tax file number information unless this is permitted under taxation, personal assistance or superannuation law. As such, AUSTRAC cannot, and does not, require a reporting entity to provide AUSTRAC with a person's TFN.

42. The definition of ***unique transaction reference number*** defines this concept which is used as part of the definition of 'tracing information'. A unique transaction reference number differs from other forms of tracing information in relating specifically to a given transfer of value and not information of a more general or enduring nature such as account number, virtual asset wallet address etc.

1-5—Domestic politically exposed person

43. Section 1-5 prescribed offices and positions for the purpose of paragraph (a) of the definition of domestic PEP in section 5 of the Act. The offices and positions and officers prescribed under section 1-5 of the Rules represent offices and positions in Australia which may present significant ML/TF risks, as they have the opportunity to use their political or public position to enrich themselves through corrupt activities. In order for reporting entities to treat PEPs in a risk-based way, it is a necessary that they can correctly identify them.

44. Paragraphs (a) to (f) are straightforward as to the text of the Rules.

45. Paragraph (g) specifies an accountable authority or member of the accountable authority, of a Commonwealth entity within the meaning of the *Public Governance, Performance and Accountability Act 2013* (**PGPA Act**). Under the PGPA Act, the person or group of persons responsible for, and control over, each Commonwealth entity's operations. The person(s) or body that is the accountable authority of a Commonwealth entity is as follows:

Commonwealth entity	**Accountable authority**
Department of State	Secretary of the Department
a parliamentary department	Secretary of the Department
a listed entity	the person or group of persons prescribed by an Act or the rules to be the accountable authority of the entity
a body corporate established by a law of the Commonwealth	the governing body of the entity, unless otherwise prescribed by an Act or rules

46. Paragraph (h) specifies that a member of a governing body of a wholly-owned Commonwealth company within the meaning of the PGPA Act is a domestic PEP under (a) of the definition in the Act. A Commonwealth company is a company whose shares are not beneficially owned by any person other than the Commonwealth.

47. The Department of Finance maintains a list of Commonwealth entities and companies at https://www.finance.gov.au/government/managing-commonwealth-resources/structure-australian-government-public-sector/pgpa-act-flipchart-and-list which can assist with identifying relevant government bodies and their accountable authorities or governing bodies for the purpose of paragraphs (g) and (h) of section 1-5.

48. Paragraph (i) specifies that heads, regardless of the title of the position, of Departments of State of a State or Territory; or an agency or authority of a State or Territory that has a prominent public function are domestic PEPs under (a) of the definition in the Act.

This paragraph covers such Departments even where alternative naming conventions are used, such as in the Australian Capital Territory which names departments as 'Directorates', and where a department is styled as an 'Office' such as the Tasmanian Audit Office.

49. Paragraph (j) also covers State or Territory agencies or authorities that have a prominent public function. In line with FATF's guidance on PEPs (accessible at: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Peps-r12-r22.html), what constitutes as having a prominent public function depends on the organisation's size, organisational framework, and powers and responsibilities that may influence known national ML/TF risks (such as those identified in AUSTRAC's 2024 Money Laundering National Risk Assessment). For example, the State and Territory environmental protection authorities have a prominent public function due to their ability to significantly influence the outcomes and operations of development projects.

50. Paragraph (j) specifies heads (however described) of local government councils in a State or Territory as domestic PEPs under (a) of the definition in the Act. Local government councils are vulnerable to corruption or financial misconduct, as they generally have key responsibilities and decision making authority for land planning and zoning, building regulations and approvals, health services and licenses, waste management, emergency management, recreation and culture. They receive funds from their communities via municipal rates, charges and fees for service and fines, as well as grant funding from state and federal governments.

51. Paragraph (k) specifies the following offices of a wholly- or majority-owned State or Territory owned enterprises as domestic PEPs under (a) of the definition in the Act:
    - Chair of the board.
    - Chief executive officer.
    - Chief financial officer.

52. Corruption risk is the most significant risk associated with these positions in State or Territory owned enterprises. Individuals who are heads of such bodies can be vulnerable to corruption or financial misconduct as they generally have a high degree of influence regarding valuable contracts as well as decision making on potentially lucrative matters such as infrastructure development and access rights to local resources. The OECD's 2018 report titled 'State-Owned Enterprises and Corruption: What Are the Risks and What Can Be Done?' identified the oil, gas, mining, postal, energy, transportation and logistics sectors as more likely to have had experienced corruption or otherwise irregular practices than in other sectors. Australian State or Territory owned enterprises generally operate in the utilities (particularly energy and water), transport, infrastructure (particularly rail and ports) and forestry sectors.

53. Paragraphs (l) to (o) are straightforward on the text of the Rules. The individuals occupying these offices and positions are publicly available on the respective defence force websites (accessible at https://www.defence.gov.au/about/who-we-are/leaders,

https://www.airforce.gov.au/about-us/leadership, https://www.army.gov.au/about-us/leadership, https://www.navy.gov.au/about-navy/leaders).

54. Paragraph (p) specifies the most senior Australian diplomatic appointments as domestic PEPs under paragraph (a) of the definition under the Act. The Foreign Affairs Department publishes the list of individuals occupying such positions on its website at https://www.dfat.gov.au/about-us/our-people/homs/australian-ambassadors-and-other-representatives. The offices in paragraph (p) are limited to appointments made by the Governor-General so not to capture where individuals may temporarily occupy, or 'act in', the office while the substantive appointee is on leave.

55. Paragraph (q) specifies members of governing bodies of political parties represented in a legislature of the Commonwealth, a State or Territory are domestic PEPs under paragraph (a) of the definition under the Act. These individuals may be vulnerable to ML/TF risk due to the capacity of governing bodies to influence a party's public policy positions, and ability to select candidates that may stand for election in a legislature. Each party typically publishes the governing body members on its website.

1-6—Enrolment details

56. Section 1-6 specifies that enrolment details for the purpose of section 5 of the Act are the information mentioned in section 3-2, 3-3, and 3-4 of the Rules. The most significant implication of this definition is that where information is within the definition of 'enrolment details' in relation to a reporting entity or prospective reporting entity, the reporting entity must include the information in its enrolment application, and advise the AUSTRAC CEO of changes to those enrolment details within 14 days of the change arising under section 51F of the Act if the change relates to the information specified in sections 3-2 or 3-3 or within 12 months of the change occurring if the change relates to information specified in section 3-4 (annual earnings information).

1-7—Registrable details

57. Section 1-7 specifies what comprises registrable details in section 5 of the Act. The most significant implication of this definition is that it sets out what details AUSTRAC will publish on the Remittance Sector Register and the Virtual Asset Service Provider Register. These details can then be accessed by foreign regulators and law enforcement, reporting entities and foreign equivalents to allow them to verify that the person is appropriately regulated for AML/CTF to provide remittance or virtual asset services.

1-8—Transfer of value—excluded transfers

58. Pursuant to paragraph (b) of the definition of transfer of value in the Act, section 1-8 specifies which transfers are excluded from being transfers of value. Paragraph 1-8(2) prescribes that a transfer of a security or derivative that is not a virtual asset is not a transfer of value. Paragraph 1-8(3) identifies that a transfer of money is not a transfer of value if the following circumstances described in subparagraphs 1-8(3)(a) to (d) apply:

- the transfer of the money occurs in the course of a person performing administrative services for a client of the person that is an employer, and
- the administrative services relate to payments on payments, on behalf of the employer, of salary, wages or other benefits to its employees; or arrangements between the employer and its employees under which employees forgo amounts of salary or wages in return for benefits of a similar cost; or payments, on behalf of the employer, of superannuation contributions for its employees; and
- the transfer does not involve the receipt of physical currency from the payer or a person acting on behalf of the payer; and
- the transfer does not involve making physical currency available to the payee or to a person acting on behalf of the payee.

1-9 Security—managed investment schemes

59. To avoid doubt, section 1-9 clarifies that for the purposes of paragraph 7A(2)(a) of the Act, an interest in a managed investment scheme is a security. Under section 5 of the Act, managed investment scheme has the same meaning as in the Corporations Act 2001, which in section 9, defines an interest in a managed investment scheme (including a notified foreign passport fund) as a right to benefits produced by the scheme (whether the right is actual, prospective or contingent and whether it is enforceable or not). That reflects the position that an interest in a managed investment scheme is regarded as an ownership interest.

Part 2—Reporting groups

60. The amendments to the AML/CTF Act relating to reporting groups are set out in Part 1 of the Act. The amendments replace the former concept of a Designated Business Group (DBG) and introduces the concept of a 'reporting group' and 'lead entity' of a reporting group. Under subsection 10A(1) of the AML/CTF Act, a reporting group is broadly:

    - a business group (as defined in s 10A(3)), where at least one person in the group provides a designated service and each member of the group satisfies such conditions as specified in the AML/CTF Rules and the group is not of a kind ineligible under the Rules to be a reporting entity; or
    - a group of two or more persons, where each member of the group has elected in writing to be a member of the group and each election was made in accordance with the Rules.

61. The intention behind the establishment of reporting groups is group level management and mitigation of ML/TF risk, and AML/CTF compliance management consistent with FATF recommendation 18. This will also allow more efficient implementation of AML/CTF program obligations amongst group members by recognising and capturing traditional corporate group arrangements as found in the financial services sector, as well as other non-corporate structures and franchise arrangements. Non-reporting

entities are included in the concept as this reflecting the way modern businesses are structured in practice and under subsection 236B(5) of the Act, members of a reporting group may discharge obligations on behalf of other members in the reporting group. To avoid doubt, it is not a requirement for the lead entity to discharge obligations on behalf of members of the reporting group, this may be done by any entity that is a member of the reporting group, provided the conditions in section 2-3 and 2-4 of the Rules are satisfied.

2-1—Reporting group that is a business group

62. For the purposes of a reporting group to which paragraph 10A(1)(a) of the Act applies, it is a condition under subparagraph 10A(1)(a)(ii) of the Act, that each member of the group must have agreed in writing as to which member is the lead entity of the reporting group. All members of the business group, including members of the group that are not reporting entities must agree in writing to which member is the lead entity of the reporting group.

63. Subsection 2-1(1) sets out eligibility criteria for lead entities of reporting groups that are business groups, and that the agreement on which eligible member of the group is the lead entity must be made by each member of the business group in writing.

64. The requirement in paragraph 2-1(1)(a) is that the member who is to be lead entity must not be controlled by another member of the reporting group that provides designated services. Put another way, this means that the lead entity must sit above, or be equal with, any other reporting entities in a corporate or other ownership hierarchy structure. The lead entity may be the ultimate parent in a corporate hierarchy, or another level between an entity that provides designated services and the ultimate parent. This provides flexibility to reporting groups to select an appropriate lead entity.

65. The requirement in paragraph 2-1(1)(b) is that the member who is to be the lead entity must have capacity to determine the AML/CTF policies of other members in the group. This may be by virtue of the lead entity owning other members of the reporting group, or due to the practical influence, practices or patterns of behaviour relevant to the lead entity's relationship with other members of the reporting group.

66. The requirement in paragraph 2-1(1)(c) is that the member who is to be the lead entity has one of the specified connections to Australia, e.g. a body corporate being incorporated in Australia, which is essential to allowing AUSTRAC to supervise and regulate the lead entity's compliance with its obligations.

2-2—Reporting group formed by election

67. Section 2-2 sets out who may be in a reporting group formed by election, being a reporting entity or a person who discharges obligations imposed on members of the reporting group by the Act, the regulations or the Rules.

68. The requirement in subsection 2-2(1) provides the conditions that must be met by each member of a reporting group. This includes paragraph 2-2(1)(c), which captures circumstances where a reporting group may include members of a business group as well as other persons not captured as a member of a business group under paragraph 10A(1)(a) of the Act.

69. Subsection 2-2(2) provides that reporting group membership in this manner is available to a business group member only if all other members of its business group are also members of that same reporting group.

70. For the purposes of a reporting group formed by election, the lead entity of a reporting group is the member of the group that satisfies the requirements outlined in paragraphs 2-2(3)(a) to (d) of the Rules.

71. The requirement in paragraph 2-2(3)(a) is that the member who is to be lead entity must not be controlled by another member of the reporting group that provides designated services.

72. The requirement in paragraph 2-2(3)(b) is that, where the reporting group includes a member of a business group, the lead entity must be a member of that business group.

73. The requirement in paragraph 2-2(3)(c) is that the member who is to be the lead entity must have agreed to the member having capacity to determine AML/CTF policies of other members in the group. This agreement is likely to be recorded in a contract or written arrangement between members.

74. The requirement in paragraph 2-2(3)(d) is that the member who is to be the lead entity has one of the specified connections to Australia, e.g. a body corporate being incorporated in Australia, which is essential to allowing AUSTRAC to supervise and regulate the lead entity's compliance with its obligations.

75. Subsection 2-2(4) requires that where a person wants to join a reporting group, the lead entity of the reporting group must provide consent.

76. Subsection 2-2(5) provides that a business group member can make an election in writing to join a reporting group on behalf, and with consent, of all members of that business group. Where a person becomes a member of that business group, subsection 2-2(6) provides that that person also becomes a member of that reporting group.

77. Subsections 2-2(7) and (8) deal with the conditions for a member to leave a reporting group. Under subsection 2-2(4), an ordinary member (a member that is not the lead entity) may leave a reporting group if it gives the lead entity notice in writing. Under subsection 2-2(8), a lead entity may leave a reporting group if it gives the other members notice in writing. Subsection 2-2(9) provides that, if a reporting group member who is electing to leave that reporting group is also a business group member,

all members of that business group are also taken to have elected to leave that reporting group.

78. Subsection 2-2(10) sets the conditions for the continual operation of a reporting group formed by election. Paragraph 2-2(10)(a) specifies that a reporting group must not operate without a lead entity for a continuous period of more than 28 days. During the period within which a reporting group is operating without a lead entity, paragraph 2-2(10)(b) specifies that members of a reporting group must continue to comply with the AML/CTF policies of the most recent lead entity of the group that applied to the member immediately before the previous lead entity ceased to be lead entity of the group. Subsection 2-2(10) assists in ensuring business continuity for members of the group in the absence of a lead entity until a new lead entity is agreed upon by the members of the reporting group.

79. Subsection 2-2(11) provides operational clarity for a reporting group that includes business group members. In such circumstances, the member will be taken to be a member of the reporting group (rather than just the business group).

2-3—Conditions for discharge of obligations by members of a reporting group

80. Section 2-3 prescribes the requirements that a reporting group must satisfy before a member of the reporting group can discharge an obligation on behalf of another member in the reporting group. For the purposes of subsection 236B(5) of the Act, if a reporting entity is a member of a reporting group; and an obligation is imposed on the reporting entity by a provision of the Act, the regulations or the Rules, section 2-3 specifies that it is a condition that the reporting group has a lead entity before the obligation may be discharged by any other member of the reporting group.

2-4—Conditions for discharge of obligations by members of a reporting group that are not reporting entities

81. Section 2-4 prescribes the conditions that a reporting group must satisfy before a member of the reporting group can discharge an obligation on behalf of another member in the reporting group for the purposes of subsection 236B(5) of the Act. Subsection 236B(5) allows other members in a reporting group to discharge obligations imposed on reporting entities within the reporting group on behalf of any member within the group. The member who discharges the obligation need not be a reporting entity.

82. Subsections 2-4(2) and (3) of the Rules specifies that where a discharging member is not itself a reporting entity, the discharging member must have:
    - undertaken due diligence, in relation to persons who are employed or otherwise engaged and who perform functions relevant to discharging the obligation, that satisfies the requirements of the AML/CTF policies of the reporting entity included in those policies for the purpose of paragraph 26F(4)(d) of the Act; and

- provided training to those persons that satisfies the requirements of the AML/CTF policies of the reporting entity included in those policies for the purposes of paragraph 26F(4)(e) of the Act.

83. This is because non reporting entity members within a reporting group do not need to develop and maintain AML/CTF policies for the purposes of section 26F of the Act. The purpose of subsections 2-4(2) and (3) is to ensure that the discharging member undertakes personnel due diligence in relation to those persons who are employed or otherwise engaged and who perform functions relevant to discharging the obligation and provides personnel training to those persons that the persons would have otherwise received if they were employed or otherwise engaged by a reporting entity member of the reporting group.

Part 3—Enrolment

84. Part 3 of the Rules deals with the Reporting Entities Roll established under Part 3A of the Act.

85. Subsection 51C(1) of the Act prescribes that the AUSTRAC CEO must maintain a roll to be known as the Reporting Entities Roll. The Reporting Entities Roll serves as a record of reporting entities which are regulated by AUSTRAC. The information provided by reporting entities upon enrolment enables AUSTRAC to be informed of and understand persons who it regulates, as well as allow it to communicate with, and effectively regulate, those reporting entities.

Division 1—Applications

86. Subsection 51B(1) of the Act prescribes that a person commencing to provide a designated service must apply for enrolment as a reporting entity under subsection 51E(1) of the Act, no later than 28 days after the day on which the person commences to provide the designated service.

87. Subsection 51E(1) of the Act prescribes that a person may apply in writing to the AUSTRAC CEO for enrolment as a reporting entity. Paragraph 51E(2)(b) of the Act specifies that the enrolment application must be in the approved form, and contain the information required by the Rules.

3-1—Purpose of this Division

88. Section 3-1 provides the purpose of Part 3, Division 1 of the Rules, which is to prescribe the information that must be contained in an enrolment application made for the purposes of subsection 51E(1) of the Act.

3-2—Information about applicant's designated services

89. Section 3-2 prescribes the information about designated services provided or proposed to be provided that a reporting entity must include in an enrolment application made for the purposes of subsection 51E(1) of the Act. Collecting this information through enrolment will enable AUSTRAC to understand the designated service offerings of businesses it regulates.

90. Paragraphs 3-2(1)(a),(b), and (d) require a description of the designated service, the date the applicant commenced to provide or proposes to provide the designated service, and information on the industry in which the applicant provides or proposes to provide the designated service. The 'description of the designated service' in paragraph 3-2(1)(a) requires the applicant to identify which designated services prescribed in section 6 of the Act are relevant to their business whereas 'information on the industry in which the applicant provides or proposes to provide the designated service' seeks information on the type of industry within which the applicant is operating its business and providing designated services. For example, when applying via the approved form in paragraph 51E(2)(a) of the Act, a law firm might select multiple designated services from table 6 of section 6 of the Act in response to paragraph 3-2(1)(a), and then select 'legal sector' as the industry in which it provides or proposes to provide the designated service in response to paragraph 3-2(1)(d).

91. Paragraph 3-2(1)(c) deals with the way in which the applicant meets the geographical link test contained in subsection 6(6) of the Act. This allows AUSTRAC to understand the geographical footprint of the reporting entity to support effective supervision.

92. Paragraphs 3-2(2)(a) to (c) requires the applicant to advise whether it is registered, has applied or intends to apply for registration on the RSR or VASPR.

93. Subsection 3-2(3) requires an applicant to advise whether section 233K of the Act—being an exemption relating to the operation of no more than 15 gaming machines—applies or will apply to the applicant if they provide a designated service. Under section 233K of the Act, certain provisions of the Act do not apply to a reporting entity that provides specified gambling services in circumstances where the entity and any related entity that is a reporting entity, are entitled to operate in total no more than 15 gaming machines under State or Territory licences.

94. Subsection 3-2(4) requires an applicant to advise whether the applicant is solely providing designated service item 54 from table 1 of section 6 of the Act. Item 54 of table 1 in section 6 of the Act covers a holder of an Australian financial services licence who arranges for a person to receive another designated service. Reporting entities who provide designated services only of that kind are subject to fewer obligations under the Act (see sections 26T, 30(10), 39(7), 44(6), 47(5) of the Act).

3-3—Information relating to the applicant

95. Section 3-3 of the Rules prescribes the information about the reporting entity that must be included in an enrolment application made for the purposes of subsection 51E(1) of the Act.

96. Information provided by an applicant under subsections 3-3(1) to (7) is information needed for AUSTRAC to perform its functions under the Act, by allowing AUSTRAC to understand identifying information about the applicant, where it provides designated services, the identities of beneficial owners and governing bodies of the applicants.

97. Some of the information, such as that required under 3-3(1)(h) and (i) are to allow AUSTRAC to better understand the demographics of the reporting entity population to enable better education and support, and to assist with its policy development function under the Act.

98. Paragraph 3-3(1)(i) requires a reporting entity to identify whether it is a small business entity within the meaning of sections 328-110 of the Income Tax Assessment Act 1997 for the previous year, if the applicant is resident in Australia. AUSTRAC considers this a low-regulatory burden method of understanding the volume of reporting entities that are small businesses as it does not require businesses to apply a new test to itself, it should generally already know whether it meets the eligibility requirements due to its taxation arrangements. Under Australia's tax laws, small business entities are afforded concessions such as instant asset write-offs, capital gains tax concessions, simplified depreciation rules, roll-over relief and immediate deductions for certain start-up expenses. A business is eligible to be a small business entity for an income year if it carries on a business in that year, and has an aggregated turnover of less than $10 million. Aggregated turnover includes the turnover of businesses 'connected with' (which is based on control) or affiliated with the applicant.

99. Paragraph 3-3(1)(n) requires the application to advise the domain names for all websites (if any) through which the applicant provides or will provide its designated services. The current Macquarie dictionary entry for 'domain name' is 'the name of a server connected to the internet comprising the name of the host, followed by the domain, such as commercial, academic, news, etc., followed by the country of origin (with the exception of the US).'

100. Subsections 3-3(2) to (7) are straightforward on the face of the text. The incorporation by reference in subsection 3-3(3) of the term 'ultimate holding company' in the Corporations Act 2001 is permitted by paragraph 14(1)(a) of the Legislation Act 2003.

101. Paragraph 3-3(8) requires the applicant to provide information so AUSTRAC can understand whether the applicant is a member of a reporting group, whether the applicant is the lead entity of a reporting group, information about the members of the reporting group if the applicant is the lead entity, and information about the lead entity if the applicant is a member of a reporting group but not the lead entity.

3-4—Information relating to earnings

102. Section 3-4 of the Rules requires enrolment applications to include information about the most recent 12 month earnings of the applicant, where the applicant or the applicant's corporate group's earnings are greater than $100,000,000. This section recreates the provisions from the former rules relating to earnings information, updated in the contemporary drafting style to increase readability.

103. Subsection 3-4(1) provides the definition of earnings, determined by whether the applicant is an ADI or registered financial sector entity (or a related body corporate of one) and whether the applicant is a foreign company (of a subsidiary of one). ADIs and registered financial sector entities (defined in section 1-4 as a registered corporation under the Financial Sector (Collection of Data) Act 2001) are to provide total profit (rather than earnings) before tax, depreciation and amortisation in recognition of different treatment of interest expenses for entities who engage in the provision of finance in the course of carrying on business in Australia. For other applicants, earnings is defined as the total earnings of the person for the period before tax, interest, depreciation and amortisation.

104. Subsection 3-4(2) prescribes the information the application must contain, being just the applicant's earnings for a period of 12 months if it is not a member of a corporate group; and where the applicant is a member of a corporate group, the total aggregate earnings of the applicant and all other related bodies corporate that are leviable entities. Subsection 3-4(2) does not prescribe which 12 month period earnings are to pertain to, allowing the requirement to be adaptable to applicants' varying financial years.

105. The effect of section 1-6 and subsection 3-9(2) of the Rules and section 51F of the Act is that reporting entities are required to advise AUSTRAC in accordance with the approved form of the most recently finalised 12 month period earnings within 14 days of the financial statements being finalised.

3-5—Information about the person completing the application and declaration

106. Section 3-5 of the Rules prescribes the information that needs to be included about the person completing the reporting entity's enrolment application and requires that a declaration be made about the truthfulness and correctness of the information included in an enrolment application made for the purposes of subsection 51E(1) of the Act.

Division 2—Correction and removal of enrolment details

107. Division 2 of Part 3 of the Rules contain sections 3-6 to 3-8, which relate to the management of the Reporting Entities Roll, including correction of entries, removal of enrolment details (including names), requests to remove reporting entities from the roll, and changes to enrolment details. These machinery provisions allow the AUSTRAC CEO to maintain an accurate up-to-date Reporting Entities Roll.

3-6—Correction of entries in the Reporting Entities Roll

108. Section 3-6 is made for the purpose of paragraph 51C(4)(a) of the Act to prescribe that where the AUSTRAC CEO reasonably believes there is an error in, or an omission from, an entry in the Reporting Entities Roll, the AUSTRAC CEO may correct the error or omission. This permits the AUSTRAC CEO to update the Reporting Entities Roll based on information obtained by means other than a reporting entity advising updates to its enrolment details by way of the approved form required by section 51F of the Act. Information sources may include (but are not limited to) other government body data holdings or information obtained throughout AUSTRAC's supervision activities.

3-7—Removal of name and enrolment details on AUSTRAC CEO's own initiative

109. Section 3-7 is made for the purpose of paragraph 51C(4)(b) of the Act to prescribe that the AUSTRAC CEO may remove a person's name and enrolment details from the Reporting Entities Roll on the AUSTRAC CEO's own initiative if the AUSTRAC CEO reasonably believes that the person has ceased to provide designated services or has not commenced to provide designated services. This will allow the AUSTRAC CEO to remove a person's name and enrolment details from the Reporting Entities Roll:
    - if the AUSTRAC CEO reasonably believes that the person has ceased to provide designated services but the person has not informed the AUSTRAC CEO of the cessation,
    - if the AUSTRAC CEO reasonably believes the reporting entity no longer exists,
    - if a reporting entity notifies the AUSTRAC CEO informally (in a way other than in the approved form requesting removal from the Reporting Entities Roll under section 51G of the Act) that it has ceased to provide designated services.

110. The ability for the AUSTRAC CEO to keep the Reporting Entities Roll accurate and up-to-date is important for regulatory and economic efficiency, so AUSTRAC can determine how to deploy its education and supervision functions.

3-8—Request to remove entry from Reporting Entities Roll—required information

111. Section 3-8 is made for the purpose of paragraph 51G(2)(b) of the Act to prescribe the information that is required to be provided in a request by a person under subsection 51G(1) of the Act to remove the person's name and enrolment details from the Reporting Entities Roll. The AUSTRAC CEO must consider the request and remove the person's name and enrolment details from the Reporting Entities Roll if he or she is satisfied that it is appropriate to do so, having regard to the matters in paragraphs 51G(3)(a) to (c) of the Act.

Division 3—Changes in enrolment details

3-9—Changes in enrolment details

112. Section 3-9 is made for the purposes of paragraph 51F(1) of the Act to prescribe the types of changes to enrolment details that are required to be advised to the AUSTRAC CEO. The effect of subsection 3-9(1) is that any change to enrolment details set out in sections 3-2, and 3-3 and of the Rules must be advised to the AUSTRAC CEO in the approved form within 14 days of the change arising.

113. Subsection 3-9(2) provides that any change to enrolment details set out in section 3-4 of the Rules (information relating to earnings) must be advised to the AUSTRAC CEO in the approved form for each succeeding period of 12 months.

Part 4—Registration

114. Parts 6 and 6A of the Act respectively deal with the Remittance Sector Register (RSR) and the Virtual Asset Service Provider Register (VASP Register). These Parts of the Act implement FATF recommendation 26, which requires countries to take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner, or holding a significant or controlling interest in, or holding a management function in a remitter or VASP. Recommendation 26 provides that at a minimum, countries should ensure that a business providing a value transfer service or virtual asset service, is licensed or registered and subject to effective systems for monitoring and ensuring compliance with national AML/CTF requirements.

115. FATF recommendation 27 also requires countries to empower supervisors to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the financial institution's license.

116. The interpretive note to FATF recommendation 14 clarifies that a country need not impose a separate licensing or registration system with respect to already licensed or registered businesses, if under such license or registration, the person is permitted to perform money or value transfer services which are already subject to measures giving effect to FATF recommendation 26 and 27. Parts 6 and 6A of the Act reflect parliament's intent to fill the gap by subjecting remitters and VASPs to registration with the AUSTRAC CEO.

117. Section 75 of the AML/CTF Act requires the AUSTRAC CEO to maintain a register to be known as the RSR. Section 76B of the Act requires the AUSTRAC CEO to maintain a register to be known as the VASP Register. The registers also serve as a record of reporting entities who are registered with AUSTRAC as a remittance network provider, an independent remittance dealer, a remittance affiliate of a registered remittance network provider or a virtual asset service provider.

118. Section 74 of the AML/CTF Act prohibits a person from providing registrable remittance services or registrable remittance network services unless they are

registered. Similarly, section 76 of the Act prohibits a person providing registrable virtual asset services if they are not registered.

119. Sections 75B and 76D of the Act set out that a person may apply in writing to the AUSTRAC CEO for registration. The application must be in the approved form and contain the information required by the Rules.

120. The requirement for remitters and VASPs to register with AUSTRAC prior to the provision of a registrable service is intended to mitigate the risk of criminals and their associates from abusing and infiltrating these sectors.

121. Part 4 of the Rules reflects an enhanced registration framework, to prevent criminal entities from infiltrating and exploiting the remittance and VASP sectors. The provisions now require an application for registration to cover the following areas:
    - the candidate's ML/TF risk exposure and management of ML/TF risks;
    - the candidate's capability to meet AML/CTF obligations; and
    - additional background screening questions on individuals who own or manage the applicant.

122. The increased standard and level of information to be required in an application for registration is consistent with the approaches taken in other jurisdictions, such as the United Kingdom, Singapore, and Hong Kong.

123. Remittance services and virtual asset services were assessed by AUSTRAC in the ML NRA as high and medium-high vulnerability respectively, for money laundering, whereas both were assessed in the TF NRA as highly vulnerable to misuse for terrorism financing. This was in part because remittance and virtual asset service providers are subject to less oversight and regulation than other financial sub-sectors by other Australian regulators.

124. A strengthened registration process will enable AUSTRAC to more comprehensively identify, assess and mitigate the ML/TF risks associated with the remittance and virtual asset services, and effectively deploy the regulatory tools available to uplift compliance in those sectors.

125. The information collected in an application for registration will be a component of an effective mechanism to identity and mitigate ML/TF risks in the financial system by preventing registration of, or imposing conditions on the registration of, candidates:
    - who have demonstrated limited understanding of their AML/CTF obligations or ML/TF risks, or do not have, or plan to have, adequate AML/CTF policies in place to identity, mitigate and manage their ML/TF risks; or
    - do not have the required capability or competency within its existing resources, to meet its AML/CTF obligations.

126. An enhanced registration process should also provide reporting entities with greater confidence in the registration process and contribute to reducing undue de-banking and de-risking of remitters and virtual asset service providers by other reporting entities.

127. Commonalities between the information required for registration on the RSR and VASP register have been amalgamated where possible for simplicity. However, the provisions demarcate obligations where they are solely applicable to either RSP or VASP registration. This reflects that Part 4 of the Rules streamlines the requirements for the RSR and VASP Register for reporting entities and AUSTRAC, which further advances the AML/CTF reform objectives of simplification and modernisation.

Division 1—Management of the RSR and VASP Register

4-1—Correction of entries

128. If the AUSTRAC CEO decides to register a person under subsections 75C(2) or 76E(2) of the Act, the information required by section 75A or 76C respectively, must be entered on either the RSR or VASP Register, as applicable.

129. Specified information from these registers will be published on the AUSTRAC website so it is necessary that the information set out on the registers is correct and complete. To ensure that information on the registers contains accurate and up-to-date details relating to a person's registration, subsection 4-1(2) permits the AUSTRAC CEO to correct information which the AUSTRAC CEO reasonably believes is incorrect or incomplete.

130. Where the AUSTRAC CEO makes a correction of an entry under subsection 4-1(2), subsection 4-1(3) the AUSTRAC CEO is required to provide a notice detailing the changes to the person whose registration the correction relates to. If that person is a registered remittance affiliate of a registered remittance network provider, the notice must be given to the registered remittance network provider.

4-2—Publication of register information

131. Subsection 4-2(1) requires the AUSTRAC CEO to publish the following information from each entry on the RSR and the VASP register:
    - the name of the person;
    - the registrable details in relation to the person (which are defined in section 1-7 of the Rules); and
    - if the person's registration is suspended, information identifying that the person's registration is suspended.

132. For entries on the RSR, the following information will also be published:
    - whether the person is registered as
        - a remittance network provider; or

    - an independent remittance dealer; or a remittance affiliate of a registered remittance network provider.
- if the person is registered as a remittance affiliate of a registered remittance network provider-the name of the registered remittance network provider.

133. The RSR and VASP Register are to be published by the AUSTRAC CEO on the AUSTRAC website which is accessible at www.austrac.gov.au.

134. Publication of each register will allow foreign remittance service providers and VASPs to verify that their counterparties are appropriately registered for AML/CTF, as well as assist foreign regulators and law enforcement understand the registration details of Australian remitters and VASPs. Registration on the RSR and VASP Register does not indicate to prospective customers or investors that reporting entities registered that any consumer guarantees, quality assurance or that minimum capital requirements apply as these are outside of AUSTRAC's regulatory remit but, depending on the nature of the business, may be overseen by other Commonwealth regulators such as APRA, ASIC, ACCC and State and Territory offices of fair trading.

135. Subsection 4-2(2) of the Rules allows the AUSTRAC CEO to publish, on AUSTRAC's website, one or more conditions, mentioned in paragraph 75A(1)(d) or 76C(b) of the Act, to which the registration of a person is subject. AUSTRAC will generally publish details of conditions placed on registration, with the exception of where a condition may be sensitive, such as the imposition of particular transaction monitoring or enhanced customer due diligence triggers, which would not be published so not to allow conditions to be deliberately circumvented by customers seeking to exploit the registered entities' services.

Division 2—Information requirements for registration applications

4-3—Purpose of this Division

136. Section 4-3 provides the purpose of Part 4, Division 2 of the Rules, which is to prescribe the information that must be contained in a registration application made under subsections 75B(1) and (2), and 76D(1). Information to be included in applications for registration is used by the AUSTRAC CEO when making a decision under sections 75C or 76E of the Act. The AUSTRAC CEO must decide to register a candidate if the AUSTRAC CEO is satisfied that it is appropriate to do so, having regard to:
    - whether registering the person would involve a significant ML/TF or other serious crime risk; and
    - any other matters specified in the Rules. See Division 3 of Part 4 for other matters to which the AUSTRAC CEO must have regard.

4-4—Application—general information

137. Subsections 4-4(1) to 4-4(7) of the Rules prescribes the general identifying, ownership, and operating structure information about the candidate that is proposed to be registered and that must be included in a registration application made for the purposes of subsections 75B(1), 75B(2) or 76D(1) of the Act. Information provided about the candidate under these subsections is information that is required for the AUSTRAC CEO to perform their functions under the Act, by allowing the AUSTRAC CEO to understand identifying information about the candidate, the locations the candidate intends to provide registrable services, the identities of beneficial owners and governing bodies of the candidate, and generally the size, nature and complexity of the candidate's business.

4-5—Information relating to ML/TF risks

138. Section 4-5 requires the applicant to provide information relating to the key ML/TF risks a candidate faces in providing its proposed designated services which that be provided in a registration application. Subparagraph 4-5(a) requires the applicant to have assessed and identified the key ML/TF risks.

139. Paragraph 4-5(b) sets out five broad categories on which the applicant must provide information on. They are:
    - the ML/TF risks posed by the different types of legal entity that the candidate provides registrable services to;
    - the ML/TF risks of providing registrable services in countries, other than Australia, in which the candidate operates;
    - the products and services which will be provided to the candidate's customers and the ML/TF risks of those products and services;
    - which delivery channels will be used by the candidate to provide the registrable services. For example, will the services be provided face-to-face, through a website or an app. The ML/TF risks of providing the registrable services using these delivery channels;
    - the kinds of transactions the candidate will undertake in providing the registrable services. For example, the methods of payment the customer can use, how the candidate will transfer value from the payer to the payee. The ML/TF risks of providing the registrable services using these transaction types.

140. This information, as well as the candidate's processes to undertake, review and keep up to date its ML/TF risk assessment, will be used by the AUSTRAC CEO to consider the ML/TF risks of the candidate including whether the candidate has identified relevant ML/TF risks that it may reasonably face in providing registrable services.

4-6—Information relating to AML/CTF policies

141. Section 4-6 requires information be provided in a registration application about the candidate's AML/CTF policies. This information allows the AUSTRAC CEO to consider whether the candidate has in place policies, procedures, systems and controls

to appropriately manage ML/TF risks it may reasonably face, as well as the candidate's ability to meet its AML/CTF obligations.

4-7—Information relating to accounts with financial institutions

142. Section 4-7 sets out information required in a registration application relating to each account with a financial institution that the candidate will use in providing its registrable services, covering both accounts in the name of the applicant or any other individual who is an account holder or signatory of the account. This information allows the AUSTRAC CEO to make enquiries within AUSTRAC's information holdings of international funds transfer instructions reports to identify whether the candidate may have provided remittance or virtual asset services prior to registration, and provides details on the individuals that will have account authority within the candidate's business.

4-8—Information relating to other persons assisting

143. Section 4-8 sets out information relating to other persons assisting the candidate to meet its obligations (under outsourcing arrangements) that must be included in a candidate's application. This information allows the AUSTRAC CEO to consider whether the outsourcing arrangements will increase or reduce the ML/TF risk of the applicant providing registrable services.

4-9—Information relating to key personnel and past unlawful activity etc.

144. Section 4-9 sets out information regarding key personnel of the candidate that must be included in a registration application.

145. Subsection 4-9(1) includes information regarding personal information of each of the candidate's key personnel.
    - Under paragraph 4-9(2)(a), whether the candidate or any of its key personnel have been charged or convicted of an offence against the Act, or of an offence against a law of the Commonwealth, a State or Territory or a foreign country of any of the following kinds:
        - money laundering;
        - financing of terrorism;
        - proliferation financing;
        - people smuggling;
        - fraud (including scams);
        - a serious offence (as defined in the Act) of any other kind, and
    - Under paragraphs 4-9(2)(b) and (c), information about the candidate and its key personnel relating to any contraventions under the Act, and other civil proceedings or regulatory or disciplinary process in Australia or a foreign country related to the management of an entity, or commercial or professional activity is also

required; and involved an adverse finding as to the competence, diligence, judgement, honesty or integrity of the candidate or the key personnel (as applicable).

- Under paragraphs 4-9(2)(f) and (g), the details of key personnel's past registration, licencing or approval (as the case may be) on the Remittance Sector Register, the Virtual Asset Service Provider Register or for any regulated activity in the financial sector (in Australia or otherwise).
- Under paragraph 4-9(2)(h), the details of key personnel's training over the last 12 months.

146. This section allows the AUSTRAC CEO to consider the criminal history (if any) of the key personnel of the candidate to support the assessment of the ML/TF risk involved in registering the person, as well as prior compliance with other regulatory regime or contractual requirements.

4-10—Additional requirements for application by a remittance network provider for registration of an affiliate

147. Section 4-10 sets out the information required in an application made by a registered RNP for the candidate to be registered as a remittance affiliate of the RNP. This information allows the AUSTRAC CEO to consider whether the RNP has assessed the suitability of the candidate to be a remittance affiliate of the RNP and whether the RNP, in its assessment of the affiliate's suitability, has taken into account the related ML/TF risks that the provider may reasonably face. Subsection 4-10(c) requires the RNP to provide information on whether the candidate to be registered as a remittance affiliate of the RNP has consented to the making of the application by the provider.

4-11—Additional requirements for application by independent remittance dealer for registration as a remittance affiliate

148. Section 4-11 sets out the requirements for a registered RNP to provide information on whether the candidate who is the independent remittance dealer has consented to the RNP making the application as well as information on when the consent was given.

4-12—Additional requirements for application for registration as an independent remittance dealer or a remittance affiliate of network provider

149. Section 4-12 sets out additional information required in an application for registration as an independent remittance dealer or a remittance affiliate of a registered RNP. This information allows the AUSTRAC CEO to consider the ML/TF risks associated with the candidate's proposed provision of remittance services as either an independent remittance dealer or a remittance affiliate of a registered RNP.

4-13—Additional requirements for application for registration as a remittance affiliate of remittance network provider

150. Section 4-13 sets out the additional requirements in an application for registration as a remittance affiliate of a RNP. This information allows the AUSTRAC CEO to consider the overall ML/TF risk of the RNP and its remittance affiliates in the management of its remittance operations.

4-14—Additional requirements for application for registration as a virtual asset service provider

151. Section 4-14 sets out information required in a registration application for registration as a VASP. This information allows the AUSTRAC CEO to consider the ML/TF risks associated with the candidate's proposed provision of virtual asset related designated services.

Division 3—Registration decisions

152. Subsection 75C(2) of the Act requires the AUSTRAC CEO to register a person only if the AUSTRAC CEO is satisfied that it is appropriate to do so having regard to whether the registering the RSP would involve a significant money laundering, financing of terrorism, people smuggling or other serious crime risk, and such other matters, if any, as are specified in the Rules. Similarly, subsection 76E(2) of the Act sets out the same requirements for VASP registration although people smuggling risk is not a named risk factor.

153. Subsection 75C(3) of the Act outlines, for RSP registration decisions (without limiting the matters that may be specified), that the matters the Rules may specify may relate to the following:
    - offences of which the applicant for registration, a person proposed to be entered on the Remittance Sector Register as a remittance affiliate of the applicant, or any other person, has been charged or convicted under the law of the Commonwealth, a State or Territory or a foreign country;
    - the compliance or non-compliance of the applicant, a person proposed to be entered on the Remittance Sector Register as a remittance affiliate of the applicant, or any other person, with this Act or any other law;
    - the legal and beneficial ownership and control of the applicant, a person proposed to be entered on the Remittance Sector Register as a remittance affiliate of the applicant, or any other person;
    - the kinds of designated services to be provided by the applicant or by a person proposed to be entered on the Remittance Sector Register as a remittance affiliate of the applicant;
    - the consent of a person proposed to be entered on the Remittance Sector Register as a remittance affiliate of the applicant.

154. For VASP registration decisions, the additional matters are set out in subsection 76E(3) and in effect, replicate (a) to (c) of subsection 75C(3) of the Act.

4-15—Registration decisions—matters to which AUSTRAC CEO must have regard

155. Section 4-15 of the Rules provide the other matters to which the AUSTRAC CEO must have regard to in an application for registration. Section 4-15 focuses on the candidate's ML/TF risk exposure and management of its ML/TF risk, and its capacity to meet its AML/CTF obligations in addition to the considerations prescribed in subsections 75(2) and 76E(3) of the Act.

156. Paragraph 4-15(a) of the Rules allows the AUSTRAC CEO, in deciding whether to register a person, to have regard to any offences of which any of the following persons has been charged or convicted under the law of the Commonwealth, a State or Territory or a foreign country:

    (i) the candidate; and

    (ii) the key personnel of the candidate.

157. Paragraph 4-15(b) allows the AUSTRAC CEO to consider both the compliance and non-compliance of the persons specified in subparagraphs 4-15(b)(i) to (iii) with the Act or any other law of the Commonwealth, a State or Territory or a foreign country, in deciding whether to register a person. This means that where a person, who is specified in subparagraphs 4-15(b)(i) to (iii) has failed to meet a legal obligation or follow the rules and regulations outlined in the Act or any other law of the Commonwealth, a State or Territory or a foreign country the AUSTRAC CEO may weigh this as a factor in determining whether the candidate is appropriate to provide registrable services.

158. Paragraph 4-15(c) allows the AUSTRAC CEO to consider whether consent was obtained by the remittance network provider if it is applying for registration on behalf of a remittance affiliate. If the consent of the remittance affiliate has not been obtained by the remittance network provider, the AUSTRAC CEO is unlikely to register the remittance affiliate.

159. Paragraph 4-15(d) allows the AUSTRAC CEO to consider whether the candidate and its key personnel have experience that is appropriate, having regard:
    - the nature, size and complexity of the candidate's business; and
    - the risks of money laundering, financing of terrorism and proliferation financing that the candidate may reasonably face in providing its registrable services.

160. This paragraph allows the AUSTRAC CEO to identify which candidates, and its key personnel, have experience that may not be appropriate, having regard to the matters specified in paragraph 4-15(d)(i) and (ii). While a low level of experience may not automatically disqualify a person from registration with AUSTRAC, the AUSTRAC CEO will also consider other factors, such as the candidate's capability and competency to be registered, when making their decision.

161. Paragraph 4-15(e) allows the AUSTRAC CEO to consider the likelihood of the candidate conducting a business involving the provision of registrable services. There are circumstances wherein persons will apply for registration with AUSTRAC for the sole purpose of on-selling the registration once approved. On-selling in these circumstances introduces ML/TF risk into the RSP and VASP ecosystems. This is because, by using a purchased registration, criminals can bypass the usual due diligence and registration application procedures that they would otherwise have undergone if they had, themselves, had applied for registration with AUSTRAC.

162. Subsection 4-15(f) allows the AUSTRAC CEO to consider, in deciding whether to register a person, the operational readiness of the candidate in relation to the proposed registration, including its ability to comply with the Act, the regulations and the Rules following registration. By way of an example, if a candidate does not provide information setting out the AML/CTF policies that it has in relation to carrying out customer due diligence in accordance with Part 2 of the Act, the AUSTRAC CEO may refuse the candidate's application for registration as the candidate would not be operationally ready within the meaning of paragraph 4-15(e), given the requirement to provide such information about the policy pursuant to paragraph 4-6(1)(f) of the Rules.

163. Paragraph 4-15(g) allows the AUSTRAC CEO to consider, in deciding whether to register a person, the proposed resourcing (including personnel resourcing) of the candidate in relation to the provision of its registrable services. In assessing the proposed resourcing of the candidate, the AUSTRAC CEO is able to consider whether the candidate will have sufficient resources to comply with its AML/CTF obligations. Insufficient resourcing of AML/CTF compliance functions within registered reporting entities increases the likelihood that the business cannot appropriately identify, assess, manage and mitigate ML/TF risks it faces.

164. A decision by the AUSTRAC CEO to not register a person is a reviewable decision and enlivens the reviewable decision framework under Part 17A of the Act.

Division 4—Suspension of registration

165. The ability to suspend registrations is an important regulatory tool for AUSTRAC and complements the power that the AUSTRAC CEO possesses to cancel or impose conditions on registration. The suspension powers give the AUSTRAC CEO the ability to quickly respond to a wide range of operational circumstances, reduce the likelihood of imminent ML/TF harm, and provide for the stopping of remittance or virtual asset services while matters are investigated.

4-16—Purpose of this Division

166. Section 4-16 provides the purpose of Part 4, Division 4 of the Rules, which is to prescribe requirements relating to suspension of registration for the purpose of section 75H and 76K of the Act.

4-17—Suspension of registration

167. Section 4-17 specifies the grounds on which the AUSTRAC CEO may suspend a person's registration. The grounds specified largely reflect the matters that the AUSTRAC CEO must have regard to when determining whether it is appropriate to register a person.

168. If the AUSTRAC CEO reasonably suspects that the registered person, any of its key personnel or any associate of the person or its key personnel, has been charged or convicted of an offence against the Act, or an offence against a law of the Commonwealth, a State or Territory or a foreign country of any of the following kinds:
    - money laundering;
    - terrorism or financing of terrorism;
    - proliferation financing;
    - people smuggling;
    - fraud (including scams);
    - a serious offence of any other kind,

    the AUSTRAC CEO may suspend a person's registration under Part 6 or Part 6A of the Act.

169. The inclusion of the "any associate of the person or its key personnel" in paragraph 4-17(a) allows the AUSTRAC CEO to consider any offences of which an individual, who is associated with the registered person or its key personnel, has been charged or convicted of an offence against the Act, or an offence against a law of the Commonwealth, a State or Territory of a foreign country of the kinds specified in paragraphs 4-17(a)(i) to (vi). This may be relevant if the AUSTRAC CEO suspects that an associate of a key personnel is involved in the operation of a registered reporting entity, and reasonably suspects that person is involved in criminality.

170. If the AUSTRAC CEO reasonably suspects that the registered person or its key personnel are repeatedly contravening or are continually contravening the Act, the regulations or the Rules, paragraph 4-17(d) allows the AUSTRAC CEO to suspend a person's registration under Part 6 or Part 6A of the Act on that basis. This is a lower threshold than paragraph 4-17(b) which requires the court to find that the person or any of its key personnel has contravened the Act, the regulations or the Rules. This allows the AUSTRAC CEO an opportunity to suspend the registration while further investigation is undertaken to determine an appropriate enforcement response (if any).

171. A decision by the AUSTRAC CEO to suspend a person's registration is not a reviewable decision. The suspension of a person's registration is a preliminary decision that may lead to the making of a substantive decision. It allows AUSTRAC a period of time to investigate the matters and determine if it is appropriate to take further action relating to the person's registration including imposing conditions or cancelling the

person's registration with AUSTRAC as a remittance service or virtual asset service provider.

172. The AUSTRAC CEO may suspend a registration if the AUSTRAC CEO has a reasonable suspicion that one of the matters in paragraphs 4-17(a) to (i) apply. This is a purposefully lower threshold that what is required to make a decision to cancel a person's registration in recognition that suspension is an interim measure allowing AUSTRAC to collect evidence or make enquiries to inform whether to take further regulatory action.

4-18—Effect of suspension—renewal and advising of certain matters

173. While a reporting entity cannot provide a registrable services while their registration is suspended, the effect of section 4-18 of the Rules is that the renewal of registration provisions set out in Division 6 of Part 4 of the Rules continue to apply to the reporting entity. Additionally, the reporting entity has a continuing obligation to advise of both changes in circumstances that could materially affect the reporting entity's registration, and the matters set out in Part 4, Division 7 of the Rules.

4-19—Period of suspension

174. Subsection 4-19(1) provides that suspension of registration has effect for a period of up to 3 months. Subsection 4-19(2) and (3) provide that the period of the suspension of registration can be extended once for a period of up to three months if the AUSTRAC CEO continues to reasonably suspect that one or more of the grounds set out in section 4-17 applies.

4-20—Notice of suspension decision

175. Section 4-20 requires that if the AUSTRAC CEO decides to suspend a person's registration under Part 6 or 6A of the Act, the AUSTRAC CEO must give to the person a written notice containing the information specified in subsection 4-20(2) as soon as practicable. The notice will inform the recipients of the period of suspension, the effect of the suspension, being that for the period of suspension, the person cannot provide registrable services.

176. If the person is a registered remittance affiliate of a RNP, the notice must also be provided to that RNP as the RNP cannot provide an item 32A of table 1 in section 6 of the Act designated service to the remittance affiliate for the period of the remittance affiliate's suspension.

177. If a registered RNP's registration is suspended, the notice of suspension must also be provided to each of its registered remittance affiliates as each affiliate is unable provide an item 29 or 30 of table 1 in section 6 of the Act designated service using platform or operating system of the registered RNP, while the network provider's registration is suspended.

4-21—Notice of extension of suspension

178. Following a decision by the AUSTRAC CEO under sections 4-17 and 4-19 to extend the suspension of a person's registration for a further period of time, section 4-21 of the Rules requires that the AUSTRAC CEO give to the person a written notice containing the information specified in subsection 4-21(2). The notice will inform the recipients of the further period of suspension, the effect of the continuing suspension, which is that for the extended period of suspension, the person cannot provide registrable services.

179. If the person is a registered remittance affiliate of a RNP, the notice must also be provided to that RNP as the registered network provider cannot provide an item 32A of table 1 in section 6 of the Act designated service to the remittance affiliate for the extended period of the remittance affiliate's suspension.

180. If a registered RNP's registration is suspended for an extended period, the notice must also be provided to each of its registered remittance affiliates as each affiliate is unable provide an item 29 or 30 of table 1 in section 6 of the Act designated service using platform or operating system of the registered remittance network provider, while the network provider's registration continues to be suspended.

4-22—Revocation of suspension of registration

181. Section 4-22 allows the AUSTRAC CEO to lift the suspension of a person before the period of suspension ends if the AUSTRAC CEO is satisfied that it is appropriate to do so. Such circumstances may include where the suspended person has completed remediation on the issue that triggered the AUSTRAC CEO to decide to suspend the person's registration.

4-23—Notice of decision to revoke suspension of registration

182. Section 4-23 requires the AUSTRAC CEO, if the AUSTRAC CEO has decided to revoke the suspension of a person's registration, to provide that person with written notice of the decision as soon as practicable after the decision to revoke the suspension of the person is made. The notice must also contain the date the suspension is to be lifted, which may be a date distinct from the date the AUSTRAC CEO decides to lift the suspension (for example, if the suspended person has demonstrated to AUSTRAC that remediation activity is substantially complete, and projected to be finished on a particular date).

4-24—Register entry in relation to suspension of registration

183. Section 4-24 requires that when the AUSTRAC CEO suspends a person's registration, the person's entry on the applicable register must be updated to show the registration is suspended. This information is also part of the information required by section 4-2 to be published on the AUSTRAC website.

184. The AUSTRAC CEO must remove the information from the register after the suspension is revoked under subsection 4-22(1) or following the end of the suspension period.

Division 5—Cancellation of registration

185. Sections 75G and 76J of the Act allows the AUSTRAC CEO to cancel a person's registration if the AUSTRAC CEO is satisfied that it is appropriate to do so having regard to the matters set out in subsections 75G(1) and 76(J)(1).

186. Subsections 75G(1) and 76J(1) of the AML/CTF Act allow the AUSTRAC CEO to cancel the registration of a person if satisfied that it is appropriate to do so, having regard to:
- whether the continued registration of the person involves, or may involve a significant money laundering, financing of terrorism, people smuggling (section 75G only) or other serious crime risk; or
- one or more breaches by the person of a condition of registration; or
- such other matters (if any) as are specified in the AML/CTF Rules.

4-25—Cancellation of registration

187. Section 4-25 builds upon the matters that the AUSTRAC CEO must consider as required under subsections 75G(a) and 76J(1) of the Act in relation to cancellation of registration by providing that allow the AUSTRAC CEO to have regard to, among other matters:
- whether the person, any of its key personnel or its key personnel, has been charged or convicted of an offence of the kind specified in subsection 4-25(a) of the Rules;
- whether the person is (if at all) carrying on a business that involves providing registrable services;
- the registered persons operational capability necessary to comply with the obligations imposed on the person by the AML/CTF regime; and
- whether the person and the person's key personnel continue to have experience that is appropriate in functions relevant to the person's obligations under the AML/CTF regime or functions relevant to providing registrable services.

188. Similar to one of the matters specified in subsection 4-17(a) pertaining to suspension, the AUSTRAC CEO can have regard to whether "any associate of the person or its key personnel", has been charged or convicted of an offence of the kind specified in paragraphs 4-25(a)(i) to (vi) in deciding whether it is appropriate to cancel a person's registration under Part 6 or Part 6A of the Act.

189. Subsection 4-25(d) allows the AUSTRAC CEO to have regard to whether the person carries on a business that involves providing a registrable service and to cancel a person's registration if the AUSTRAC CEO is satisfied it is appropriate to do so. This

subsection allows the AUSTRAC CEO to cancel a person's registration if the registered person does not carry on a business that involves providing registrable services. Registration with AUSTRAC provides legitimacy to businesses, and inactive businesses are vulnerable to being bought and run by criminals who wish to avoid the scrutiny involved with applying for registration. If a person is registered with AUSTRAC but does not carry on a business that involves providing registrable services, subsection 4-25(d) allows the AUSTRAC CEO to cancel that person's registration.

190. These matters align with the matters the AUSTRAC CEO must have regard to when considering a registration application, or suspension of registration.

191. Part 17A of the Act sets out a number of requirements designed to afford procedural fairness to a person affected by an adverse cancellation decision. In substance, that is shown in the notice requirements in the Act (such as sections 75Q and 76S). These provisions require the AUSTRAC CEO, before making a reviewable decision under the Act in relation to one or more persons, must give a written notice to each of the persons containing:
    - the terms of the proposed decision; and
    - if the proposed decision is to cancel a registration—the date on which the cancellation is proposed to take effect; and
    - the reasons for the proposed decision; and
    - a statement that the person may, within 28 days of the giving of the notice, make a submission in relation to the decision.

192. The AUSTRAC CEO's obligation to consider these expanded matters when considering whether it is appropriate to cancel a person's registration aligns with AUSTRAC's intention to implement a more robust registration lifecycle of a person to prevent criminals and their associates from infiltrating, continuing their business in, and exploiting the remittance and VASP sectors.

4-26—Publication of cancellation information

193. Subsections 75G(3) and 76J(4) of the Act enables the AUSTRAC to publish a list of the names of persons whose registration on the RSR and VASP have been cancelled and the date the cancellation takes effect.

194. The effect of section 4-26 of the Rules is that publication of the list of names and dates may be on the AUSTRAC website, or on the Remittance Sector Register or the Virtual Asset Service Provider Register (as relevant), or on both AUSTRAC's website and the relevant Register.

195. Publication of details of cancellation decisions by the AUSTRAC CEO will inform reporting entities, foreign remittance service providers, and VASPs and other persons

regulated for AML/CTF, when assessing the ML/TF risk associated with entering into commercial relationships with another entity.

Division 6—Renewal of registration

196. Subsections 75J(1) and 76L(1) of the Act specify that the Rules may make provision for, and in relation to, the renewal of registrations for RSPs and VASPs, respectively. Paragraphs 75F(1)(c) and 76H(1)(c) of the Act prescribe that, by default, RSP and VASP registrations are for a period of 3 years, unless the registrations cease for another reason, for example, if the registration has been suspended or cancelled.

197. The renewal of registration process provides a regular re-assessment by the AUSTRAC CEO of a RSP or VASPs suitability to maintain registration. Division 6 of Part 4 of the Rules simplify the requirements for the renewal of registration whilst preserving the overarching principles in Chapters 70 and 76 of the AML/CTF Rules 2007. Persons currently registered will need to meet the new renewal of registration standards as prescribed in Part 4, Division 6 of the Rules when having a renewal application decided by the AUSTRAC CEO.

4-27—Purpose of this Division

198. Section 4-27 provides the purpose of Part 4, Division 6 of the Rules, which is to prescribe requirements relating to the renewal of registration for the purpose of section 75J and 76L of the Act.

4-28 to 4-33

199. These sections set out:
- the application process for the renewal of a person's registration (section 4-28);
- the period within which a renewal of application may be made (section 4-29);
- the matters which the AUSTRAC CEO must have regard to when deciding to renew the registration of a person, being the same matters to be considered as a decision to register a person upon initial application (section 4-30);
- the period for which renewed registrations have effect, being 3 years (section 4-31);
- a decision to not renew a person's registration by the AUSTRAC CEO is a reviewable decision, enlivening the reviewable decision framework under Part 17A of the Act (section 4-32); and
- the continuation of a person's registration pending a decision by the AUSTRAC CEO on the renewal of that person's renewal application (section 4-33).

Division 7—Matters registered persons required to advise

200. Paragraphs 75M(1)(d) to (e) and 76P(1)(a) to (b) of the Act require that a person who is registered as a RSP or VASP to advise the AUSTRAC CEO, within 14 days of:

- any change in circumstances that could materially affect the person's registration; and
- any matters specified in the Rules.

201. However, subsection 75M(2) of the Act requires that a registered remittance affiliate that did not apply for registration itself, must advise the RNP of any changes in circumstances that could materially affect the person's registration and specified matters. Subsection 75M(3) of the Act requires the RNP to advise the AUSTRAC CEO of any changes notified to it by its remittance affiliates.

4-34—Matters registered persons required to advise

202. Section 4-34 specifies the matters that the person must advise the AUSTRAC CEO of within 14 days of the change occurring. These matters are in addition to any change in circumstance that could materially affect the person's registration.

203. The matters specified at subsection 4-34(2) reflect information required in initial registration applications which either:
    - have the capacity to affect the ML/TF or other serious risk registration of the person presents,
    - have the capacity to affect whether the person continues to have the operational capacity to comply with the Act, the regulations and Rules, or
    - is required for effective ongoing supervision of the person.

Division 8—Other matters

4-35—Spent convictions

204. Section 4-35 preserves the primacy of the Commonwealth Spent Convictions Scheme in Part VIIC of the Crimes Act 1914. The provisions of Part 4 of the Rules do not override the Commonwealth Spent Convictions Scheme.

205. Under the Commonwealth Spent Convictions Scheme, a 'spent conviction' is a Commonwealth, territory, state or foreign conviction that satisfies all of the following:
    - there was no imprisonment for the conviction, or imprisonment for the conviction did not exceed 30 months;
    - it has been 10 years since the conviction, or 5 years if the individual were convicted as a child;
    - the individual did not reoffend during those 10 years, or 5 years for juvenile offenders;
    - there is no statutory or prescribed exclusion that applies.

206. The scheme also protects convictions when the individual has been granted a pardon because they were wrongly convicted, or the conviction has been quashed.

207. The Scheme generally gives a person the right to not tell another individual or authority about spent, pardoned or quashed convictions, whether it's a federal, state or territory, or foreign offence. This is called a 'right to non-disclosure'. It includes the right to claim on oath that the person was not charged with or convicted of the offence. Where a person's conviction is spent, they do not have to disclose it to anyone, including an employer or AUSTRAC unless an exception applies. Part 4 of the Rules does not constitute such an exception.

Part 5—AML/CTF programs

Division 1—ML/TF risk assessment

5-1—Review of ML/TF risk assessment

208. Section 26D of the Act sets out an obligation for a reporting entity to review its ML/TF risk assessment in certain circumstances to ensure that the reporting entity has identified and assessed any new or changed ML/TF risks. Additionally, the Act sets out triggers for when a reporting entity must review and update its ML/TF risk assessment and allows the Rules to provide further detail on other kinds of circumstances that trigger reviews of ML/TF risk assessments.

209. The Act is largely self-contained in relation to ML/TF risk assessments. Section 5-1 of the Rules does, however, set out an additional trigger for the review of a reporting entity's ML/TF risk assessment where there are adverse findings in an independent evaluation report in relation to the ML/TF risk assessment. An example of where an independent evaluation report will contain adverse findings in relation to its ML/TF risk assessment is where the report indicates that a reporting entity has not, or may not have, appropriately identified or assessed the ML/TF risks it reasonably faces in providing designated services. Additionally, if the report determines that a reporting entity has failed to have regard to the matters prescribed under subsection 26C(3) of the Act when undertaking its ML/TF risk assessment, this would be another example of an adverse finding.

210. The provision also specifies that the review of the ML/TF risk assessment must be undertaken as soon as practicable after receiving the independent evaluation report. What constitutes as soon as practicable will vary across each reporting entity, but it does imply that the review should be conducted promptly and without unreasonable delay, allowing for considerations of a reporting entity's nature, size, and complexity.

Division 2—AML/CTF policies related to ML/TF risk mitigation

5-2—Carrying out customer due diligence

211. Paragraph 26F(3)(b) of the Act requires that a reporting entity's AML/CTF policies must deal with carrying out CDD obligations in accordance with Part 2 of the Act.

212. Section 5-2 of the Rules prescribes that the AML/CTF policies made pursuant to paragraph 26F(3)(b) of the Act must set out the circumstances in which the reporting entity will, as a part of undertaking initial and ongoing CDD, collect and/or verify additional KYC information relating to the customer, including the circumstances the reporting entity will collect and/or verify information on the customer's source of wealth or source of funds. Circumstances identified under this section deal with both where enhanced CDD is required under Division 4 of Part 6 of the Rules, and circumstances where additional KYC information (including information related to source of funds and source of wealth) where enhanced CDD does not apply. This requirement links back to the outcomes-based requirement at subsections 26F(1), 28(1) and 30(1) of the Act, that reporting entities must appropriately manage and mitigate the risks of money laundering, financing of terrorism and proliferation financing that the reporting entity may reasonably face in providing its designated services.

213. The requirements in section 5-2 will, in practice, require reporting entities to forecast the triggers for obtaining a greater volume of KYC information where this is required to appropriately mitigate and manage ML/TF risk. This may appear in AML/CTF policies with requirements such as:
    - Collecting information on source of funds or source of wealth where any customer places a bet over a predetermined limit
    - The customer is a former PEP and continues to retain material influence over public policy, expenditure decisions etc. arising from their former status.
    - Identifying the beneficial owner of the corporate beneficiaries where the customer has atypical transaction patterns that may indicate ML/TF activity
    - Obtaining more detailed information on the nature of the customer's business, if there are frequent changes in directors of the company
    - Making enquiries about the purpose of international value transfers to countries with high rates of producing child exploitation material.

5-3 —Policies relating to targeted financial sanctions

214. Section 5-3 of the Rules requires reporting entities to develop and maintain AML/CTF policies which deal with ensuring that they do not contravene targeted financial sanctions, including asset freezing obligations, required by the *Autonomous Sanctions Act 2011* or the *Charter of the United Nations Act 1945*, in the provision of their designated services. This section complements the requirement in the Act to establish whether a customer, any beneficial owner of a customer, any beneficiary or any agent is a person designated for targeted financial sanctions (information on targeted financial sanctions is accessible at: https://www.dfat.gov.au/international-relations/security/sanctions/consolidated-list).

215. A reporting entity's AML/CTF policies relating to targeted financial sanctions will enable it to respond appropriately if a customer is designated for targeted financial sanctions or is associated with a person designated for targeted financial sanctions.

They will also enable a reporting entity to avoid dealings with third parties that are designated for targeted financial sanctions when providing designated services. Such policies would ordinarily include appropriate mechanisms (such as screening) for determining when a customer, associated person or third party the customer is dealing with is subject to targeted financial sanctions; appropriate governance for resolving possible matches with persons or entities on the DFAT Consolidated List; the mechanisms and governance arrangements to ensure that assets remain frozen where required. This will, among other things, assist reporting entities from inadvertently dealing with frozen assets, or returning frozen assets to a designated person in the mistaken belief that this will reduce risk.

5-4—Reviewing and updating AML/CTF policies following independent evaluation

216. Section 5-4 requires that a reporting entity's AML/CTF policies must deal with reviewing and updating the AML/CTF policies in response to an independent evaluation report that contains adverse findings in relation to the AML/CTF policies.

217. The purpose of this section is to ensure that a reporting entity's AML/CTF policies deal with how a reporting entity responds where it receives an adverse independent evaluation finding for the purposes of remedying those adverse findings. The Rules do not prescribe how a reporting entity must remedy any adverse findings but require a reporting entity to determine how it will respond in the event of such adverse findings. Responding to an adverse finding does not necessarily mean that a reporting entity has to agree and act on it if it reasonably determines that it does not accept finding of the independent evaluator. Similarly, a reporting entity does not necessarily need to address a shortcoming in its AML/CTF policies in the manner an independent evaluator may recommend, so long as the reporting entity appropriately mitigates and manages the ML/TF risk it reasonably faces in providing designated services.

5-5—Actions requiring approval or that senior manager be informed

218. Section 5-5 deals with the requirement for reporting entities' AML/CTF policies to deal with decisions about accepting or continuing to provide designated services in higher ML/TF risk circumstances.

219. Subsection 5-5(1) of the Rules requires that a reporting entity's AML/CTF policies must deal with circumstances where a senior manager must give approval before:
    - commencing to provide a designated services (or continuing to provide designated services, for an existing customer) where the customer, any beneficial owner of the customer or any person on whose behalf the customer is receiving the service is:
        - a foreign politically exposed person
        - a domestic politically exposed person or an international organisation politically exposed person and the ML/TF risk of the customer is high

- commencing to provide a designated service as part of a nested service relationship (see section 6-25), and
- entering into an agreement or arrangement for reliance on another reporting entity for collection and verification of KYC information under section 37A of the Act.

220. Subsection 5-5(2) deals with circumstances where a reporting entity is providing designated services at or through a permanent establishment in a foreign country. Senior manager approval under subsection 5-5(1) is not required if the foreign country the designated service is provided within is the same foreign country the person's foreign politically exposed person status arises from, and the customer is not high risk. For example, a reporting entity providing designated services through a branch in Singapore would not need to seek senior manager approval in relation to the head of the Singapore Ministry of Health, unless that customer was identified or assessed as high ML/TF risk.

221. Subsection 5-5(3) deals with AML/CTF policies of a reporting entity ensuring that a senior manager will be informed prior to commencing to provide a designated service covered by item 39 of table 1 in section 6 (in the capacity of insurer for a life policy or sinking fund policy, making a payment to a person under the policy) and the ML/TF risk of the customer is high. This implements FATF recommendation 12.

222. Subsection 5-5(4) requires reporting entities to develop and maintain AML/CTF policies which deal with circumstances in which approval is required relating to commencing to provide a designated service to a customer or whether the reporting entity should continue a business relationship with a customer, and determine who is authorised to give approvals under which circumstances. This section represents a flexible approach to governance and oversight of higher ML/TF risk customers, giving reporting entities discretion about what factors will require escalation through a reporting entity's AML/CTF compliance function or management hierarchy.

223. Subsection 5-5(5) of the Rules specifies that a reporting entity's AML/CTF policies must deal with circumstances in which the approval of a senior manager of the reporting entity is required if the customer, any beneficial owner of the customer or any person on whose behalf of the customer is receiving a designated service was previously a PEP. This includes circumstances where a reporting entity commences a business relationship of occasional transaction with a customer who previously met the definition of PEP, but who no longer does. This is a non-prescriptive requirement which allows reporting entities to determine how to manage and mitigate ML/TF risks associated with PEPs in a risk-sensitive and practical way, particularly where a former PEP continues to retain material influence over public policy, expenditure decisions etc. arising from their former status. Reporting entities AML/CTF polices developed for the purpose of subsection 5-5(5) may have regard to factors such as the time that has elapsed since the person was a PEP, whether the person is still prominent and politically connected, and other publicly available information.

Division 3—AML/CTF policies related to governance and compliance management

5-6—Provision of information to governing body

224. The Act introduces the concept of the governing body of a reporting entity as the body responsible for strategic oversight of specified aspects of a reporting entity's AML/CTF obligations. If the governing body, being an individual or group of individuals with primary responsibility for the governance and executive decisions of the reporting entity, fails to carry out its obligations, the reporting entity contravenes a civil penalty requirement under subsection 26H(2) of the Act.

225. Paragraph 26H(1)(b) requires that a governing body must take reasonable steps to ensure that:
    - the reporting entity is appropriately identifying and mitigating risks of ML/TF and proliferation financing that the reporting entity may reasonably face in providing its designated services; and
    - the reporting entity is complying with its AML/CTF policies.

226. Section 5-6 supports the governing body's responsibilities under the Act by specifying that a reporting entity's AML/CTF policies must deal with the provision of information to the governing body. This requirement endeavours to ensure that there is an adequate flow of information between the AML/CTF functions and those responsible for providing designated services in a reporting entity and its governing body so it can exercise appropriate, ongoing oversight to fulfil its responsibilities under the Act.

5-7—Reporting from AML/CTF compliance officer to governing body

227. The reforms to the Act reinforce the importance of the role of the AML/CTF compliance officer in a reporting entity's ML/TF risk mitigation and management. Section 5-7 requires that a reporting entity's AML/CTF policies must ensure regular reporting by the AML/CTF compliance officer to the governing body about:
    - the reporting entity's compliance with AML/CTF policies;
    - the extent to which the reporting entity's policies are appropriately managing and mitigating the risks of ML/TF and proliferation financing that the reporting entity may reasonably face in providing its designated services; and
    - the reporting entity's compliance with the Act, regulations and AML/CTF Rules.

228. 'Regular' is not defined. The frequency of reporting must be determined by the reporting entity and documented in its AML/CTF policies. The regularity of reporting must be sufficiently frequent to ensure that the governing body can, among other things, satisfy its obligations under the AML/CTF regime. Like all AML/CTF policies, 'regularity' must be appropriate to the nature, size and complexity of the reporting entity. Section 5-7 nonetheless requires that such reporting occur with a frequency of at least once every 12 months.

229. The Act contemplates that the distinction between a governing body, senior manager and AML/CTF compliance officer may be redundant for a sole trader or other micro-business, Accordingly, subsection 5-7(3) exempts a reporting entity from section 5-4 where it would otherwise involve a person reporting to himself or herself, i.e.:
    - the reporting entity is an individual; or
    - the AML/CTF compliance officer of the reporting entity is the same individual who is the governing body of the reporting entity.

230. Sections 5-6 and 5-7 are also intended to reinforce the important roles of the governing body and the AML/CTF compliance officer in ensuring the effectiveness of a reporting entity's AML/CTF program. Section 5-7 seeks to ensure a direct line of communication between the AML/CTF compliance officer and the governing body.

5-8—Undertaking personnel due diligence

231. Paragraph 26F(4)(d) of the Act and section 5-8 of the Rules replace what was formerly known as 'employee due diligence' with the concept of 'personnel due diligence'. For the purposes of the personnel due diligence requirement in paragraph 26F(4)(d) of the Act, the pertinent functions or roles of persons relate to those that are:
    - relevant persons who perform, or will perform, functions relevant to the reporting entity's obligations under the Act, Rules or Regulations; or
    - otherwise, capable of contributing to the:
        - identification or mitigation of the risks of ML/TF and proliferation financing of the reporting entity, or
        - prevention or detection of money laundering, terrorist financing and proliferation financing.

232. These relevant roles and functions of persons who are employed or otherwise engaged by the reporting entity are engaged in AML/CTF duties may pose ML/TF risk. Section 5-8 of the Rules requires the reporting entity to have AML/CTF policies in place to assess and to determine a person's suitability for a role. The provision specifies that a reporting entity's AML/CTF policies must deal with how the reporting entity will be required to undertake personnel due diligence and assess suitability, before employing or engaging a person, and on an ongoing basis. The reporting entity must assess:
    - the person's skills, knowledge and expertise relevant to the responsibilities of the person under the AML/CTF policies; and
    - the person's integrity.

233. The purpose of personnel due diligence is to mitigate the risk of engaging persons who could be involved in money laundering or other financial crimes, e.g. by inappropriately using sensitive information (such as information included in SMRs) or by circumventing AML/CTF policies. By conducting appropriate due diligence, reporting entities can ensure the integrity of their workforce and reduce the likelihood of internal fraud or complicity in illicit activities. Personnel due diligence processes

help identify individuals with a history of financial crimes, criminal activity, or association with known money launderers. Ongoing personnel due diligence is important to ensure the reporting entity can continuously identify personnel who might be involved in money laundering or other illicit activities, allowing for early intervention and prevention.

234. If a person were appointed to a role without adequate skills, knowledge of expertise, the reporting entity's ability to manage and mitigate risk will be impeded—for example, if a developer of an automated transaction monitoring program did not have sufficient programming skills, knowledge and expertise, the reporting entity could not be confident that programs developed would appropriately detect customer behaviour and transactions as required by the entity's AML/CTF Program.

235. If a person were appointed to a role relevant to performing AML/CTF functions without the reporting entity making any enquiries into the integrity of the person, it may not discover information which indicates the person is vulnerable to exploitation in their role by criminals, or vulnerable to other insider threats. Again, without this knowledge the reporting entity would not be able to effectively manage the ML/TF risk as it would not know whether to place additional controls around the person's role and responsibilities, or otherwise.

236. Personnel due diligence is to be appropriate to the size, nature and complexity of the reporting entity. Personnel due diligence should also be appropriate to the ML/TF risks posed by the role of the person. Where the subject of the due diligence operates in, or proposes to operate in roles more directly relevant to the ML/TF risk that the reporting entity faces, the due diligence should be more rigorous than persons in other roles.

237. Undertaking personnel due diligence may include:

- a national police certificate to identify whether prospective or current employees have any relevant criminal convictions
- employment or character references
- for positions that require technical qualifications and/or practising certificates, such as a lawyer or an accountant, confirming the person is a member of the relevant professional association and is not, and has not been subject to disciplinary action.

238. Where persons employed or otherwise engaged by a reporting entity are already subject to personnel due diligence by virtue of the profession in which the reporting entity operates, such protocols may be used to supplement AML/CTF personnel due diligence checks where the protocols are relevant and they are adequately documented in the reporting entity's AML/CTF policies. However, the type of due diligence required must be relevant to the person's skills, knowledge and expertise relevant to the particular responsibilities of the person under the AML/CTF policies of the reporting entity.

5-9—Providing personnel training

239. Paragraph 26F(4)(e) of the Act requires that a reporting entity's AML/CTF policies must deal with providing AML/CTF related training to persons employed or otherwise engaged by the reporting entity.

240. Section 5-9 supplements paragraph 26F(4)(e) of the Act to the provide further detail on what training under that paragraph requires:
- the training must be provided both to a person upon initial engagement, and on an ongoing basis while the person is engaged;
- the training to be appropriate to the person's functions, their ML/TF risk exposure and responsibilities under the reporting entity's AML/CTF policies; and
- be readily understandable by the person.

241. For training to be readily understandable, it must be designed and delivered in a way that is easily understood by the person, considering their role within the reporting entity as well as their literacy levels and language barriers (if any). The training must be informative and relevant to the roles and responsibilities of the person. A reporting entity's AML/CTF policies in relation to the provision of personnel training must be appropriate to the nature, size, and complexity of the entity.

242. A reporting entity must ensure that training is provided to, and obtained by, a reporting entity's employees or persons otherwise engaged by the reporting entity who perform, or will perform, AML/CTF functions. Provision of training includes the personnel receiving the training. If personnel fail to receive, or refuse to take part in training a reporting entity would need to implement measures to ensure these persons receive necessary training to ensure the reporting entity's compliance with its AML/CTF obligations or prevent the personnel from performing duties that require such training. Records of the training provided by the reporting entity to its relevant personal or persons engaged by the entity are required by section 116 of the Act and assist the reporting entity in demonstrating its compliance with its obligations under the AML/CTF regime.

5-10—Independent evaluations

243. Section 26F(4)(f) of the Act requires that a reporting entity's AML/CTF policies must deal with the conduct of independent evaluations of its AML/CTF program, including the frequency of such evaluation which must be appropriate to the nature, size and complexity of the reporting entity's business; and be at least once every three years.

244. Section 5-10 of the Rules specifies that a reporting entity's AML/CTF policies must require a number of steps to be taken by it as part of its independent evaluations. These requirements align with FATF recommendation 18 that requires for an independent audit function to test the system.

245. This section supplements the requirements in paragraph 26F(4)(f) of the Act and prescribes what the AML/CTF policies of a reporting entity must deal with, including outlining the requirements that form part of the conduct of an independent evaluation, and dealing with how the reporting entity will respond to an independent evaluation report. It is intended that paragraphs 5-10(2)(a) and (b) of the Rules ensure that an independent evaluation considers and identifies whether there is any inadequacy or omission in the design of the ML/TF risk assessment and/ or AML/CTF policies.

246. Additionally, and as part of the independent evaluation, the evaluator must test and evaluate the compliance of the reporting entity with the reporting entity's AML/CTF policies (paragraph 5-10(2)(c)). This is to ensure that an independent evaluation identifies instances where an aspect of the reporting entity's AML/CTF policies are not implemented as designed.

247. Under paragraph 5-10(2)(d), the AML/CTF policies for independent evaluation must also deal with testing and evaluating whether the reporting entity is appropriately identifying, assessing, managing and mitigating the ML/TF risk that it reasonably faces in providing designated services. This requirement is intended to ensure that an independent evaluator considers not only the compliance of the reporting entity with its AML/CTF program, but whether that program is effectively achieving the required outcome of ML/TF risk mitigation and management in practice.

248. Paragraphs 5-10(2)(a) to (c) and (e) are based on concepts that have been drawn from Auditing and Assurance Standards Board's Standard on Assurance Engagements Assurance Engagements on Controls (ASAE3150, available at: https://standards.auasb.gov.au/asae-3150-sep-2022), regarding the design and operational effectiveness of the reporting entity's AML/CTF policies.

249. Paragraph 5-10(2)(f) requires that the governing body of the reporting entity, and any senior manager who is responsible for approving the reporting entity's AML/CTF risk assessment and AML/CTF policies (including any updates to either) under section 26P of the Act, are to receive the report described in paragraph 5-10(2)(d).

250. Paragraph 5-10(3) is provided to require that the reporting entity must document their approach to responding to the independent evaluation report.

251. The word 'test' in paragraphs 5-10(2)(c) and (d) reflects FATF recommendation 18.

5-11—Fulfilling reporting obligations

252. Section 5-11 of the Rules requires that a reporting entity's AML/CTF policies must deal with ensuring that the information reporting by the reporting entity under sections 41, 43, 46 and 46A are complete, accurate and free from unauthorised change. The Act already contains obligations for a reporting entity to submit to AUSTRAC the following reports in an "approved form", and which contain information specified in the Rules:

- SMRs (obligation in section 41 of the Act);
- TTRs (obligation in section 43 of the Act); and
- IVTS reports (obligations section 46 and 46A of the Act).

253. Reports submitted to AUSTRAC that are complete, accurate and free from unauthorised change are crucial for detecting suspicious activity that may involve money laundering, the financing of terrorism or proliferation financing. Inaccurate or incomplete information can hinder the ability of AUSTRAC and law enforcement agencies to identify and further investigate or analyse suspicious transactions or behaviours effectively and efficiently. The method by which a reporting entity ensures the quality and accuracy of the reports will be determinative upon its business.

254. AML/CTF policies developed for the purpose of section 5-11 may include procedures that reporting entity personnel follow to locate and extract all relevant information known for the reporting entity, for inclusion in the relevant report.

255. Well developed AML/CTF policies dealing with fulfilling reporting obligations will assist reporting entities' to mitigate the risk of contravening sections 136 and 137 of the Act which create offences for giving information or documents to the AUSTRAC CEO, a reporting entity, or a person acting on a reporting entity's behalf, in accordance with the Act, knowing that the information or document is false or misleading, or omits any matter or thing without which the information is misleading.

5-12—Assessment of potential suspicious matters

256. Section 5-12 of the Rules requires that a reporting entity's AML/CTF policies must deal with timely review and determination of potential suspicious matters.

257. SMRs are required to be submitted within 24 hours if the suspicion relates to terrorism financing and, in most cases, within 3 business days if the suspicion relates to money laundering or any other offence. However, these timelines commence when the reporting entity 'suspects on reasonable grounds' one of the matters set out in section 41 of the Act. Delays in determining whether the reporting entity 'suspects on reasonable grounds', including delaying until enhanced CDD has been carried out, have lessened the utility of SMRs to AUSTRAC and partner agencies in detecting and disrupting criminal activity. Section 5-12 will require AML/CTF policies to ensure such determination as soon as practicable and that processes for making such a determination are clear and known (by being dealt with in AML/CTF policies).

5-13—Prevention of tipping off

258. Section 123 of the Act contains the offence of 'tipping off' which prohibits the disclosure of SMR information or section 49 and 49B of the Act information and information about suspect transaction reports under the now repealed Financial

Transaction Reports Act 1988 where it would or could reasonably be expected to prejudice an investigation.

259. Section 5-13 of the Rules supports the operation of the tipping off offence in the Act by requiring a reporting entity to deal with, in its AML/CTF policies, establishing safeguards to prevent any contravention of the tipping off offence. This includes implementing AML/CTF policies that deal with ensuring the confidentiality and appropriate use of information used or disclosed by the reporting entity's personnel. Paragraph 26F(1)(b) of the Act requires a reporting entity's AML/CTF policies to ensure it complies with the obligations imposed on it by the Act, regulations and AML/CTF Rules.

260. The requirement in section 5-13 of the Rules does not inhibit information sharing but rather seeks to ensure that where information is shared, it is shared appropriately with adequate safeguards in place to prevent any contravention of the tipping off offence. The safeguards a reporting entity has in place to prevent tipping off should be appropriate to its business and its risk of tipping off.

261. Safeguards implemented in AML/CTF policies under this section may include:
    - measures to ensure information is kept confidential by employees and any third parties engaged by the reporting entity
    - measures to keep information secure, for example through secure electronic document storage
    - measures to restrict access to information to those with a genuine need to know, and implement and review audit trails
    - measures to review, periodically and in response to relevant events, who has accessed the information
    - measures to reduce the risk of tipping off when engaging with customers
    - personnel training to enable them to understand the tipping off offence.

262. In addition to information handling requirements under the Act, reporting entities also have obligations under section 6E of the Privacy Act (including the requirement to comply with the Australian Privacy Principles, even if they would otherwise be exempt from the Privacy Act.) in relation to the activities carried on by the reporting entity for the purposes of, or in connection with, activities relating to the Act and Rules.

Division 4—AML/CTF compliance officers

5-14—AML/CTF compliance officer requirements—matters to have regard to in determine whether a fit and proper person

263. Section 5-14 of the Rules outlines a number of matters which a reporting entity must consider in conducting fit and proper assessments of an AML/CTF compliance officer of the reporting entity. Such matters include (but are not limited to):

- the necessary competency, skills, knowledge, diligence, expertise and soundness of judgement to properly fulfil the particular functions the AML/CTF compliance officer is responsible for under section 26L of the Act, and any other functions assigned to the AML/CTF compliance officer under the reporting entity's AML/CTF policies. Such attributes are essential to the AML/CTF compliance officer being effective in their role in the reporting entity, including the ability to make relevant compliance decisions for the reporting entity, know when to seek advice, and know how to implement advice received. Paragraph 5-14(1)(a) recognises that the necessary competency, skills, knowledge, diligence, expertise and soundness of judgement of an AML/CTF compliance officer is to be appropriate and proportionate to the size, nature and complexity of the reporting entity, acknowledging that a different skillset is required for AML/CTF compliance officers of a multinational gambling business to a bullion dealer with one store.
- the individual's character, honesty and integrity. This may be assessed having regard to other relevant fit and proper regimes.
- whether the individual has been convicted of a serious offence, as defined in the Act.
- whether the individual has been the subject of civil or criminal proceedings; or subject to regulatory or disciplinary processes which reflected adversely on the person's competence, diligence, judgement, honesty or integrity.
- whether the individual currently has the required financial soundness, i.e. they are not bankrupt or subject to a person insolvency agreement, to avoid any actual or apparent conflicts of interest that may prevent them from appropriately fulfilling the function of the AML/CTF compliance officer. Paragraph 5-14(1)(f) refers to a personal insolvency agreement executed under Pt X of the *Bankruptcy Act 1966*. The incorporation by reference to that provision is permitted by paragraph 14(1)(a) of the *Legislation Act 2003*.
- whether the individual has a conflict of interest that will create a material risk that the individual will fail to properly perform the duties of the AML/CTF compliance officer for the reporting entity.

264. The matters at paragraphs 5-14(b) to (f) are attributes essential to the proper fulfilment of AML/CTF compliance officer functions, as the AML/CTF compliance officer is in a unique position to lessen the effectiveness of a reporting entity's AML/CTF program if they have a lack of willingness to comply with legal obligations or lack the required character, honesty or integrity. This list is, however, not a checklist of mandatory eligibility criteria or disqualifications—the list sets out things that must be considered as part of an overarching determination about whether a person is fit and proper to be an AML/CTF compliance officer. A person may, for example, have had a historic conviction for a serious offence but in light of the elapsed time and a person's subsequent life history they could still reasonably be fit and proper to be an AML/CTF compliance officer.

265. Subsection 5-14(2) confirms that paragraph 5-14(1)(c) does not affect the operation of the Commonwealth Spent Convictions Scheme under Part VIIC of the *Crimes Act 1914*. Implications for reporting entities and individuals with past criminal convictions are discussed above in relation to section 4-35 of the Rules.

Division 5—AML/CTF program documentation

5-15—Time period for AML/CTF program documentation

266. Section 5-15 of the Rules specifies the period within which a reporting entity must document its ML/TF risk assessment, the AML/CTF policies developed by the reporting entity under section 26F of the Act, and any updates to both the ML/TF risk assessment and AML/CTF policies of the reporting entity.

267. The time period in section 5-15 relates solely to the formal reducing of the AML/CTF program and any updates to writing or other documentary form. Section 5-15 of the Rules does *not* relate to:
- The time in which it takes a reporting entity to assess the impacts of a trigger for a review or update of an AML/CTF program. In this case the time period would commence once any updates have been approved by the appropriate senior manager.
- The implementation of the update or the scope of the updates required to the ML/TF risk assessment and/ or AML/CTF policies of the reporting entity.

268. In cases where the required senior manager approval is given or recorded in writing in a document containing the update being approved, then section 5-15 is inherently met. However, if a change is made to an AML/CTF policy with the verbal approval of the senior manager (e.g. due to urgency) and the new AML/CTF policy is implemented in practice, then the clock starts ticking to document the new AML/CTF policy. Separately, a record of the senior manager approval must be made and kept under subsection 116(1) of the Act.

269. Two deadlines for documenting an AML/CTF program and any updates. A reporting entity must document its ML/TF risk assessment and AML/CTF policies before the reporting entity first commences providing a designated service to a customer. Where a reporting entity updates its ML/TF risk assessment and/ or AML/CTF policies, the reporting entity must document these updates in its AML/CTF program within 14 days after the update has occurred.

270. The requirement to 'document' for the purposes of section 5-15 of the Rules has the same meaning as in the *Acts Interpretation Act 1901*:

document means any record of information, and includes:

(a) anything on which there is writing; and

(b) anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; and

(c) anything from which sounds, images or writings can be reproduced with or without the aid of anything else; and
(d) a map, plan, drawing or photograph.

271. The Rules do not prescribe the format in which updates to a reporting entity's ML/TF risk assessment and AML/CTF policies must be documented. However, whichever approach is taken, a reporting entity's updated AML/CTF program should be useable by the governing body in fulfilling its obligations under the Act, and by employees or persons otherwise engaged by the reporting entity to implement its updated AML/CTF policies effectively. Additionally, documentation of an AML/CTF program and any updates should be able to demonstrate a reporting entity's compliance with its AML/CTF obligations.

272. Separately from the deadline for documenting an AML/CTF program and any updates, subsection 26D(4) of the Act outlines the circumstances in which a reporting entity must update its ML/TF risk assessment. Paragraphs 26D(4)(a) and (b) specifies the period within which these updates must occur as a result of a trigger for an update:
- for a significant change that is within the control of the reporting entity—before the change occurs; or
- in any other case—as soon as practicable after the review is completed.

273. Section 5-1 of the Rules also specifies time periods for reviewing a reporting entity's ML/TF risk assessment following adverse findings in an independent evaluation report.

274. No time period is specified in the Act or Rules for completing the reviews or updates of AML/CTF policies—a reporting entity's AML/CTF policies must deal with reviewing and updating AML/CTF policies in response to various triggers under paragraph 26F(3)(c) of the Act and section 5-4 of the Rules. However, importantly, a reporting entity's policies at any given time must, under section 26F(1) of the Act, appropriately manage and mitigate the ML/TF risk that the reporting entity faces in providing designated services, and ensure compliance with AML/CTF obligations. Undue delays or non-compliant AML/CTF policies in relation to undertaking a review or update of AML/CTF policies would be inconsistent with this.

275. The requirement to 'document' for the purposes of section 5-15 of the Rules has the same meaning as in the *Acts Interpretation Act 1901*:

document means any record of information, and includes:
(a) anything on which there is writing; and
(b) anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; and
(c) anything from which sounds, images or writings can be reproduced with or without the aid of anything else; and
(d) a map, plan, drawing or photograph.

Division 6—AML/CTF policies related to lead entities

5-16—Record keeping by lead entity of a reporting group

276. Section 5-16 of the Rules requires the AML/CTF policies of the lead entity of the reporting group to deal with keeping up-to-date records about the membership of the reporting group (including recording any changes of membership). The requirement for the lead entity of the reporting group to keep up-to-date records about the membership of the reporting group include keeping records that are reasonably necessary to demonstrate compliance with:
    - agreeing on a member being the lead entity of the reporting group pursuant to subsections 2-1(1) to (3) of the Rules;
    - forming a reporting group by election pursuant to subsection 2-2(1) of the Rules;
    - a member of the reporting group satisfying the requirements prescribed in subsection 2-2(2) of the Rules to be a member of the reporting group; and
    - a member of the reporting group or the lead entity of a reporting group proposing to leave the reporting group pursuant to the conditions outlined in subsection 2-2(7) to (9) of the Rules

Division 7—AML/CTF policies related to transfers of value

5-17—Policies relating to the obligations of ordering institutions

277. Section 5-17 of the Rules sets out the requirements for a reporting entity who is an ordering institution (i.e. that provides a designated service covered by item 29 of table 1 in section 6 of the Act) to have AML/CTF policies in place that deal with the matters specified in subsections 5-17(2), (5) and (6) of the Rules.

278. Subsection 5-17(2) of the Rules relates to the AML/CTF policies for all transfers of value. It requires that such AML/CTF policies must deal with how the reporting entity provides information to another institution in the value transfer chain as soon as practicable after receiving the request. Subsection 5-17(3) of the Rules specifies that a reporting entity will satisfy the requirement under subsection 5-17(2) of the Rules if its AML/CTF policies require the provision of information within 3 business days. Longer periods for response, where sufficient information is included in the request, are unlikely to be 'as soon as reasonably practicable'. For the information that must be provided, see subsection 64(2) of the Act and sections 8-3 and 8-8 of the Rules.

279. Subsections 5-17(4) and (5) of the Rules relate to merchant payments, i.e. card payments to merchants initiated by beneficiary institution. Where a designated service relates to a merchant payment and the designated service is provided in Australia, these subsections require the ordering institution's AML/CTF policies must enable it to provide the ordering institution's name and the location of the relevant permanent establishment on request to the beneficiary and intermediary institutions within 3 business days. This implements the requirements under the revised FATF recommendation 16.

280. Subsection 5-17(6) of the Rules relates to virtual asset transfers. Where the designated service relates to a transfer of a virtual asset, the subsection specifies what the reporting entity's AML/CTF policies must deal with, including how the reporting entity will undertake due diligence for the purposes of subsection 66A(2) of the Act. Section 66A of the Act sets out a range of specific obligations for ordering institutions involved in the transfer of virtual assets, a number of which require reporting entities to develop and maintain AML/CTF policies to support effective implementation. These obligations are additional to those such as customer due diligence and requirements to pass on payer and the payee's full name which apply to all ordering institutions (whether transferring money, property or digital currency).

281. The ordering institution for transfers of virtual assets is required to undertake counterparty due diligence to determine whether the virtual asset wallet to which the value is being transferred is a custodial wallet controlled by an AML/CTF regulated business, a business not required to be regulated, an illegally operating business or whether it is a self-hosted wallet controlled by the payee. Counterparty due diligence is required to determine what the ordering institution's travel rule and other obligations are, for example;
    - to pass on information as required under section 64 of the Act;
    - to collect information but not pass it on, where the transfer is to a self-hosted wallet controlled by the payee; or
    - not to carry out the transfer whether the transfer is to a custodial wallet controlled by an illegally operating business, which is prohibited by subsection 66A(4) of the Act.

282. The AML/CTF policies of a reporting entity to which subsections 5-17(a) to (d) applies are required to deal with how relevant reporting entities will fulfil their obligations under Part 5 of the Act.

5-18—Policies relating to the obligations of beneficiary institutions

283. Subsection 5-18(2) of the Rules sets out the requirements for a beneficiary institution who is a reporting entity for any transfer of value (i.e. that provides a designated service covered by item 30 of table 1 in section 6 of the Act) to have AML/CTF policies in place that deal with the matters specified in paragraphs 5-18(1)(a) to (c) of the Rules in relation to the transfers of value to a payee.

284. The FATF methodology in relation to FATF recommendation 16 sets out, among other things, the following travel rule risk mitigation measures that beneficiary institutions are required to have regard to, including:
    - taking reasonable measures, which may include post-event monitoring or real time monitoring where feasible, to identify cross-border wire transfers that lack required payer or required information about the payee (paragraph 16.13 of the FATF methodology); and
    - having risk-based policies and procedures for determining:

- when to execute, reject or suspend a wire transfer lacking required payer or required information about the payee; and
- the appropriate follow-up action (paragraph 16.15 of the FATF methodology).

285. Under subsection 65(2) of the Act, beneficiary institutions are required to take reasonable steps to identify missing payer and information about the payee in a transfer of value (consistent with criterion 16.13 of the FATF methodology), and inaccurate information about the payee (consistent with criterion 16.14 and customer due diligence obligations triggered by the designated service in item 30 of table 1 in section 6 of the Act).

286. Paragraphs 5-18(2)(a) to (c) of the Rules give effect to the FATF recommendation 16 by requiring reporting entities that provide a designated service covered by item 30 of table 1 in section 6 of the Act to have in place AML/CTF policies that deal with monitoring for missing and inaccurate information about its customer, the payee. The AML/CTF policies must also deal with what a beneficiary institution will do in the event that it detects missing or inaccurate information—such policies must, under section 26F(1)(a) of the Act, appropriately manage and mitigate the ML/TF risks the beneficiary institution faces in providing this designated service.

287. A note under the subsection 5-18(2), alerts readers to subsection 66A(6) of the Act which prohibits a beneficiary institution from making available transferred virtual assets unless it has received, or otherwise obtained, the required information, subject to specific exceptions in subsection 66A(10).

288. Subsection 5-18(3) of the Rules contains specific AML/CTF policy requirements for beneficiary institutions that make available virtual assets. Where a reporting entity who is a beneficiary institution provides designated services in relation to the transfer of a virtual asset, it must have AML/CTF policies in place that deal with the matters specified in paragraphs 5-18(2)(a) to (d) of the Rules. These matters give effect to beneficiary institution obligations under section 66A of the Act as well as give effect to FATF recommendations 15 and 16.

289. Section 66A of the Act sets out a range of specific obligations for beneficiary institutions involved in the transfer of virtual assets, a number of which require reporting entities to develop and maintain AML/CTF policies to support effective implementation. Subsection 66A(5) of the Act specifies that the beneficiary institution must undertake due diligence to determine whether the virtual asset wallet to which the value is being transferred is a custodial wallet controlled by an AML/CTF regulated business, a business not required to be regulated, an illegally operating business or whether it is a self-hosted wallet controlled by the payer.

290. Subsections 5-18(4) and (5) of the Rules relates to merchant payments, i.e. card payments to merchants initiated by beneficiary institution. Where a designated service

relates to a merchant payment and the designated service is provided in Australia, these subsections require the beneficiary institution's AML/CTF policies must enable it to provide the beneficiary institution's name and the location of the relevant permanent establishment on request to the ordering and intermediary institutions within 3 business days. This implements the requirements under the revised FATF Recommendation 16.

5-19—Polices relating to the obligations of intermediary institutions

291. Section 5-19 of the Rules sets out the requirements for an intermediary institution that is a reporting entity (i.e. that provides a designated service covered by item 31 of table 1 in section 6 of the Act) in relation to the transfer of value, to have in place AML/CTF policies that deal with the matters specified in subsections 5-19(a) to (c) of the Rules.

292. The FATF methodology in relation to FATF recommendation 16 sets outs, among other things, the following travel rule risk mitigation measures that intermediary institutions are required to have regard to:
    - taking reasonable measures, which are consistent with straight-through processing, to identify cross-border wire transfers that lack required originator information or required beneficiary information (paragraph 16.11 of the FATF methodology); and
    - having risk-based policies and procedures for determining:
        - when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information, and
        - the appropriate follow-up action (paragraph 16.12 of the FATF methodology).

293. The FATF requires intermediary institutions to ensure that the required payer and information about the payee is retained with the transfer of value (i.e. monitor for missing information about the payer and payee). However, there is no requirement for an intermediary institution to monitor the accuracy of the required information about the payer and payee (due to the absence of a direct customer relationship with either the payer or payee).

294. The matters specified in paragraphs 5-19(2)(a) to (c) give effect to the above-mentioned FATF methodology by requiring the AML/CTF policies of the reporting entity to which subsection 5-19 of the Rules applies, to:
    - take reasonable steps monitor whether the reporting entity has received the information specified in section 8-5 of the Rules relating to the transfer of value;
    - determine whether to pass on a transfer message for the transfer of value in the where it detects that it has not received all of the required information; and
    - determine whether to request further information from another institution in the value transfer chain where it detects that it has not received all of the required information.

Division 8—AML/CTF policies related to real estate transactions

5-20—Policies relating to customer due diligence for real estate transactions

295. Section 5-20 of the Rules is applicable to the AML/CTF policies of a reporting entity that is:
    - proposing to provide a designated service specified under item 1 of table 5 in section 6 of the Act (brokering the sale, purchase or transfer of real estate) or item 1 of table 6 in section 6 of the Act (assisting a person in a transaction to sell, buy or otherwise transfer real estate); and
    - party to an information sharing arrangement with other reporting entities participating in a real estate transaction pursuant to paragraph 6-33(e) of the Rules.

296. This section requires that the AML/CTF policies of the reporting entity relying on this information sharing arrangement must deal with how it will verify the KYC information pursuant to paragraph 28(3)(d) of the Act if does not obtain the information necessary to meet that verification obligation by way of that information sharing arrangement. Section 5-20 accounts for circumstances where the information sharing arrangement cannot meet the needs of the relying reporting entity. For example, this may include circumstances where the other reporting entity party to the information sharing arrangement:
    - has not verified the customer in accordance with its responsibilities allocated under the arrangement pursuant to paragraph 6-33(g) of the Rules.
    - has verified the customer in accordance with its responsibilities allocated under the arrangement pursuant to paragraph 6-33(g) of the Rules, but the level of KYC information collected by the other reporting entity for the purposes of verification is not sufficient for the relying reporting entity to meet its own verification obligations on the customer pursuant to paragraph 28(3)(d) of the Act. This could arise where the ML/TF risks that each of those reporting entities reasonably face is significantly different, resulting in a different understanding of what is appropriate to the ML/TF risk of the customer in the circumstances pursuant to paragraphs 28(3)(d) and (4)(a) of the Act, and
    - has verified the customer in accordance with its responsibilities allocated under the arrangement pursuant to paragraph 6-33(g) of the Rules but does not share the KYC information or associated verification data with the relying reporting entity.

297. In such circumstances, the relying reporting entity's obligations under the Act and Rules remains unsatisfied unless it undertakes other measures to ensure that the relevant KYC information about the customer is verified pursuant to paragraph 28(3)(d) of the Act, before settlement of the real estate sale, purchase or transfer. The purpose of this section is to ensure that the relying reporting entity is prepared and can appropriately respond if such circumstances arise.

Part 6—Customer Due Diligence

Division 1—Initial customer due diligence

298. Division 1 of Part 6 of the Rules can be split into four parts:

- **The minimum KYC information to collect for different kinds of customer (sections 6-1, 6-2, 6-3 and 6-4)**
  Part 2 of the Act does not prescribe specific information that a reporting entity must consider when it is establishing the matters under subsection 28(2) of the Amended AML/CTF Act. The requirements in these sections are split by customer type and provide the *minimum KYC information* reporting entities must collect to establish a matter in subsection 28(2) of the Act.

  Depending on the kind of customer, the KYC information collected under sections 6-1 to 6-4 may not solicit enough information for a reporting entity to have reached the standard of 'establish [the matter] on reasonable grounds'. To establish a matter on 'reasonable grounds' is an objective test which is well established in the Australian legal system, and generally requires the existence of facts which are sufficient to induce that state of mind in a reasonable person.

  All customers who are not individuals are dealt with under one of these four sections. These sections specify requirements only relating to the collection of KYC information pursuant to paragraph 28(3)(c) of the Act.

  These sections do not prescribe what KYC information must be verified. Verification of KYC information is required as appropriate to the ML/TF risk of the customer, as specified in paragraph 28(3)(d) of the Act. Generally reporting entities must verify KYC information pertaining to each matter in subsection 28(2) of the Act, unless sections 6-10, or 6-16 to 6-19 of the Rules apply.

  The Rules do not specify minimum KYC information collection requirements for customers that are individuals, this maintains flexibility for reporting entities to determine what KYC information it will collect to establish the identity of individuals and whether they are subject to targeted financial sanctions or are a politically exposed person.

  Part 6 does not specify minimum KYC information collection requirements for customers who are individuals acting in a private capacity to provide flexibility for reporting entities. However, each of the matters that apply under subsection 28(2) of the Act must still be established on reasonable grounds, including by collecting KYC information about the identity of the customer and verifying it using reliable and independent data. Further, it is a criminal offence under section 139 of the Act to provide a designated service to any customer using a false name or customer anonymity. Under section 141 it is also an offence for a customer who is commonly known by two or more names to receive a designated service without disclosing those names to the reporting entity.

- **The minimum information to collect about a person that is not the customer but is associated with the customer (section 6-5)**
  This section specifies requirements to establishing the identity of persons associated with the customer (i.e. the persons related to the customer under paragraphs 28(2)(b), (c) and (d) of the Act). It does so by specifying the minimum information to collect when establishing the identity of such associated persons (section 6-5). As per sections 6-1, 6-2, 6-3 and 6-4 of the Rules, while verification is not specified in the section, it is still required and operates pursuant to paragraph 28(3)(d) of the Act.

- **Clarification as to whether the initial CDD obligation under section 28 of the Act applies (sections 6-6 and 6-11)**
  Section 6-6 of the Rules clarifies that the identity of the customer's customer is not required to be established in relation to the matters under paragraphs 28(2)(b), (c) and (d) of the Act. The matter in subsection 28(2)(b) is instead focused on beneficiaries of trusts and foreign equivalents, and beneficiaries of life policies and sinking fund policies.

- **Alternative approaches to establishing a matter under subsection 28(2) of the Act (sections 6-19, 6-7, 6-8, 6-9 and 6-10)**
  These sections specify alternative approaches to meeting the verification element under paragraph 28(3)(d) of the Act when establishing a matter under subsection 28(2) of the Act. These sections specify circumstances where verification under paragraph 28(3)(d) of the Act is not required by offering alternative approaches to establishing the relevant matter under subsection 28(2) of the Act. These sections specify requirements that must be met before the alternative approach can be utilised.

299. The following table demonstrates, using a customer that is an Australian company, how the KYC information collection requirements relate to establishing the matters in subsection 28(2) of the Act.

AML/CTF Act s 28(2) 'matter'	**AML/CTF Rules 'KYC to collect'—customer is an Australian company**
the identity of the customer	• the customer's full name; • any business names of the customer; • any other names the customer is commonly known by; • a unique identifier for the customer (if any has been given); • the address of the principal place of business or operations of the customer;

	• the address of any registered office of the customer; • evidence of the customer's existence; • information about the powers that bind and govern the customer; • the full name, and if applicable director identification number, of the individual, or each member of the group of individuals, with primary responsibility for the governance and executive decisions of the customer.
the identity of any person on whose behalf the customer is receiving the designated service;	Reporting entities are deemed to comply with this matter under section 6-6 if the Australian company is not a corporate trustee, no KYC information collection is required.
the identity of any person acting on behalf of the customer and their authority to act	KYC information per the kind of person, see sections 6-5 (note, simplified verification is available under section 6-19).
if the customer is not an individual—the identity of any beneficial owners of the customer;	KYC information about the ownership and control structure of the customer. KYC information to establish on reasonable the identity of any beneficial owners
whether the customer, any beneficial owner of the customer, any person on whose behalf the customer is receiving the designated service, or any person acting on behalf of the customer is: i.a politically exposed person; or ii.a person designated for targeted financial sanctions;	Not specified in the AML/CTF Rules—the outcomes based obligation in the Act applies
the nature and purpose of the business relationship or occasional transaction	KYC information about the nature of the customer's business or operations.

6-1—Customer is sole trader

300. Section 6-1 of the Rules sets out specific requirements for establishing the matters under paragraphs 28(2)(a)—the identity of the customer—and (f)—the nature and purpose of the business relationship or occasional transaction—of the Act where the customer is a sole trader. The requirements relate to a customer that is an individual, and receiving designated services in relation to the customer's business. This is in recognition that sole trader's businesses do not have a separate legal personality. The requirements in section 6-1 apply where an individual is obtaining designated services for their business activities, as opposed to in their personal capacity. For example, an individual may have a home loan account with an ADI which is solely in their personal

capacity, but also a transaction account with the same ADI which is used to make and receive payments relating to the individual's business.

301. Subsection 6-1(2) of the Rules requires that a reporting entity must collect no less than the specified KYC information in relation to a customer in their capacity as a sole trader for the purpose of establishing the identity of that customer pursuant to paragraph 28(2)(a) of the Act.

302. Paragraphs 6-1(2)(a) to (c) of the Rules requires that the reporting entity collect the names used by the customer.
    - Paragraph (a) requires collection of the full name of the individual.
    - Paragraph (b) requires collection of the name used by the sole trader for their business, if the sole trader uses a business name distinct from their own name.
    - Paragraph (c) requires collection of names that the customer may be known by, to reflect the offence at section 141 of the Act (that customers must disclose all names they are commonly known by to reporting entities). There may be circumstances where there are no additional names to the ones already captured under paragraphs (a) and (b).

303. Paragraph 6-1(2)(d) of the Rules requires that the reporting entity collect the unique identifier for the customer's business, generally an ABN for a sole trader operating in Australia. In some cases, a unique identifier for the business may not be available (e.g. Australian sole traders are not required to register for an ABN if turnover is below relevant thresholds). In such circumstances, the reporting entity is required to collect a unique identifier pertaining to the individual who is the sole trader, such as their passport number or driver's licence number.

304. Paragraph 6-1(2)(e) of the Rules requires that the reporting entity collect the address of the customer's principal place of business. Even if the customer is not registered as a business (e.g. for an ABN), the reporting entity must still collect the address where the sole trader runs their business.

305. Subsection 6-1(3) of the Rules specifies that, for the purposes of establishing the nature and purpose of the business relationship or occasional transaction pursuant to paragraph 28(2)(f) of the Act, a reporting entity must collect KYC information about the nature of the customer's business. The nature of a customer's business refers to the general commercial activity or sector the sole trader operates in, such as photographer, freelance copywriting, residential plumbing services, or food services. Collecting information about the nature of the customer's business should allow the reporting entity to understand at a general level the products and services the customer offers, where it operates and who its customers are. The nature of a customer's business is a separate concept from establishing the nature and purpose of the business relationship under paragraph 28(2)(f) of the Act, which focuses on the relationship between the reporting entity and the customer. Information about the nature of a customer's business is essential to establishing the nature and purpose of the business relationship

between the customer and reporting entity, and helps identify and assess the ML/TF risk of the customer. This KYC information is not required to be verified in order to establish paragraph 28(2)(f) of the Act unless the circumstances in section 6-9 of the Rules apply.

306. Section 6-1 of the Rules applies to all designated service types, and the scope of this section is confined to designated services provided in Australia. This is in recognition that, while the FATF recommendations are consistent around the world, minor variations in how countries implement the FATF recommendations can lead to technical conflicts of laws. Reporting entities providing services at or through foreign permanent establishments must still establish on reasonable grounds the matters set out in subsection 28(2) of the Act but have the flexibility to do so in other ways, including by complying with relevant foreign laws relating the CDD.

6-2—Customer is a body corporate, partnership or unincorporated association

307. Section 6-2 of the Rules sets out specific requirements for the purposes of establishing the matters under paragraphs 28(2)(a), (d) and (f) of the Act where the customer is one of the following:
    - body corporate—while it is not defined, 'body corporate' includes any incorporated body such as companies, cooperatives, and incorporated associations, incorporated partnerships and equivalents under the laws of foreign countries
    - partnerships, or
    - unincorporated associations.

308. The requirements under section 6-2 of the Rules relate to designated services provided in Australia and applies to all designated service types. The section requires that a reporting entity must collect no less than the KYC information specified in subsections 6-2(2) to (4) of the Rules.

309. The requirements under paragraphs 6-2(2)(a) to (e) and subsection (4) of the Rules are materially the same as the requirements specified in paragraphs 6-1(2)(a) to (e) and subsection (3) of the Rules in relation to customers that are sole traders, respectively. However, what the requirements refer to in the context of body corporates, partnership and unincorporated associations will be different.

310. Paragraphs 6-2(2)(a) to (c) of the Rules requires that the reporting entity collect the names used by the customer:
    - Paragraph (a) requires collection of the full name of the customer. For example, this would be:
        - the name of the company registered on the Australian Companies Register with ASIC for a company incorporated under the *Corporations Act 2001*, or the Australian Company Number if the customer hasn't chosen a name.

    - the collective names of all the partners or members of a partnership or unincorporated association (as the case may be) for a partnership or unincorporated association that has not chosen (as is available to the customer) to operate under a different business or charity name that has been registered on the Australian Business Register or the ACNC Charity Register.
- Paragraph (b) requires collection of any other business name the customer operates under. All business names a person uses to run a business in Australia must be registered on the Australian Business Register. This requirement is only triggered where the customer has more than one name, beyond what is collected under paragraph 6-2(2)(a).
- Paragraph (c) requires collection of any other names that the customer may be known by, to reflect the offence at section 141 of the Act (that customers must disclose all names they are commonly known by to reporting entities). For example, 'Australian Transactions and Reports Analysis Centre' may be collected under paragraph 6-2(2)(a) and 'AUSTRAC' under paragraph 6-2(2)(c). As with sole traders, there may be circumstances where there are no additional names to the ones already captured under paragraphs (a) and (b).

311. Paragraph 6-2(2)(d) of the Rules requires that the reporting entity collect a unique identifier for the customer's business. This will generally be an ABN or ACN for a customer operating in Australia. In some cases, a unique identifier for the business may not be available (e.g. an incorporated association in Australia that does not carry on a business).

312. Paragraphs 6-2(2)(e) and (f) of the Rules relates to the customer's addresses. The key distinction between the requirements under the two paragraphs relates to the purpose of the address:
    - Paragraph (e) requires collection of the customer's address of principal place of business or operations, being the main location from which business or operations are conducted and decisions are made. For example, this would be the head office of a customer that has multiple offices. For companies, this is the address registered with ASIC as the company's principal place of business address. This paragraph also makes the distinction between business and operations to capture circumstances where the customer does not run a business in the typical sense (such as charities or community organisations). A customer will always have an address for the purposes of this paragraph. This address may also be the same address as the registered address required under paragraph (f).
    - Paragraph (f) requires collection of the registered address of the customer, if the customer has an address distinct from its principal place of business or operations where communications and notices are sent. In some cases, this KYC information will be the same as the address of the customer's principal place of business or operations, or it may be the customer's accountant or lawyers' address.

313. Paragraph 6-2(2)(g) of the Rules specifies that a reporting entity must collect evidence of the existence of the customer. What this evidence may be differs for the legal form of the customer. For example:
    - For companies incorporated in Australia, evidence of existence may be a certificate of registration from ASIC's Business Registration Services provided by the customer, or an organisation extract from ASIC's registries.
    - For partnerships formed in Australia, evidence of existence may be the partnership agreement as partnerships are not registered in Australia. For foreign countries where partnerships are registered, a certificate of registration with the relevant regulatory body could form this evidence.
    - For incorporated associations incorporated in a State or Territory in Australia, evidence of existence may be a certificate of incorporation from the relevant regulatory body (e.g. NSW Fair Trading for those incorporated in NSW), or an organisation extract from a register of incorporated associations. If it is a charity, the certificate of registration with the Australian Charities and Not-for-profits Commission could form this evidence.
    - Similarly to partnerships, unincorporated associations are not required to be registered in Australia, so evidence of existence may be the customer's constitution.

314. Subsection 6-2(2)(h) of the Rules requires a reporting entity to collect KYC information on the powers that bind and govern the customer. Information on the powers that bind and govern refers to the contractual or legal authorities creating the legal framework that defines how the body corporate is owned and run, detailing the powers, rights and duties of office holders and equity holders. Company or association constitutions, partnership agreements, shareholders agreements, and any equivalent documents are examples of things that could give information on powers that bind and regulate. Where a customer is an Australian company, a reporting entity may obtain information that the customer uses the replaceable rules from the *Corporations Act 2001*, which would fulfil the obligation to collect information on the powers that bind and govern the customer. Information about the powers that bind and govern can also assist reporting entities to identify beneficial owners and the basis on which they are a beneficial owner, whether through ownership and/or control.

315. Paragraph 6-2(2)(i) of the Rules requires reporting entities to collect the full name of the individual, or each member of the group of individuals, with primary responsibility for the governance and executive decisions of the customer. Paragraph 6-2(2)(i) also requires collection of the director identification number (if any) of each eligible officer within the meaning of the *Corporations Act 2001*. Director identification numbers are numbers given to individuals by ASIC after ASIC verifies the director's identity. A director identification number applies for life, and does not change even if the director changes company, changes their name or moves interstate. The objective of the director identification number regime is to prevent criminal and unlawful conduct, including preventing use of false or fraudulent director identities, identify and eliminate director

involvement in unlawful activity, such as illegal phoenix activity, and help regulators and law enforcement trace directors' relationships with companies over time.

316. Subsection 6-2(3) of the Rules specifies that a reporting entity must collect KYC information on the ownership and control structure of the customer as a minimum requirement for establishing whether there are beneficial owners of the customer, and if so, the identity of those individuals. Information on the ownership and control structure refers to the arrangement and distribution of ownership rights in a body corporate, partnership or unincorporated association, and delineates how the ownership is divided among shareholders, partners or members, and it influences the control, decision-making processes and financial benefits within the entity. Understanding an ownership structure is crucial for determining the distribution of power, responsibilities, and profits. Collecting information about the ownership and control structure is essential for reporting entities to identify beneficial owners and the basis on which they are a beneficial owner, whether through ownership and/or control.

317. Subsection 6-2(4) of the Rules specifies that as part of establishing the nature and purpose of the business relationship or occasional transaction under paragraph 28(2)(f) of the Act, a reporting entity must collect KYC information about the nature of the customer's business. The nature of a customer's business refers to the general commercial activity or sector the customer operates in, such as critical minerals mining, forestry, defence industry manufacturing, commercial construction, or automotive importing importer. Collecting information about the nature of the customer's business should allow the reporting entity to understand at a general level the products and services the customer offers, where it operates and who its customers are. The nature of a customer's business is a separate concept from establishing the nature and purpose of the business relationship under paragraph 28(2)(f) of the Act, which focuses on the relationship between the reporting entity and the customer. Information about the nature of a customer's business is essential to establishing the nature and purpose of the business relationship between the customer and reporting entity, and helps identify and assess the ML/TF risk of the customer. This KYC information is not required to be verified in order to establish paragraph 28(2)(f) of the Act unless the circumstances in section 6-9 of the Rules apply.

318. The requirements in section 6-2 of the Rules are specified in relation to the matter established under subsection 28(2) of the Act. However, this does not limit a reporting entity from using that collected KYC information for establishing other matters under subsection 28(2) of the Act, if it considers it appropriate to do so. For example:

KYC information to collect under s 6-2 of the Rules	**Matter under s 28(2) of the Act that it is key to establishing**	**Matter under s 28(2) of the Act that it also contributes to establishing**

Full name: para (2)(a)	Identity of customer matter: para (2)(a)	N/A
Business name: para (2)(b)	Identity of customer matter: para (2)(a)	N/A
Other names: para (2)(c)	Identity of customer matter: para (2)(a)	N/A
Unique identifier: para (2)(d)	Identity of customer matter: para (2)(a)	N/A
Address of principal place of business/operations: para (2)(e)	Identity of customer matter: para (2)(a)	Contributes to establishing nature and purpose matter: para (2)(f)
Address of registered office: para (2)(f)	Identity of customer matter: para (2)(a)	N/A
Evidence of existence: para (2)(g)	Identity of customer matter: para (2)(a)	Contributes to establishing nature and purpose matter: para (2)(f)
Powers that bind and govern: para (2)(h)	Identity of customer matter: para (2)(a)	Strong link to establishing beneficial owner matter: para (2)(d)
Persons with primary responsibility for governance and executive decisions: para (2)(i)	Identity of customer matter: para (2)(a)	Contributes to establishing beneficial owner matter: para (2)(d)
Ownership and control structure: subsection (3)	Beneficial owner matter: para (2)(d)	Contributes to establishing beneficial owner matter: para (2)(d)
Nature of business: subsection (4)	Nature and purpose matter: para (2)(f)	Contributes to establishing identity of the customer matter: para (2)(a)

319. The requirement to collect the KYC information specified in this section aligns with FATF recommendation 10 (10.3, 10.8 and 10.9 in the FATF methodology) regarding customers that are legal persons.

6-3—Customer is a trust or foreign equivalent

320. The FATF recommendations relating to customer due diligence for trusts, particularly as they relate to beneficial ownership, are most easily understood by treating the trust estate as the customer of designated services. In the Act and these Rules, this is enabled by the designation of a trust as a 'person' in section 5 of the Act. Section 5 further provides that the definition of trust means (as the case requires) a trust estate.

321. For the purposes of customer due diligence, reporting entities are to treat the trust as the person who is the customer according to the tables in section 6 of the Act, which does not always reflect that the customer for AML/CTF purposes is the same person who enters into a contract in relation to the service underpinning the designated service. In other words, the Act and Rules do not prevent a reporting entity from entering into or maintaining a contractual relationship with the trustee of an express trust as the client or customer for other purposes.

322. Section 6-3 also extends to any equivalents of trusts recognised under foreign laws, including legal arrangements such as fiducie, treuhand and fideicomiso and waqf.

323. Subsection 6-3 of the Rules sets out minimum KYC information collection requirements for the purposes of establishing the matters under paragraphs 28(2)(a) to (c) and (f) of the Act where the customer is a trust or equivalent under foreign legal systems. The requirements in the section relate to designated services provided in Australia and applies to all designated service types.

324. The KYC information specified in subsection 6-3(2) of the Rules for the purposes of establishing paragraph 28(2)(a) of the Act are largely the same as the KYC information specified in subsection 6-3(2) of the Rules in relation to customers that are bodies corporates, partnerships or unincorporated associations.

325. Paragraphs 6-3(2)(a), (c) and (d) of the Rules relate to the names of the trust estate.
    - The customer's full name under paragraph (a) is the name of the trust, for example Smythe Family Discretionary Trust, Pyramid Unit Trust, or the Estate of Davy Jones.
    - The customer's business name under paragraph (c) requires collection of any name the trust estate uses to carry on a business.
    - Paragraph (d) requires the collection of any other names that the customer is known by. As above, there may be circumstances where the customer is not known by any names additional to the ones already captured under paragraphs (a) and (c).

326. Paragraph 6-3(2)(b) of the Rules specifies that a reporting entity must collect KYC information on the kind of trust or equivalent that the customer is, providing discretionary trust, bare trust or unit trust as non-exhaustive examples. The form of the trust or equivalent can influence the level of rights and control (if any) held over the customer by associated persons such as the trustee, beneficiaries, settlor, appointor, guardian and protector, and is therefore relevant to the reporting entity's identification and assessment of the ML/TF of the trust. Accordingly, while this KYC information is essential to establishing the identity of the customer pursuant to paragraph 28(2)(a) of the Act, it is also important to understanding the identity of the persons on whose behalf the designated service is received under paragraphs 28(2)(b) and the identity of the person acting on behalf of the customer and their authority to act under paragraph 28(2)(c) of the Act.

327. Paragraph 6-3 (2)(e) of the Rules specifies that a reporting entity must collect a unique identifier of the customer, if any has been given. Similarly to unincorporated associations, trusts may not have a unique identifier as trusts are not required to be registered with a government body upon creation in Australia, so may not have a unique identifier to provide.

328. Paragraph 6-3(2)(f) of the Rules specifies that a reporting entity must collect the address of the customer's principal place of business or operation. For the same reason as noted in relation to paragraphs 6-2(2)(e) above, this paragraph makes the distinction between business and operations to capture circumstances where the customer does not run a business. A customer will always have an address for the purposes of this paragraph.

329. Paragraph 6-3(2)(g) of the Rules specifies that a reporting entity must collect evidence of the customer's existence. Collection of the trust deed, or equivalent instrument for a fiducie, fideicomiso, waqf or treuhand, a will, or letter of administration will generally be necessary to meet this requirement. Some such legal arrangements may appear on registers maintained by government bodies, particularly those overseas, which may also go to establishing existence.

330. Subsection 6-3(2)(h) of the Rules requires a reporting entity to collect KYC information on the powers that bind and govern the customer. Information on the powers that bind and govern refers to the trust deed or legal authorities creating the legal framework that defines how the trust is governed and run, detailing the powers, rights and duties of office holders and beneficiaries. Information about the powers that bind and govern can also assist reporting entities to identify beneficial owners and the basis on which they are a beneficial owner, whether through ownership and/or control.

331. One document or data source may provide KYC information required under numerous paragraphs of this subsection. For example, a trust deed may satisfy paragraphs (a), (b), (g) and (h).

332. Subsection 6-3(3) of the Rules specifies requirements relating to the identity of associated persons associated with a trust for the purpose of establishing the identify of any person on whose behalf the customer is receiving the designated service under paragraph 28(2)(b) of the Act.
    - Paragraph (a) requires the reporting entity to collect KYC information on the identity of each beneficiary to the trust or equivalent. Where a beneficiary is not an individual, reporting entities should refer to section 6-5 regarding KYC information collection requirements.
    - Under paragraph (b) if the nature of the trust means that it is not possible to identify each beneficiary of the trust, either due to there being an extreme volume of beneficiaries or because there are not named beneficiaries, the reporting entity may instead collect a description of each class of beneficiary. For example, family trust deeds will often identify secondary beneficiaries by their relationship to a primary beneficiary, such as their spouse, children, or future descendants, and may not be individually named in the deed. In the context of charitable trusts, the class of beneficiaries is the general class of persons who will benefit from the objects of the trust.

333. Subsection 6-3(4) of the Rules specifies that a reporting entity must collect KYC information about the identity of the trustees of the trust for the purposes of establishing the identity of a person acting on behalf of the customer under section 28(2)(c) of the Act. Where a trustee is not an individual, reporting entities should refer to section 6-5 regarding KYC information collection requirements.

334. Subsection 6-3(5) of the Rules specifies requirements relating to establishing whether there are any beneficial owners of the trust, and the identify of any beneficial owners. In establishing that matter, a reporting entity must:
    - Under paragraph (a), collect at least KYC information about the ownership and control structure of the trust as a minimum requirement for establishing whether there are beneficial owners of the customer, and if so, the identity of those individuals. Information on the control structure refers to the duties, rights and entitlement in relation to administration of the trust and control, decision-making processes in relation to administering the trust. Collecting information about the control structure is essential for reporting entities to identify beneficial owners and the basis on which they are a beneficial owner, whether through ownership and/or control. This information would also assist the reporting entity to establish a trustee's authority to act pursuant to paragraph 28(2)(c) of the Act.
    - Under paragraph (b), collect at least KYC information on the identity of any settlor, appointor, guardian or protector of the trust or equivalent. The persons appointed to these positions are to be identified because they may have control over the trust, and depending on the level of control, may trigger the beneficial owner definition on the basis of the control limb. The requirement applies only if an individual has been appointed to that role.

335. Subsection 6-3(6) of the Rules specifies that, for the purposes of establishing the nature and purpose of the business relationship or occasional transaction pursuant to paragraph 28(2)(f) of the Act, a reporting entity must collect KYC information about the nature of the customer's business. The nature of a customer's business refers to the general commercial activity or sector the customer operates in, such as wealth management, legal services, remitting money, superannuation administration, self-managed super fund, hotel, or if not engaged in commercial activity, the nature of the trust's business may be that the trust is a vehicle for managing personal assets, or that the trust has a charitable purpose. Collecting information about the nature of the customer's business should allow the reporting entity to understand at a general level the products and services the customer offers, where it operates and who its customers are; or the purpose the trust exists.

336. The requirements in section 6-3 of the Rules are specified in relation to the matter that it is key to establishing under subsection 28(2) of the Act. However, this does not limit a reporting entity from using that collected KYC information for establishing other matters under subsection 28(2) of the Act, if it considers it appropriate to do so. For example:

KYC information to collect under s 6-3 of the Rules	Matter under s 28(2) of the Act that it is key to establishing	Matter under s 28(2) of the Act that it contributes to establishing
Full name: para (2)(a)	Identity of customer matter: para (2)(a)	N/A
Kind of trust or equivalent: para (2)(b)	Identity of customer matter: para (2)(a)	• Contributes to establishing trustee's authority to act: para (2)(c) • Contributes to establishing nature and purpose matter: para (2)(f)
Business name: para (2)(c)	Identity of customer matter: para (2)(a)	N/A
Other names: para (2)(d)	Identity of customer matter: para (2)(a)	N/A
Unique identifier: para (2)(e)	Identity of customer matter: para (2)(a)	N/A
Address of principal place of business/operations: para (2)(f)	Identity of customer matter: para (2)(a)	N/A
Evidence of existence: para (2)(g)	Identity of customer matter: para (2)(a)	N/A
Powers that bind and govern: para (2)(h)	Identity of customer matter: para (2)(a)	• Strong link to establishing trustee's authority to act: para (2)(c) • Strong link to establishing nature and purpose matter: para (2)(f)
Persons with primary responsibility for governance and executive decisions: para (2)(i)	Identity of customer matter: para (2)(a)	Contributes to establishing trustee's authority to act: para (2)(c)
Ownership and control structure: para (3)(a)	Identity of person on whose behalf customer is receiving the designated service: para (2)(b)	• Strong link to establishing trustee's authority to act: para (2)(c) • Strong link to establishing nature and purpose matter: para (2)(f)
Identity of beneficiary or description of class of beneficiary: para (3)(b)	Identity of person on whose behalf customer is receiving	N/A

	the designated service: para (2)(b)	
Identity of settlor, appointor, guardian or protector: para (3)(c)	Identity of person on whose behalf customer is receiving the designated service: para (2)(b)	N/A
Identity of trustees: subsection (4)	Identity of person acting on behalf of customer: para (2)(c)	N/A
Nature of business: subsection (5)	Nature and purpose matter: para (2)(f)	Contributes to establishing identity of the customer matter: para (2)(a)

337. The requirements under section 6-3 of the Rules reflect FATF recommendation 10 (10.3, 10.8, 10.9 and 10.11 in the FATF methodology) in relation to legal arrangements.

6-4—Customer is a government body

338. Subsection 6-4 sets out specific requirements for establishing the identity of customers under paragraph 28(2)(a) of the Act where the customer is a government body. The requirements under section 6-4 of the Rules relate to designated services provided in Australia and applies to all designated service types.

339. The section requires that a reporting entity must collect at least the specified KYC information where the customer is a government body. The KYC information is specified in subsection 6-4(2) of the Rules.

340. Aside from paragraph 6-4(2)(c) of the Rules, subsection 6-4(2) of the Rules largely reflect the equivalent requirements under subsection 6-2(2) of the Rules in relation to a customer that is a body corporate, partnership or unincorporated association.

341. Paragraph 6-4(2)(c) of the Rules requires a reporting entity to collect KYC information on the name of the country or part of a country under which the customer is established where the customer is a government body. For example, for the Independent Broad-based Anti-corruption Commission (IBAC), this would be Victoria—while the IBAC exists in Australia, the part of Australia in which was established is Victoria.

6-5—Establishing the identity of persons associated with the customer

342. Section 6-5 of the Rules relates to circumstances where the customer has:
- a person on whose behalf a customer is receiving a designated service, and/or
- a person acting on behalf of a customer, and/or
- a beneficial owner.

343. In such circumstances, subsections 28(2)(b) to (d) of the Act requires a reporting entity to establish the identity of that associated person. Section 6-5 of the Rules specifies the KYC information that the reporting entity must collect in relation to that associated person. The KYC information specified will depend on the type of person that the associated person is.

344. For example, if the customer is a body corporate and has a beneficial owner that is a partnership, the reporting entity must collect in relation to that beneficial owner at least the KYC information specified in subsection 6-2(2) of the Rules for the purposes of establishing the identity of that beneficial owner pursuant to paragraph 28(2)(d) of the Act. Similarly, if a customer is a trust with a corporate trustee, the reporting entity must collect information in relation to the corporate trustee as required under section 6-2 for bodies corporate. If the corporate trustee is a publicly listed company, a reporting entity may also, for example, take advantage of section 6-7 which reduces the requirement to establish beneficial ownership of the publicly listed corporate trustee.

6-6—Person on whose behalf customer is receiving the designated services

345. Section 6-6 of the Rules clarifies the scope of paragraph 28(2)(b) of the Act which requires reporting entities to establish on reasonable grounds the person on whose behalf the customer is receiving the designated service, that is, to clarify that a reporting entity is not required to establish the identity of its customers' customers.

346. The principal situation under which a customer receives a designated service on behalf of another person under Australian law arises where a customer is receiving services on behalf of beneficiaries, e.g.:
    - a trust (actioned by the trustee acting on its behalf) is the customer receiving designated services of behalf of its beneficiaries (beneficiaries ordinarily do not 'control' the trust and therefore are not the same as 'beneficial owners'). Some similar legal arrangements under foreign laws can also involve equivalents to beneficiaries. This is distinct from agency and power of attorney arrangements under which the agent or attorney receives the designated service not as the customer, but on behalf of the customer.
    - a holder of a life policy or sinking fund policy may be receiving designated services specified under items 37 or 38 of table 1 of section 6 of the Act from the insurer on behalf of beneficiaries of the policy. See Division 10 for requirements relating to those designated services.

347. See Division 10 for sections relating to those designated services.

6-7—Beneficial owners of the customer

348. Section 6-7 of the Rules provides an exception from the requirement to establish the identity of the beneficial owners of a customer pursuant to paragraph 28(2)(d) of the Act where the customer is a listed company subject to public disclosure requirements.

Where a reporting entity establishes on reasonable grounds that a customer is of this type, it is taken to have met its beneficial owner obligations in relation to that customer. This section aligns with FATF recommendation 10 (10.10 and footnote 71 in the FATF methodology).

349. In light of this exception, section 6-7 also relieves reporting entities of the requirement to establish whether any beneficial owner of listed company is designated for targeted financial sanctions (since there is no information on which to establish this). This does not, however, relieve reporting entities of the obligation to establish whether the listed company, its customer, is designated for targeted financial sanctions.

350. The relief offered by this section from establishing the identity of beneficial owners is not restricted to designated services provided at or through permanent establishments in Australia and applies to designated services provided anywhere in the world.

6-8—Beneficial owners and senior manager, for bodies corporate, partnerships and unincorporated associations

351. Section 6-8 of the Rules provides for circumstances where a reporting entity either:
    - is unable to establish the identity of any beneficial owners, or
    - establishes that there are no beneficial owners.

352. The section specifies that, in such circumstances, the reporting entity must establish the identity of the individual who is the chief executive officer (or equivalent) of the customer. The relief offered by this section from establishing the identity of beneficial owners is not restricted to designated services provided at or through permanent establishments in Australia and applies to designated services provided anywhere in the world.

353. This section aligns with FATF recommendation 10 (10.10 in the FATF methodology) to identify the relevant natural person who holds the position of senior managing official in such circumstances.

6-9—The nature and purpose of the occasional transaction or business relationship

354. Section 6-9 of the Rules provides relief from verifying the nature and purpose of a business relationship unless the reporting entity is required to apply enhanced due diligence to the customer under section 32 of the Act. A reporting entity must still identify the ML/TF risk of the customer (which in most cases is necessary to determine whether enhanced due diligence is required), and collect information about the nature and purpose of the business relationship that is appropriate to the ML/TF risk of the customer. If the customer is an individual, a reporting must take reasonable steps to establish that the person the customer claims to be. This section aligns with FATF recommendation 10 (10.8 in the FATF methodology) to understand the nature of the customer's business where the customer is a legal person or arrangement. It also aligns

with item 10.6 in the FATF methodology to understand the purpose and intended nature of the business relationship and, if appropriate, obtain information to support it.

355. The relief offered by this section from verifying KYC information to establish the nature and purposes of the business relationship or occasional transaction is not restricted to designated services provided at or through permanent establishments in Australia and applies to designated services provided anywhere in the world.

6-10—individual cannot provide satisfactory evidence regarding a matter

356. Section 6-10 provides relief from the requirement to verify KYC information using reliable and independent data for some customers and associated persons who are individuals. In these circumstances, an alternative standard applies requiring verification from data reasonably available to the reporting entity and implementation of AML/CTF policies to mitigate the associated risks.

357. The section allows for alternative verification requirements for a person who is:
    - an individual, and
    - unable to provide information or evidence of identity because they are:
        - unable to obtain the information or evidence, or
        - unable to access the information or evidence due to circumstances beyond their control.

358. These circumstances are intended to encompass people who may not have access to standard verification methods, such as:
    - Aboriginal and Torres Strait Islander peoples
    - people affected by natural disasters such as floods or bushfires
    - people affected by family and domestic violence
    - people experiencing periods of homelessness
    - people who are or have recently been in prison
    - refugees, asylum seekers and recent migrants to Australia (including people from culturally and linguistically diverse backgrounds)
    - intersex, transgender and gender diverse people
    - people who have difficulty providing identification due to health or ageing related reasons
    - people who did not have their birth registered
    - young people who have not established a social footprint in the community
    - people in less developed jurisdictions with limited access to formal evidence of identity.

359. In these circumstances, the reporting entity must:
    - determine the customer's ML/TF risk based on the KYC information about that person that is reasonably available to the reporting entity before commencing to provide the designated service,

- collect KYC information about the person appropriate to the customer's ML/TF risk, and
- take reasonable steps to verify KYC information using data reasonably available to them. This permits reporting entities to rely on alternate data to verify a customer's identity, such as referee statements, government correspondence, or a community identification documents or Indigenous organisation membership card for Aboriginal and Torres Strait Islander peoples.

360. The reporting entity must also implement AML/CTF policies to mitigate and manage any additional ML/TF risk arising from the lack of information or evidence of the person's identity.

361. The relief offered by this section from verifying KYC information using reliable and independent data is not restricted to designated services provided at or through permanent establishments in Australia and applies to designated services provided anywhere in the world, including to support financial inclusion in less developed jurisdictions.

6-11—Previous compliance in a foreign country

362. Section 6-11 of the Rules enables a reporting entity to 'passport' a customer to receive designated services in Australia, where the reporting entity or a member of its reporting group has undertaken initial CDD under the law of a foreign country.

363. The section is limited to initial CDD carried out by persons regulated by laws of a foreign country that give effect to the CDD and record-keeping requirements under the FATF recommendations. The intent of these requirements is to offer relief from the regulatory impost on a reporting entity from having to undertake initial CDD when it has already applied an equivalent process to that customer under laws that achieve the same AML/CTF outcome.

364. The CDD undertaken under the law of a foreign country must still establish each of the matters in subsection 28(2) of the Act, unless the law of the foreign country does not require the matter to be established on the basis of low risk (e.g. where a relevant simplified due diligence measure is available under the foreign law).

Division 2—Providing services before completion of initial customer due diligence

365. Division 2 of Part 6 of the Rules specifies the circumstances and conditions in which a reporting entity can delay verification or other initial CDD measures related to a customer until after commencing to provide a designated service, despite the general obligation under subsection 28(1) of the Act to do so beforehand.

366. The sections in the Rules made under section 29 of the Act recognise that there are circumstances where it would otherwise not be practically and operationally feasible to meet the initial CDD requirements without interrupting the ordinary conduct of

business. Under section 29 of the Act, a reporting entity can delay the verification or initial CDD of a customer if it can satisfy each of the circumstances and requirements under that section, as well as any requirements set out in the Rules. In the absence of such Rules, delayed verification under section 29 is not available.

367. Section 29 of the Act requires, for any of the circumstances in which the Rules permit delayed initial CDD measures, that a reporting entity must:
    - determine on reasonable grounds that commencing to provide the designated service to the customer before completing initial CDD is essential to avoid interrupting the ordinary course of business,
    - have AML/CTF policies to complete initial CDD on the customer as soon as practicable and not later than the period specified in the Rules (if any),
    - determine on reasonable grounds that any additional risk of ML/TF or proliferation financing associated with delaying completion of initial CDD is low, and
    - implement AML/CTF policies to mitigate and manage the associated risks.

368. The sections set out below enliven delayed initial CDD but must be read together with the requirements in section 29 of the Act.

6-12—Delayed verification—various designated services provided in Australia

369. Where a reporting entity meets all of the other requirements of section 29 of the Act, this section permits a reporting entity to delay verification (but not collection) of KYC information relating to the matters specified under paragraphs 28(2)(b), (d), (e), (f) and (g) of the Act. The verification of KYC information related to the matters under paragraphs 28(2)(a) and (c) of the Act (the identity of the customer and the identity of any person acting on behalf of the customer and their authority to act, respectively) cannot be delayed. As the reporting entity will generally be dealing directly with the customer or a person acting on their behalf, obtaining reliable and independent data to verify their identity and, for persons acting on behalf of the customer, their authority act, should generally be straightforward.

370. This section applies to designated services provided at or through a permanent establishment in Australia. Subsection 6-12(4) also specifies the requirement that a reporting entity can provide a designated service before satisfying subsection 28(2) of the Act if that designated service does not allow either:
    - the transfer of money, property or virtual assets for on behalf of the customer, or
    - otherwise making money, property or virtual assets available to the customer (except where the money, property or virtual asset is made available to the customer in an account or otherwise on deposit).

371. Accordingly, in practice, while it may be possible to *commence* to provide most designated services, where a designated service which inherently involves the transfer of, or dealing with, assets, verification of relevant KYC information may only be able

to be delayed until a very early stage in the provision of the service. For example, while it may be possible for a reporting entity to accept an instruction to transfer money, property or virtual assets under item 29 in table 1 of section 6 of the Act, the reporting entity will be prevented from giving effect to that instruction until all required verification is completed. This limits the ML/TF risk arising from the delayed verification by limiting the access that the customer has to the money, property or virtual asset or the benefit a customer would obtain from transferring or receiving money, property or virtual assets in dealings with third parties.

372. This section also provides that verification pursuant to paragraph 28(3)(d) of the Act must be complete within 20 business days after commencing to provide the designated service. However, this does not operate to allow delaying verification for 20 business days where it is practicable to complete it sooner; subsection 29(c)(i) of the Act requires that initial CDD must be completed as soon as reasonably practicable in all cases.

373. To avoid conflict between delayed verification provisions, this section does not apply in circumstances where a delay is available to the reporting entity under another section in the Rules (currently, sections 6-13, 6-14 and 6-32 of the Rules).

6-13—Delayed verification—opening an account and deposit

374. Section 6-13 substantively reproduces the delayed verification rules in Chapter 79 of the former rules which permit a financial institution to delay the verification of KYC information as part of initial CDD in relation to the opening of accounts and accepting deposits. This section relates to delayed collection and verification of KYC information. In accordance with section 29 of the Act, initial CDD must be completed as soon as reasonably practicable, replacing the former deadline of 15 business days.

375. The section includes restrictions to mitigate the risks of providing a financial institution account to a customer before completing initial CDD, i.e. the only designated services that can be provided before completion of initial CDD are opening the account and accepting deposits (and designated services incidental to these). A financial institution must also not allow any of the following to occur before completing initial customer due diligence in accordance with section 28(1) of the Act:
    - the transfer of money, property or virtual assets for on behalf of the customer, or
    - otherwise making money, property or virtual assets available to the customer (except where the money, property or virtual asset is made available to the customer in an account or otherwise on deposit).

6-14—Delayed verification—certain financial markets transactions

376. Section 6-14 substantively reproduces the delayed verification rules in Chapter 46 of the former rules. The section permits delayed collection and verification of KYC information as part of initial CDD when specific kinds of designated services are

provided on declared financial markets. The section requires that the verification must be completed no later than 5 business days after the day on which it first provided those relevant designated services to the customer. However, this does not operate to allow delaying verification for 5 business days where it is practicable to complete it sooner; subsection 29(c)(i) of the Act requires that initial CDD must be completed as soon as reasonably practicable in all cases.

377. The intent of this section is to address circumstances where the transaction must be performed rapidly due to financial market conditions relevant to the transaction. The term 'declared financial market' has the meaning given by the *Corporations Act 2001* and its incorporation by reference into subsection 6-14(1) is permitted by paragraph 14(1)(a) of the *Legislation Act 2003*.

6-15—Delayed initial customer due diligence—service provided in foreign country

378. Under section 6 of the Act, certain designated services provided by reporting entities at or through permanent establishments in foreign countries are subject to the Act. Section 6-15 of the Rules recognises that these designated services will in many cases also be subject to foreign AML/CTF laws, which may permit delayed initial CDD in circumstances not otherwise permitted under the Rules.

379. Section 6-15 seeks to reduce possible conflicting AML/CTF obligations for reporting entities providing designated services in foreign countries by permitting delayed initial CDD where the laws of the foreign country in which that designated service is being provided:
- give effect to the FATF recommendations, and
- allow delayed completion of initial CDD.

380. Consistent with FATF recommendation 10, delayed initial CDD under section 6-15 remains subject to the overarching requirements of section 29 of the Act, including that the reporting entity:
- determines on reasonable grounds that commencing to provide the designated service to the customer before completing initial CDD is essential to avoid interrupting the ordinary course of business,
- has AML/CTF policies to complete initial CDD as soon as reasonably practicable after commencing to provide the designated service to the customer,
- has in place AML/CTF policies to manage and mitigate associated ML/TF risk, etc.

Division 3—Simplified customer due diligence

381. Section 31 of the Act permits reporting entities to apply simplified customer due diligence measures where:
- the ML/TF risk of the customer is low

- section 32 does not require enhanced due diligence measures to be applied to the customer, and
- the reporting entity complies with the requirements specified in the AML/CTF Rules.

382. Under criterion 10.18 of the FATF methodology, countries commit to allow and encourage simplified customer due diligence where lower risks have been identified. The Rules in Division 3 support reporting entities to apply simplified measures in a range of low-risk situations.

6-16—Simplified customer due diligence requirements generally

383. The purpose of section 6-16 is to enliven the simplified due diligence provision under section 31 of the Act by specifying the circumstances in which a reporting entity can apply simplified due diligence. Section 6-16 specifies that a reporting entity's AML/CTF policies must deal with simplified due diligence before it can undertake simplified measures.

6-17—Simplified initial customer due diligence for certain matters

384. Section 6-17 of the Rules relieves reporting entities of the obligation to verify KYC information in relation to certain matters in subsection 28(2) of the Act where simplified due diligence is permitted under section 31 of the Act.

385. Under section 6-17, a reporting entity applying simplified customer due diligence is not required to verify KYC information related to the following matters:
- the identity of any person on whose behalf the customer is receiving the designated service;
- the identity of any person acting on behalf of the customer and their authority to act;
- if the customer is not an individual—the identity of any beneficial owners of the customer.
- where there are no reasonable grounds for the reporting entity to doubt the adequacy or veracity of the KYC information collected in relation to these matters.

386. This section should be read together with section 6-9 which relieves reporting entities of the obligation to verify KYC information related to the nature and purpose of the business relationship or occasional transaction where the customer is low or medium, and enhanced customer due diligence obligations don't otherwise apply.

387. KYC information related matters not listed above must still be verified, although the information collected and verification undertaken must appropriate to the ML/TF risk of the customer. This means:

- Reporting entities must verify KYC information related to the identity of the customer even when applying simplified customer due diligence.
- Reporting entities must verify KYC information related to whether the customer and any related persons (listed in paragraph 28(2)(e) of the Act) are politically exposed persons or subject to targeted financial sanctions for all customers. These are fundamental considerations in determining whether a reporting entity is even permitted to undertake simplified customer due diligence for a customer.
- While a reporting entity may not have verified, for example, the beneficial owner(s) of a customer, the information collected in relation to the beneficial owners may still be used for determining their PEP and sanctions status.

Section 6-18—Simplified initial customer due diligence for identity of beneficial owners

388. Section 6-18 relieves reporting entities of the obligation to establish the identity of beneficial owners of certain kinds of customer, where these customers are otherwise eligible for simplified customer due diligence under section 31. The kinds of customers are customers that are, or are controlled by, one of the following types of persons:
    - a government body, a term defined under the Act.
    - an entity subject to active supervisory oversight by a prudential, insurance or investor protection regulator through registration or licencing requirements (such as APRA and ASIC in Australia, and their equivalents in foreign countries; simple registration of a business name or of a company with ASIC, nor registration of a self-managed super fund with the ATO do not qualify).
    - owners corporations or strata title schemes.

389. If a reporting entity establishes on reasonable grounds its customer is one of the kinds of customers above, and eligible for simplified customer due diligence under section 31 of the Act, the reporting entity is taken to have complied with the requirement to establish the beneficial owner of the customer under paragraph 28(2)(d) of the Act.

6-19—Person acting on behalf of customer

390. Section 6-19 of the Rules relates only to a reporting entity's obligation to establish the identity of a person acting on behalf of a customer and their authority to act pursuant to paragraph 28(2)(c) of the Act. This section is limited undertaking initial customer due diligence for non-individual customers.

391. This section is designed to address circumstances where the reporting entity has established the authority to act element under paragraph 28(2)(c) of the Act, but is impractical and disproportionate to ML/TF risk to establish the identity of the person acting on behalf of the customer.

392. This section specifies that a reporting entity is taken to have complied with both elements of its obligation under paragraph 28(2)(c) of the Act where:

- the scope of authority to act does not significantly increase the ML/TF risk of the customer,
- the reporting entity has collected KYC information about the associated person that is appropriate to the customer's ML/TF risk, and
- there are no reasonable grounds for the reporting entity to doubt the adequacy or veracity of that KYC information.

393. These requirements do not require the reporting entity to identify the ML/TF risk of the associated person, however, they acknowledge that the customer's relationship with the associated person can influence the customer's ML/TF risk. This section permits reporting entities to take simplified measures that are appropriate to the risk.

Division 4—Enhanced customer due diligence

394. Section 32 of the Act requires reporting entities to undertake enhanced customer due diligence measures in a range of circumstances, including where the ML/TF risk of the customer is high, the customer is a foreign politically exposed person, or the reporting entity is providing designated services to the customer in a nested service relationship.

6-20—Enhanced customer due diligence required when customer seeks unusual services

395. The interpretive note to FATF recommendation 10 states that reporting entities should examine, as far as reasonably possible, the background and purpose of all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Section 6-20 implements this requirement and is in addition to the enhanced CDD triggers set out in subsections 32(a) to (e) of the Act.

396. The Act andRules are generally not prescriptive about what enhanced CDD measures require, but where enhanced CDD is to be applied due to the operation of section 6-20, enhanced measures may include:
    - collecting additional KYC information;
    - verifying KYC information using additional reliable and independent data,
    - taking additional measures to understand better the background, ownership and financial situation of the customer, and other parties to the transaction,
    - taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the business relationship or occasional transaction; or
    - increasing the monitoring of the customer, including greater scrutiny of transactions.

397. Enhanced CDD under this section may arise from monitoring undertaken as part of ongoing CDD under section 30 of the Act. Enhanced CDD under this section is not, however, a pre-condition to a reporting entity 'suspecting on reasonable grounds' a

matter under section 41 of the Act, i.e. giving a SMR to AUSTRAC must not be delayed on account of completing enhanced CDD.

6-21—Establishing source of wealth and source of funds when enhanced due diligence required in certain circumstances

398. Section 6-21 of the Rules specifies the circumstances in which a reporting entity must conduct source of funds and wealth checks on a customer as part of enhanced CDD. The section applies both when undertaking initial CDD under section 28 of the Act and ongoing CDD under section 30 of the Act, when:
    - source of funds or wealth information is relevant to the nature of the customer's ML/TF risk, and
    - an enhanced CDD obligation has arisen in relation to that customer because of one of the following:
        - the customer's ML/TF risk is high (section 32(a) of the Act).
        - a suspicious matter reporting obligation has arisen in relation to the customer (section 32(b) of the Act).
        - the customer or associated person is present or was formed in a jurisdiction that FATF identifies as high risk and in relation to which enhanced CDD should be applied (section 32(d) of the Act). These jurisdictions are often referred to as being on the 'black list'—further information can be found on the FATF website.

399. For example, a reporting entity must establish the source of wealth and source of funds of a customer that has previously been a high-risk domestic or international organisation PEP, or foreign PEP, and who remains high ML/TF risk after ceasing to be a PEP due to continuing political influence.

6-22—Enhanced customer due diligence required for certain virtual asset services

400. Section 6-22 of the Rules requires that a reporting entity must apply enhanced CDD measures on a customer where the customer has deposited or received physical currency in the course of exchanging virtual money or assets under items 50A of table 1 of section 6 of the Act. Such enhanced CDD includes, but is not limited to:
    - collecting and verifying KYC information about the customer's source of wealth (noting also the additional trigger for establishing source of wealth for initial and ongoing customer due diligence under section 6-21), and
    - collecting and verifying KYC information about the customer's source of funds for every transaction involving the exchange of physical currency for virtual assets or vice versa.

401. This section responds to the inherently very high ML/TF risks presented by crypto-ATM and other physical currency based virtual asset exchange services.

Division 5—Politically exposed persons

402. The ML NRA states that PEPs can be an attractive target for bribery and corruption given their capacity to influence government spending and decision making. The ML NRA states that foreign PEPs pose a particularly high ML/TF risk due to their potential to receive and handle proceeds of bribery and corruption. Domestic PEPs and international organisation PEPs are not necessarily considered high ML/TF risk, however, the potential influence of persons in these positions on the operation of domestic governments and international public organisations should be considered a factor that may influence the impact on the ML/TF risk posed by such persons.

6-23—Matters for initial customer due diligence—politically exposed person

403. Section 6-31 prescribes additional matters which must be established on reasonable grounds once a reporting entity has established on reasonable grounds that a customer, beneficial owner of a customer, or person on whole behalf the customer is receiving the designated service is:
    - a foreign PEP,
    - a domestic PEP or international organisation PEP and the ML/TF risk of the customer is high.

404. The additional matters to be established on reasonable grounds are the PEP's source of funds and source of wealth.

405. This requirement to establish source of funds and source of wealth does not automatically extend to PEPs acting on behalf of a customer. In such cases, risk-based enhanced customer due diligence applies.

406. Subsection 6-23(3) applies to those situations where a reporting entity provides a designated service at or through a permanent establishment in a foreign country, and the customer is PEP by because of their connection to that foreign country. In most circumstances such a PEP would be considered a domestic PEP under the laws of the foreign country. Subsection 6-23(3) of the Rules therefore allows reporting entities subject to the AML/CTF Act but proving services at or through a permanent establishment in a foreign country to treat that country's PEPs in the same way as domestic PEPs, i.e. the specific PEP due diligence requirements apply only where the ML/TF risk of the customer is high.

6-24—Ongoing customer due diligence—politically exposed person

407. Section 6-24 of the Rules provides an express trigger for a reporting entity to review, and where appropriate, update and reverify KYC information relating to the customer, as part of ongoing customer due diligence where the customer becomes a foreign PEP or a high-risk domestic or international organisation PEP.

408. As with subsection 6-23(3) of the Rules in relation to initial customer due diligence, this section applies to customers that have been provided designated services at or

through a permanent establishment in a foreign country for which the customer is a PEP—in such circumstances, the customer should be treated as a domestic PEP.

Division 6—Nested services relationships

409. FATF recommendation 13 sets out specific due diligence and governance measures for banks entering and providing services as part of correspondent banking relationships. Recommendations 13 and 15 extend these requirements to 'other similar relationships' including those entered into by VASPs.

410. Correspondent banking relationships among authorised deposit-taking institutions and foreign banks, building societies, credit unions are dealt with under Part 8 of the Act and Part 7 of the Rules.

411. The Act covers 'other similar relationships' as described in the FATF recommendations under the term 'nested services relationships'. This recognises that the ML/TF risks addressed by special due diligence measures required for such relationships arises from the fact that the Australian-regulated reporting entity is facilitating an overseas counterpart to provide services to the overseas counterpart's own customers, without having any direct visibility of those customers. This leaves Australian-regulated reporting entities potentially exposed to ML/TF risk (including sanctions risk) without knowing it.

412. Nested services relationships are defined in section 5 of the Act as a relationship that involves the provision of a designated service by a reporting entity that is a remitter, virtual asset service provider or financial institution to a customer that is a remitter, virtual asset service provider or financial institution where:
    - the reporting entity provides the designated service at or through a permanent establishment in one country; and
    - the customer uses the designated service to provide services to its own customers at or through a permanent establishment in another country; and
    - the relationship is not a correspondent banking relationship.

413. The exclusion of correspondent banking relationships from the definition recognises that such relationships are regulated under other provisions. This exclusion needs to be read together with the definition of 'correspondent banking relationship' in section 5 of the Act which applies more broadly than simply those relationships involving 'vostro' accounts. Correspondent banking relationships for the purposes of the carve out from 'nested services relationships' extends to any 'banking services' provided by one financial institution to another financial institution where certain geographic requirements are met relating to the cross-border nature of the relationship.

414. Australian financial institutions (ADIs, banks, building societies and credit unions) may be party to a nested services relationship where they provide a designated service to a

foreign bank, remitter or VASP outside the scope of a correspondent banking relationship (as defined in section 5 of the Act), e.g:

- the Australian financial institution provides services to a foreign counterpart related to the foreign counterpart's provision of virtual asset exchange or virtual asset safe-keeping services to its own customers
- the Australian financial institution provides services to a foreign remitter or VASP related to the foreign remitter's or VASP's provision of value transfer services (however, facilitating international value transfer services among ADIs, banks, building societies and credit unions will ordinarily be done within a correspondent banking relationships).

415. The correspondent banking relationship exclusion is not applicable to Australian remitters and VASPs, who will be party to a nested services relationship whenever they provide designated services to any foreign financial institution, remitter or VASP that the foreign counterpart uses to provide services to its own customers.

416. Subsection 32(e) of the Act requires reporting entities to undertake enhanced customer due diligence when providing designated services as part of a nested services relationship. When providing a designated service as part of a nested services relationship, enhanced customer due diligence does not automatically extend to 'know your customer's customer' (KYCC) requirements for each service provided by the foreign counterpart, but sets out risk mitigation measures related to the relationship itself.

417. Division 6 should be read together with section 5-5 of the Rules which set out AML/CTF program requirements relating to senior manager approval for commencing to provide a designated service as part of a nested services relationship.

6-25—Matters for initial customer due diligence—nested services relationship

418. Section 6-25 sets out a range of information that a reporting entity providing designated services as part of a nested services relationship must establish. These matters generally align with those matters required as part of correspondent banking relationship due diligence under Part 6 of the Act.

419. The alignment of the requirements is intended to facilitate the use or adaptation of globally recognised correspondent banking due diligence tools, such as the Wolfsberg Group's Correspondent Banking Due Diligence Questionnaire (accessible at https://wolfsberg-group.org/resources) and Financial Crime Compliance Questionnaire (accessible at https://wolfsberg-group.org/resources) as part of meeting nested services enhanced due diligence requirements under the Act and Rules.

420. The matters to be established in section 6-25 go to:

- Subsections (a) to (c)—the ownership and control of the customer and their ultimate parent, and relevant geographic factors about both.

- Subsections (d) to (f)—the existence and quality of AML/CTF supervision to which the customer is subject, the appropriateness of the customer's own AML/CTF systems and controls, and any publicly available information about the customer's compliance with AML/CTF and sanctions obligations or contravention of relevant criminal offices. Given the reporting entity will not have direct visibility of the foreign counterpart's customers these matters ensure consideration is given at the systemic level to the foreign counterpart's implementation of, and compliance with, relevant laws.
- Subsection (g)—the foreign counterpart's carrying out of initial customer due diligence on its own customers, and the ability to provide relevant information to the Australian-regulated reporting entity on request. This is not a KYCC requirement, but an appropriate risk mitigation where, for example, the Australian-regulated reporting entity needs to investigate possible ML/TF risks arising in relation to the nested services relationship. This is particularly applicable for any services that are equivalent to 'payable-through accounts' mentioned in criterion 13.2 of the FATF methodology.
- Subsection (h) and (i)—ensuring that the Australian-regulated reporting entity does not provide designated services to any foreign counterpart that provides services to shell banks. This implements criterion 13.3 of the FATF methodology.

6-26— Ongoing customer due diligence—nested services relationship

421. Subsections 6-26(1) and (2) set out ongoing customer due diligence measures that a reporting entity must undertake when providing a designated service as part of a nested services relationship, which are generally aligned with those applicable to correspondent banking due diligence:
    - if more than 2 years has elapsed since the reporting entity last identified and assessed the ML/TF risk of the customer, the reporting entity must review and, where necessary, update its identification and assessment of the ML/TF risk of the customer, and
    - if more than 2 years has elapsed since the reporting entity last collected or reviewed the KYC information relating to the customer, the reporting entity must review and, where necessary, update and re-verify KYC information about the customer.

422. Subsection 6-26(3) requires a reporting entity to undertake ongoing customer due diligence to monitor for where it begins to provide a designated service to a customer as part of a nested services relationship. In such cases, the reporting entity must review and, if necessary, update and reverify the KYC information about the customer.

423. Subsection 6-26(3) is only triggered by the provision of a new kind of designated service or providing a service for the first time as part of a nested services relationship. The ongoing provision of designated services of the same kind as part of an established

nested service relationship is, on the other hand, subject to general ongoing customer due diligence obligations under section 30 of the Act.

Division 7—Transferred customers

Section 6-27—Initial customer due diligence—transferred customer

424. Section 6-27 of the Rules provides a reporting entity with regulatory relief from initial CDD where its customer was transferred from another reporting entity (prior reporting entity) as a result of any of the following circumstances:
    - the prior reporting entity assigned, conveyed, sold or transferred the whole of a part of its business to the reporting entity.
    - the prior reporting entity was subject to a voluntary transfer under the Financial Sector (Transfer and Restructure) Act 1999.
    - the prior reporting entity transferred all or part of its assets and liabilities to the reporting entity as a result of a compulsory transfer under statute.

425. The prior reporting entity must have also provided to the reporting entity copies of the records it kept pursuant to sections 107, 108, 111 and 114 of the Act in relation to the customer.

426. A note is included with this section to remind reporting entities that the regulatory relief under this section applies only to initial CDD—the reporting entity is still required to undertake ongoing CDD on the customer, including the requirement to review, and where appropriate, update and re-verify KYC information relating to the customer if the reporting entity has doubts about the adequacy or veracity of the KYC information relating to the customer under subparagraph 30(2)(c)(i) of the Act.

6-28—Ongoing customer due diligence—transferred pre-commencement customer

427. Section 6-28 of the Rules is designed to replicate the pre-commencement customer regulatory relief under section 36 of the Act for reporting entities that have acquired pre-commencement customers as defined under section 36 of the Act as part of a business sale or transfer.

428. This section applies only to transactions for the sale or transfer of a business from one reporting entity (prior reporting entity) to another reporting entity that is one of the following:
    - The prior reporting entity assigned, conveyed, sold or transferred the whole of a part of its business to the reporting entity.
    - The prior reporting entity transferred all or part of its assets and liabilities as a result of a voluntary transfer under the Financial Sector (Transfer and Restructure) Act 1999.
    - The prior reporting entity transferred all or part of its assets and liabilities as a result of a compulsory transfer under statute.

429. The prior reporting entity must have also provided to the reporting entity copies of the records it kept pursuant to sections 107, 108, 111 and 114 of the Act in relation to the customer.

430. Following the completion of the transaction, the reporting entity must monitor for significant changes in the nature and purpose of the business relationship with the customer that may result in the ML/TF risk of the customer being high or medium (consistent with the obligations that would apply under section 36 of the Act if the customer had been a pre-commencement customer of the reporting entity itself). The regulatory relief under this section will no longer apply if:
    - a suspicious matter reporting obligation under section 41 of the Act arises, or
    - there is a significant change in the nature and purpose of the business relationship with the customer that results in the ML/TF risk of the customer being medium or high.

431. In such circumstances, the reporting entity will need to apply section 30 of the Act in relation to that customer moving forward.

Division 8—Reliance on collection and verification of KYC information

432. Division 8 of Part 6 of the Rules sets out requirements for a reporting entity that chooses to rely on collection and verification of KYC information as part of initial customer due diligence previously carried out by another reporting entity or foreign equivalent. It does not apply to 'outsourcing' or carrying out CDD through agency arrangements under section 37 of the Act.

433. There are two kinds of reliance available under the Act and this is reflected in Division 7:
    - Reliance on the collection and verification of KYC information carried out by another reporting entity or foreign equivalent under a CDD arrangement (section 37A of the Act), and
    - Reliance on the collection and verification of KYC information previously carried out by another reporting entity or foreign equivalent on a case-by-case basis (section 38).

434. The consequences of a failings in carry out initial CDD under section 37A and section 38 are different:
    - for reliance under a compliant section 37A CDD arrangement, the reporting entity remains responsible for remediation of any of the matters it was required to establish in relation to the customer under section 28 of the Act, but is still deemed to have collected and verified KYC information as required for those matters, and
    - for reliance under a section 38, the relying reporting entity is not taken to have collected or verified KYC information where this was not, in fact, done by the relied on reporting entity or foreign equivalent.

435. Chapter 7 of the former rules previously included rules made under section 38 of the Act related to reliance by a reporting entity on the collection and verification of KYC information carried out by a member of the same corporate group or designated business group. This is no longer required under the amended Act as reliance within reporting groups is now covered by:
    - AML/CTF program requirements, e.g. subsection 26F(6) of the Act related to information sharing and record keeping within reporting groups,
    - section 236B of the Act which allows for one member of a reporting group to discharge AML/CTF obligations on behalf of another reporting entity member, and
    - other sections of the Rules (e.g. section 6-11 in relation to initial CDD carried out under the laws of a foreign country).

6-29—Requirements for agreement or arrangement on collection and verification of KYC information

436. Section 6-29 sets out requirements for CDD arrangements entered into under section 37A of the Act. These requirements substantively reproduce the requirements in Chapter 7 of the former rules. These requirements are:

    - Paragraph (1)(a)—that the other party to the CDD arrangement is a reporting entity or a foreign equivalent (a person regulated by one or more laws of a foreign country that give effect to the FATF recommendations relating to customer due diligence and record keeping);
    - Paragraph (1)(b) and subsection (2)—that the CDD arrangement is appropriate to the ML/TF risks of the relying reporting entity, taking into account the nature, size and complexity of the other party's business, the kinds of customers they have and the country in which they operate or are resident. This ensures that a reporting entity that provides higher risk or complex services, deals with higher risk customers or customers with complex structures, considers the appropriateness of relying on another business that does not typically deal with these types of risks or customers and may not have the sophistication to carry out initial CDD to an appropriate standard;
    - Paragraph (c)—the requirement for the relying reporting entity to obtain the KYC information from the other party to the CDD arrangement, before commencing to provide a designated service (or later if permitted by Rules made under section 29 of the Act related to delayed initial CDD);
    - Paragraph (d)—the requirement for the relying reporting entity to obtain copies of data used for verification of KYC information in accordance with paragraph 28(3)(d) of the Act by the other party to the CDD arrangement, either immediately (e.g. under an IT system for information sharing) or as soon as practicable following a request by the relying reporting entity; and
    - Paragraph (e)—that the responsibilities of each party to the CDD arrangement be documented in the arrangement, including in relation to record-keeping.

6-30—Regular assessment of agreement or arrangement

437. Section 6-30 requires that a reporting entity must assess whether the agreement or arrangement continues to meet the requirements of section 6-29. When determining the frequency of the assessments, a reporting entity must take into account the type and level of ML/TF risks that it may reasonably face in providing designated services, though the interval between assessments cannot exceed 2 years.

438. Subsection 6-30(3) also sets out an event trigger for reviewing CDD arrangements, that is, if there is a change in circumstances that may affect whether the agreement or arrangement continues to meet the requirements of section 6-29, the reporting entity must carry out an assessment of the agreement or arrangement.

6-31—Requirements for reliance on collection and verification of KYC information

439. Section 6-31 sets out the requirements under section 38 of the Act relating to case-by-case reliance. These requirements substantively reproduce the requirements in Chapter 7 of the former rules however, as noted above, no longer require 'deemed compliance' provisions for reliance within corporate groups or designated business groups. The requirements are:

- Subsection (a)—reliance under section 6-31 is restricted to relying on another reporting entity or the foreign equivalent,
- Subsection (b)—reliance must be appropriate to the ML/TF risks of the customer, taking into account the nature, size and complexity of the other reporting entity or foreign equivalent's business, the kinds of customers they have and the country in which they operate or are resident. This ensures that a reporting entity that provides higher risk or complex services, deals with higher risk customers or customers with complex structures, considers the appropriateness of relying on another business that does not typically deal with these types of risks or customers and that may not have the sophistication to carry out initial CDD to an appropriate standard,
- Subsection (c)— the requirement for the relying reporting entity to have reasonable grounds to believe that it can obtain all of the KYC information collected from the other party to the CDD arrangement, before commencing to provide a designated service (or later if permitted by AML/CTF Rules made under section 29 of the Act related to delayed initial CDD),
- Subsection (d)—the requirement for the relying reporting entity to have reasonable grounds to believe that it can obtain copies of data used for verification of KYC information by the other party to the CDD arrangement, either immediately (e.g. under an IT system for information sharing) or as soon as practicable following a request, and
- Subsection (e)—that the reporting entity documents its reasons for believing the above requirements are met.

Division 9—Real estate transactions

6-32—Delayed initial due diligence—real estate transactions

440. Section 6-32 of the Rules permits delayed initial CDD for certain designated services provided in relation to real estate transactions. A delay under this section can only be applied in the following circumstances:
    - the real estate agent acting for the seller or transferor of real estate may delay initial CDD in relation to the buyer/transferee,
    - the real estate agent acting for the buyer or transferee may delay initial CDD in relation to the seller/transferor,
    - a professional services provider (such as a legal practitioner or conveyancer) acting for the buyer or transferee may delay initial CDD in relation to their client.

441. This section recognises that, in such circumstances, the ordinary course of business can be disrupted by the requirement to complete initial CDD before commencing to provide the relevant designated service. For example, when real estate is sold at auction, the buyer only becomes known after the fall of the hammer. There is usually a very short time between the conclusion of the auction and the signing of the contract of sale, making the completion of initial CDD challenging.

442. Similarly, the seller of the real estate who has accepted a verbal offer made by a buyer's agent's customer may only become known to the buyer's agent shortly before exchange of contracts, leaving little time complete initial CDD in relation to the seller, particularly where the seller is not an individual or has not had their identity verified by a seller's agent.

443. It is also common in Australia for legal practitioners or conveyancers to be engaged by a prospective buyer shortly before an auction or sale by private treaty.

444. In all of these circumstances, initial CDD must be completed as soon as practicable but no later than the earlier of the date of settlement or 15 business days from the date of exchange. This recognises circumstances where the settlement can, in some cases, occur sooner than 15 business days from exchange, and is designed to reflect the importance of completing initial CDD at the earliest date possible and, in any event, before the transfer of the real estate and the bulk of the consideration to be paid.

445. These delayed verification provisions are intended to operate alongside section 6-33 of the Rules relating to arrangements for the sharing of KYC information and verification data with real estate agents by other reporting entities involved in real estate transactions. However, the operation of this section is not restricted to circumstances where such arrangements are utilised.

6-33—Initial customer due diligence—real estate transactions

446. Section 6-33 of the Rules is designed to enable arrangements between reporting entities involved in a real estate transaction for the purpose of meeting many of their

obligations to complete initial CDD on their customers under section 28 of the Act. The relief available under this section is available only for reporting entities providing the specified kinds of designated service provided in Australia, namely:

- real estate agents providing a designated service under item 1 of table 5 of section 6 of the Act, and
- professional service providers providing a designated service under item 1 of table 6 of section 6 of the Act.

447. Under this section, real estate agents and professional services providers in such arrangements will be taken to comply with their obligation to establish on reasonable grounds the matters under paragraphs 28(2)(b) to (e) and (g) of the Act in relation to a customer where they:
    - have collected KYC information about these matters, and
    - are party to an arrangement that allows for the subsequent verification by another reporting entity involved in the transaction.

448. This section does not relieve real estate agents or professional service providers in such arrangements of the obligation to establish on reasonable grounds the identity of their customer, or the nature and purpose of the business relationship or occasional transaction pursuant to paragraph 28(2)(a) and (f) of the Act, respectively. Verification of the identity of a customer is relatively straightforward, and the nature and purpose of the business relationship or occasional transaction may be different for each reporting entity involved in a real estate transaction.

449. For a real estate agent or professional services provider to use this section, they must also implement the safeguards specified in this section. For example:
    - One of the safeguards requires that the arrangement can enable the relying reporting entity to receive the relevant KYC information. The relying real estate agent or professional services provider will need to assess the arrangement to ensure that the arrangement meets the requirements.
    - Initial CDD must also be completed before settlement of the sale, purchase or transfer of the real estate.
    - Another safeguard is designed to capture circumstances where an arrangement cannot be made or met, despite the intent to do so. The real estate agent or professional services provider must develop and maintain AML/CTF policies that deal with how it completes initial CDD before settlement where they do not receive the required verification data under an arrangement (see section 5-20 of the Rules).

450. The section is technology and platform neutral. This approach ensures that the flexibility afforded by this section is not limited to specific solutions.

451. This section responds to real estate industry concerns regarding duplication of initial CDD when multiple reporting entities are involved in a transaction and capability to

undertake the more complex aspects of initial CDD. This section is designed to offer concerned reporting entities a flexible framework within which to set up these arrangements to support their needs in a manner that is appropriate for their business and the ordinary course of real estate transactions across jurisdictions in Australia.

Division 10—Life policies and sinking fund policies

6-34—Initial customer due diligence—life policies and sinking fund policies

452. Section 6-34 of the Rules aligns the obligation of a reporting entity providing a life or sinking fund policy to establish the identity of the beneficiaries of that policy pursuant to paragraph 28(2)(b) of the Act with criterion 10.12 of the FATF methodology. A reporting entity must, before issuing or undertaking liability in relation to a life policy or sinking fund policy, collect the name of any person who may be entitled to receive a payment under such a policy or, if the nature of the policy means that it is not possible to identify each such person, collecting information describing each class of persons that may be entitled to a payment under the policy.

453. This section also applies when a reporting entity accepts a premium in relation such a policy. This means that if a named beneficiary, or a new class of beneficiaries, is added after a policy is issued, this name or information about the class must be collected before accepting a premium.

454. There is no requirement to verify this information—verification must, instead, occur before a payment is made to a person under such a policy, i.e. before the reporting entity commences to provide the designated service in item 39 of table 1 in section 6.

455. This section aligns with the beneficiary disclosure requirements under the *Insurance Contracts Act 1984*, where beneficiaries must be identified under an insurance policy in order to be able to claim under that policy.

Division 11—Ongoing customer due diligence

6-35—Ongoing customer due diligence—monitoring for unusual transactions and behaviours

456. Paragraph 30(2)(a) of the Act specifies, among other things, that in meeting subsection 30(1) of the Act, the reporting entity must monitor for unusual transactions and behaviours of customers that may give rise to a suspicious matter reporting obligation.

457. *Unusual transactions and behaviours* of a customer is defined (non-exhaustively) in section 30 of the Act to include the following:
- unusually large or complex transactions relating to the customer;
- transactions and behaviours that are part of an unusual pattern of transactions and behaviours relating to the customer;
- transactions and behaviours that have no apparent economic or lawful purpose;

- transactions and behaviours that are inconsistent with what the reporting entity reasonably knows about any of the following:
    - the customer;
    - the nature and purpose of the business relationship;
    - the ML/TF risk of the customer;
    - where relevant, the customer's source of funds or source of wealth.

458. Section 6-35 of the Rules specifies that a reporting entity is taken to comply with paragraph 30(2)(a) of the Act if it monitors its customers in relation to the provision of its designated services for unusual transactions and behaviours that may give rise to a suspicious matter reporting obligation because of the operation of:
    - paragraphs 41(1)(d) to (j) of the Act (other than subparagraph 41(1)(f)(iii)) which relate to where a reporting entity suspects on reasonable grounds:
        - that customer, proposed customer, or person seeking designated services (or their agent) is not who they claim to be,
        - that information the reporting entity has concerning the provision or prospective provision of the service may be relevant to investigation of, prosecution for, an evasion or attempted evasion of a Commonwealth, State or Territory taxation law,
        - that information the reporting entity has concerning the provision or prospective provision of the service may be of assistance in the enforcement of the *Proceeds of Crime Act 2002* or its regulations, or any law of a State or Territory that corresponds to that legislation,
        - that the provision or prospective provision of the service may is preparatory or the commission of an offence covered related to money laundering financing of terrorism;
    - subparagraph 41(1)(f)(iii) of the Act which relate where a reporting entity suspects on reasonable grounds to information the reporting entity has concerning the provision or prospective provision of the service may be relevant to investigation of, prosecution for an offence of a law of the Commonwealth, a State or Territory of any of the kinds listed in subparagraphs 6-35(b)(i) to (xxvi), and any other kind of offence that the reporting entity has identified in its ML/TF risk assessment as presenting a high risk in relation to the occurrence of money laundering.

459. The offences listed in subparagraphs 6-35(b)(ii) to (xxvi) are those identified by the FATF as key predicate offences for money laundering, as well as proliferation financing and other contraventions of Australian sanction laws. Subparagraph 6-35(b)(xxvii) extends ongoing transaction and behaviour monitoring requirements to any other money laundering predicate offence identified in a reporting entity's own ML/TF risk assessment as high risk.

460. The effect of section 6-35 of the Rules is that a reporting entity may limit its monitoring of customers in relation to the provision of its designated services under subsection 30(2) of the Act to these key predicate offences, as a subset of all offences in Australia.

This allows reporting entities to focus their ongoing CDD efforts and resources to comply with section 30(2) of the Act to offences which present the most serious harm to society and the financial system.

461. The section is not intended to limit the protections available in the AML/CTF Act in the event that a reporting entity does still form and report a suspicion under section 41 of the Act in relation to an offence outside one of the categories listed for transaction monitoring.

Division 12—Keep open notices

462. Sections 39A, 39B and 39C of the Act prescribe the requirements for the 'keep open notice' framework. Sections 6-36 to 6-41 of the Rules further prescribe the form and content of the various notices which form part of this framework.

463. The 'keep open notice' framework allows reporting entities to cooperate with agencies undertaking criminal investigations that involve one or more of their customers, while continuing to comply with their AML/CTF obligations.

464. The framework is also consistent with FATF recommendation 10 (detail contained in 10.20 of the FATF methodology) which requires that, in cases where reporting entities form a suspicion of money laundering or terrorism financing and they reasonably believe that performing the CDD process will tip-off the customer, they should be permitted not to pursue the CDD process and instead should be required to file a SMR.

465. Section 39B of the Act allows a 'senior member' (defined in subsection 39B(3) of the Act) of an agency (specified in subsection 39B(4) of the Act) (specified agency) to issue of a keep open notice directly to a reporting entity if the senior member reasonably believes that the provision of a designated service by the reporting entity to a customer would assist in the investigation by the agency of a 'serious offence' (defined in subsection 39B(2) of the Act).

466. The keep open notice framework replaces the regime prescribed in Chapter 75 of the former rules which allowed the AUSTRAC CEO to issue exemption notices to reporting entities for the same purpose.

467. A keep open notice will exempt a reporting entity from needing to comply with the customer due diligence obligations in sections 28, 30 and 26G of the Act in respect of the customer(s) specified in the keep open notice (section 39A of the Act).

468. Division 8 sets out technical requirements in relation to 'keep open notices'. Section 39A of the Act provides exemptions from initial customer due diligence, ongoing customer due diligence, and a reporting entity's compliance with its AML/CTF policies, to the extent that the reporting entity reasonably believes that compliance would or could reasonably be expected to alert the customer to the existence of a criminal investigation.

6-36—Senior member of agency—superintendent

469. Under section 39B of the Act, 'senior members' of federal, state and territory police forces and some other agencies listed in subsection 39B(4) may issue keep open notices.

470. Section 6-36 of the Rules prescribes that the position of superintendent of either the Australian Federal Police, or the police force or police service of a State or the Northern Territory is a 'senior member' for the purposes of subsection 39B(3) of the Act. Section 6-36 does not impose an administrative duty on a State officer; instead, it provides an administrative power that may be exercised by a State officer.

471. Accordingly and consistent with applications for exemptions under Chapter 75 of the former Rules, section 6-36 of the Rules authorises police superintendents to issue keep open notices, permitting decisions to be made by the member with the most relevant involvement, expertise and qualification to ensure operational efficiency of police investigations and operations, without the need to escalate approval for the issuing of keep open notices to agency heads, statutory office holders or SES equivalent officers or employees.

6-37—Prescribed agencies

472. Paragraph 39B(4)(g) of the Act allows for the Rules to prescribe additional Commonwealth, State or Territory agencies, 'senior members' of which are authorised to issue keep open notices.

473. Section 6-37 of the Rules is made pursuant to the enabling power in paragraph 39B(4)(g) of the Act and prescribes additional agencies that can issue a keep open notice pursuant to section 39B of the Act. The agencies prescribed in section 6-37 of the Rules are in addition to those agencies already listed in paragraphs 39B(4)(a) to (f) of the Act.

474. Section 6-37 of the Rules has prescribed the following additional agencies:
- the Independent Broad-based Anti-corruption Commission of Victoria;
- the Crime and Corruption Commission of Queensland.

475. Additional agencies, which undertake investigations of serious offences (defined in subsection 39B(2) of the Act), may be prescribed in the AML/CTF Rules in the future.

6-38—Form of keep open notice

476. Under subsection 39B(5) of the Act, a keep open notice must:
- be in the form prescribed by the AML/CTF Rules for the purposes of this paragraph; and
- contain such information, and be accompanied by such documents, as is required in the AML/CTF Rules.

477. Section 6-38 of the Rules is made for the purposes of paragraph 39B(5)(a) of the Act, and prescribes that Form 1 in Schedule 1 to the Rules is the form to be used when issuing keep open notices pursuant to subsection 39B(1) of the Act.

6-39—Information and documents required to be contained in or to accompany keep open notice

478. Section 6-39 of the Rules is made for the purposes of paragraph 39B(5)(b) of the Act, and prescribes the information to be contained in, and the documents which are required to accompany, a keep open notice issued to a reporting entity by a senior member of an agency mentioned in subsection 39B(4) of the Act. This list of prescribed information and documents mirrors the information contained in Form 1 in Schedule 1 to the Rules.

6-40—Extension notices

479. By default, under subsection 39B(6) of the Act, a keep open notice is in force for a period of up to 6 months.

480. If required, subsection 39B(7) of the Act provides that the period for which a keep open notice remains in force may be extended by a further 6 months where a senior member of the relevant agency issues an 'extension notice'.

481. As with a keep open notice, after being issued, an extension notice will also need to be sent to both the reporting entity and the AUSTRAC CEO under subsection 39C(2) of Act.

482. Subsection 39B(7) of the Act prescribes that an extension notice needs to be in the form prescribed by the Rules.

483. Section 6-40 is made for the purposes of subsection 39B(7) of the Act, and prescribes that Form 2 in Schedule 1 to the Rules is prescribed as the form to be used when issuing an extension notice.

6-41—Further extension application

484. Under subsection 39B(8) of the Act a specified agency can extend the application of a keep open notice twice under subsection 39B(7) of the Act, before an application needs to be made to the AUSTRAC CEO to further extend the application of a keep open notice.

485. Section 6-41 of the Rules is made for the purposes of paragraph 39B(8)(b) of the Act, and prescribes that Form 3 in Schedule 1 to the Rules is prescribed as the form to be used by a senior member when making an application to the AUSTRAC CEO to further extend the period that a keep open notice remains in force, following two previous

extension notice being issued under subsection 39B(7) of the Act by a senior member of an agency mentioned in subsection 39B(4) of the Act.

6-42—Initial customer due diligence—previous carrying out of applicable customer identification procedure

486. Section 6-42 of the Rules is a transitional provision giving regulatory relief to reporting entities regulated before 31 March 2026. It provides that a reporting entity is taken to have complied with its initial CDD obligations if it had already carried out its applicable customer identification procedure (ACIP) in relation to the customer prior to the commencement of these Rules. The section also provides relief where a reporting entity had previously carried out the ACIP in relation to the trustee of a customer—this recognises that under section 6-2 of the Rules, initial customer due diligence is undertaken for the trust estate rather than the trustee while previously ACIP applied to trustees.

6-43—Initial customer due diligence—service provided in a foreign country

487. Section 6-43 of the Rules is a transitional provision reporting entities that provide designated services at or through a permanent establishment in a foreign country. Such reporting entities have been subject to regulation under the AML/CTF Act since 2006, but were not subject to the requirement to undertake ACIP before commencing to provide designated services. The section provides that such a reporting entity is taken to have complied with its initial CDD obligations if:
    - The designated services being provided by the reporting entity is only at or through a permanent establishment of the reporting entity in a foreign country, and
    - Prior to the commencement of these Rules on 31 March 2026, the reporting entity was already complying with the equivalent CDD and record keeping laws in that foreign country and those laws gave effect to the FATF recommendations.

Part 7—Correspondent Banking

488. Part 7 of the Rules deals with the entry of a financial institution into a correspondent banking relationship and ongoing due diligence assessments. Part 7 replaces Chapter 3 of the former rules and is substantially the same.

Division 1— Due diligence assessment for entry into correspondent banking relationship

7-1—Requirements for due diligence assessment

489. Section 96 of the Act requires financial institutions to conduct due diligence assessments before entering into, and for the duration of, any correspondent banking relationship that will involve a vostro account. The financial institution must prepare a written record of the due diligence assessment within 10 business days after completing the assessment. The due diligence assessment will inform the senior officer of the

financial institution when they are considering whether to approve the financial institution's entry into a correspondent banking relationship.

490. Subsection 7-1(2) of the Rules requires a correspondent to assess the ML/TF, proliferation financing or other serious crime risks of a correspondent banking relationship when carrying out initial due diligence and ongoing due diligence assessments.

491. Subsection 7-1(3) of the Rules specifies the matters that must be considered by a correspondent when assessing the level of the ML/TF proliferation financing or other serious crime risk of the correspondent banking relationship on which it is carrying out due diligence. When assessing the risks, the correspondent may form the view that it is reasonable to consider additional matters when determining the level of that risk.

7-2—Matters to which a senior officer must have regard before giving approval

492. Paragraph 96(1)(b) of the Act prohibits a financial institution from entering into a correspondent banking relationship with another financial institution unless a senior officer of the financial institution approves the entering into of that relationship, having regard to such matters as are specified in the Rules.

493. Subsection 7-2(2) of the Rules requires the senior officer to have regard to the risks assessed and set out in the written record of the due diligence assessment, and if those risks can be managed and mitigated appropriately through the correspondent's AML/CTF program.

494. Payable-through accounts have a higher level of inherent ML/TF, proliferation financing or other serious crime risk as the accounts may be accessed directly by customers of the respondent financial institution. Subsection 7-3(3) of the Rules sets out the additional matters the senior officer must have regard to when deciding whether to approve the entry into the correspondent banking relationship if the correspondent is to maintain payable-through accounts.

Division 2—Requirements for ongoing due diligence assessments

7-3—Requirements for ongoing due diligence assessments

495. A due diligence assessment is a point-in-time assessment of the risks of a correspondent banking relationship. However, because risks change over time, subsection 96(3) of the Act requires a financial institution that has entered a correspondent banking relationship to periodically carry out due diligence assessments. Section 7-3 of the Rules requires that the correspondent must carry out the ongoing due diligence assessments to reassess the ML/TF proliferation financing or other serious crime risks of that correspondent banking relationship having regard to the matters set out in subsection 7-1(3).

7-4—Timing of ongoing due diligence assessments

496. Section 7-4 of the Rules prescribes the frequency of ongoing due diligence assessments where a financial institution is in a correspondent banking relationship with another financial institution that involves a vostro account.

497. Subsection 7-4(2) requires, that a correspondent must carry out a due diligence assessment at a time determined appropriate by the correspondent, based on its consideration of the ML/TF, proliferation financing or other serious crime risks, associated with the correspondent banking relationship and any material changes in respect of those risks. In any event, a due diligence assessment of the correspondent banking relationship must be conducted by the correspondent at least once every two years.

Part 8—Transfers of value

498. Sections 64, 65 and 66 of the Act set out the obligations of ordering institutions, beneficiary institutions and intermediary institutions, respectively, relating to transfers of value. Section 66A of the Act sets out specific requirements for ordering institutions and beneficiary institutions in relation to transfers of virtual assets. These obligations are commonly referred to as the 'travel rule'.

499. Section 63A of the Act provides that whether a person is an ordering institution or a beneficiary institution is to be determined in accordance with the Rules (subsections 63A(1) and 63A(5) of the Act).

500. Part 8 of the Rules:
- prescribes circumstances for determining whether a person is an ordering institution or a beneficiary institution; and
- contains requirements for the passing on of certain information in relation to instructions for the transfer of value. Different requirements apply depending on whether an 'ordering institution', 'beneficiary institution', or 'intermediary institution' is involved.

Division 1—Ordering institutions and beneficiary institutions

501. Division 1 of the Rules comprises:
- Section 8-1—Determination of who is an ordering institution; and
- Section 8-2—Determination of who is a beneficiary institution.

502. Section 8-2 of the draft Rules provides for the determination of who is a beneficiary institution under the enabling power of subsection 63A(5) of the Act.

8-1—Determination of who is an ordering institution

503. Section 8-1 of the Rules provides the criteria for determining who is an ordering institution under the subsections 63A(1) and (2) of the Act for the purposes of a transfer of value.

504. Subsection 8-1(2) of the Rules establishes the fundamental principle that a person is an ordering institution if they accept *an instruction* for a transfer of value on behalf of a payer. The subsection also clarifies that to be an ordering institution a person must accept the instruction in the course of carrying on a business.

505. Subsection 8-1(2) must be read together with section 63A of the Act, which includes a range of exceptions as to who is an ordering institution—most notably a person who transfers value in circumstances where the transfer is reasonably incidental to the provision of another service (with some specific exclusions from this exception).

506. Paragraphs 8-1(3)(a) to (d) of the Rules set out non-exhaustive circumstances in which a person may be an ordering institution.

507. Subsection 8-1(4) of the Rules clarifies that these circumstances do not affect the fundamental requirement for a person to satisfy subsection 8-1(2) of the Rules to be an ordering institution.

Circumstances in which a person may be an ordering institution under subsection 8-1(2) of the Rules

508. Paragraph 8-1(3)(a) of the Rules prescribes the following circumstance: the person receives the value that is to be transferred from the payer or a person acting on behalf of the payer.

509. Non-exhaustive examples of this circumstance would include:

Example 1: A customer provides cash or virtual assets or value in the form of property such as gold bullion over the counter to a remitter, financial institution or virtual asset service provider to fund a value transfer (whether or not the transfer of value is international or domestic).

Example 2: A customer transfers value to a remitter from an account with a financial institution, and the customer separately instructs the remitter to transfer the value (whether or not the transfer of value is international or domestic). Note, in this circumstance, the customer instructing the financial institution to transfer value from the customer's account with the financial institution to the remitter will likely be a separate transfer of value, unless there is a special arrangement between the financial institution and the remitter to facilitate the provision of value transfer services, for example, as part of white label services provided by a financial institution using a global remittance network as the payment rails.

Example 3: A customer of a casino surrenders gaming chips in Australia and requests that the casino transfer the value of those chips to a bank account in another country (note, the incidental value transfer exception does not apply to gambling services due to this being an international value transfer).

Example 4: A customer transfers value from a foreign bank account to a casino's foreign bank account and instructs the casino to make gaming chips available in Australia (note, the incidental value transfer exception does not apply to gambling services due to this being an international value transfer).

Example 5: A customer provides Australian dollars to a currency exchange business in Australia and instructs the currency exchange business to make foreign currency available in another country (note, the incidental value transfer exception does not apply to currency exchange services due to this being an international value transfer).

510. Paragraph 8-1(3)(b) of the Rules prescribes the following circumstance: the person holds the value to be transferred in an account provided to the payer or otherwise on deposit from the payer (including in a virtual asset wallet).

511. Non-exhaustive examples of this circumstance include:

Example 1: A customer instructs a financial institution to transfer value held in the customer's account with the financial institution.

Example 2: A customer instructs a virtual asset service provider to transfer virtual assets held in a custodial virtual asset wallet provided by the virtual asset service provider, whether or not the transfer is to another custodial virtual asset wallet or a self-hosted wallet.

Example 3: A customer instructs a provider of digital wallets (including a digital wallet that holds monetary value) to transfer value pre-loaded into the wallet.

512. Paragraph 8-1(3)(c) of the Rules prescribes the following circumstance: the person is authorised under an arrangement with the payer to transfer the value from a third-party deposit-taker or credit provider.

513. A non-exhaustive example of this circumstance is where the customer instructs a digital wallet provider to transfer value where the digital wallet provider has an arrangement with the customer to draw the value from an account held with a financial institution (including a credit card account).

514. However, the requirement for there to be an arrangement between the ordering institution and the payer authorising the transfer from a third party is not intended to make the merchant acquirer the ordering institution for credit card payments through merchant terminals—there is no direct authorising arrangement between the merchant acquirer and the payer. Instead, the card issuer would be the ordering institution in this circumstance because it accepts the instruction to transfer value from a credit card account.

515. Paragraph 8-1(3)(d) of the Rules prescribes the following circumstance: the person arranges for the transfer of value from the payer under an offsetting arrangement with the beneficiary institution.

516. A non-exhaustive example of this circumstance would be hawala or informal remittance arrangements, under which the ordering institution may arrange for a customer seeking to transfer value to an unrelated third party payee seeking to receive value under an unrelated transfer. When combined with a reciprocal arrangement by the beneficiary institution between other parties seeking to transfer and receive value, the combination of offsetting transfers results in the intended transfers of value from the customer to the intended payee. Under such scenarios it is not necessary that the ordering institution ever receive the value to be transferred or handle it directly.

8-2—Determination of who is a beneficiary institution

517. Section 8-2 of the Rules provides for the determination of who is a beneficiary institution under the enabling power of subsection 63A(5) of the Act for the purposes of a transfer of value.

518. Subsection 8-2(2) of the Rules establishes the fundamental principle that a person is a beneficiary institution if they make the value transferred, in relation to the transfer of value, available to payee or a person acting on behalf of the payee. To be a beneficiary institution, the person must make the value available in the course of carrying on a business.

519. Subsection 8-2(2) of the Rules must be read together with section 63A of the Act, which includes a range of exceptions as to who is a beneficiary institution, most notably a person who makes value available in circumstances where making the value available is reasonably incidental to the provision of another service (with some specific exclusions from this exception).

520. Subsection 8-2(3) of the Rules prescribes the circumstances in which a person may be a beneficiary institution under subsection 8-2(2).

521. Subsection 8-2(4) of the Rules prescribes that the circumstances identified in paragraphs 8-2(3)(a) to (d) do not affect the requirement for a person to satisfy subsection 8-2(2) to be a beneficiary institution.

Circumstances in which a person may be a beneficiary institution under subsection 8-2(2) of the Rules

522. Paragraph 8-2(3)(a) of the Rules prescribes the following circumstance: the person makes the transferred value available to the payee directly, or to a person acting on behalf of the payee

523. Non-exhaustive examples of this circumstance include:

Example 1: A remitter, financial institution or VASP provides transferred cash, virtual assets or value in the form of property such as gold bullion over the counter to the customer (whether or not the transfer of value is international or domestic).

Example 2: A casino provides gaming chips to a customer in Australia after the customer transfers value from a foreign bank account to a casino's foreign bank account (note, the incidental value transfer exception does not apply to gambling services due to this being an international value transfer).

Example 3: A currency exchange business provides foreign currency to a customer in a foreign country after the customer provided Australian dollars to the currency exchange business in Australia (note, the incidental value transfer exception does not apply to currency exchange services due to this being an international value transfer).

524. Paragraph 8-2(3)(b) of the Rules prescribes the following circumstance: the person makes the transferred value available to the payee by depositing the value into an account held by the payee with the person (including in a virtual asset wallet), or otherwise holding the value on deposit for the payee.

525. Non-exhaustive examples of this circumstance include:

Example 1: A financial institution credits transferred money to the customer's account.

Example 2: A VASP holds the transferred virtual assets in a custodial wallet.

Example 3: A digital wallet provider credits the transferred money to the customer's digital wallet.

526. Paragraph 8-2(3)(c) of the Rules prescribes the following circumstance: the person makes the transferred value available to the payee, under an arrangement with the payee, by depositing the value with a third party deposit-taker or credit provider.

527. Non-exhaustive examples of this circumstance include:

Example 1: A remitter makes value available to a customer by depositing it in the customer's account with a financial institution (whether or not the transfer of value is international or domestic). Note, in this circumstance, the remitter instructing its own financial institution to transfer value to the customer's account with a financial institution will likely be a separate transfer of value, unless there is a special arrangement between the remitter and financial institution to facilitate the provision of value transfer services, for example, as part of white label services provided by a financial institution using a global remittance network as the payment rails.

Example 2: A casino deposits money from its foreign bank account into the foreign bank account of the customer to make available the value of gaming chips that the

customer surrendered in Australia (note, the incidental value transfer exception does not apply to gambling services due to this being an international value transfer).

528. Paragraph 8-2(3)(d) of the Rules prescribes the following circumstance: the person arranges for the transferred value to be made available to the payee under an offsetting arrangement with the ordering institution.

529. A non-exhaustive example of this circumstance would be hawala or informal remittance arrangements, under which the beneficiary institution may arrange for an unrelated third party payer to transfer value to the payee customer. When combined with a reciprocal arrangement by the ordering institution between the payer and a third party payee, the combination of offsetting transfers results in the intended transfers of value from the payer to the intended payee customer. Under such scenarios it is not necessary that the beneficiary institution ever receive the value to be transferred or handle it directly.

Division 2—Transfers of value

530. The requirements in Part 8 of the Rules have been drafted to align with FATF recommendations 15 and 16. These recommendations set out the minimum information that needs to be collected, verified and passed on in a transfer of value about both the payer and payee, and the responsibilities for the ordering, intermediary and beneficiary institutions in a value transfer chain in relation to that information. FATF recommendation 16 sets out information that needs to travel with the transfer of value to provide payment transparency and aid traceability and preventative measures such as sanctions screening and financial crime monitoring. FATF recommendation 15 extends the requirement, with some specific requirements, to transfers for virtual assets.

531. The new sections, 8-3 to 8-5 of the Rules, establish the minimum information that is required to be collected, verified and passed on in a transfer of value.

8-3—Obligations of ordering institutions – collecting, verifying and passing on information

532. Paragraph 64(2)(a) of the Act prescribes an ordering institution must collect the information specified in the Rules before passing on a transfer message for the transfer of value, or otherwise giving effect to the transfer of value.

533. Paragraph 64(2)(b) Act prescribes an ordering institution must verify the information specified in the Rules before passing on a transfer message for the transfer of value, or otherwise giving effect to the transfer of value.

534. Subsection 64(3) Act prescribes that if the ordering institution and the beneficiary institution in the transfer of value are not the same person, the ordering institution must pass on the information specified in the Rules relating to the transfer of value to the next institution in the value transfer chain.

535. The table in section 8-3 of the Rules must be read together with:
    - the designated service in item 29 of table 1 in section 6 of the Act, and
    - section 64 of the Act, which sets out the requirement for the ordering institution to collect, verify and pass on information when providing value transfer services.

536. The table in section 8-3 of the Rules must also be read together with the definitions of the following terms in section 1-4 of the Rules:
    - payer information
    - tracing information
    - merchant payment
    - BECS
    - BPAY
    - DEFT

537. Column 1 of the table in section 8-3 of the Rules describes a range of circumstances in which ordering institutions provide value transfer services. These obligations to collect, verify and pass on information will differ depending on the circumstance in which the ordering institution provides the value transfer service. The default circumstance is set out in item 1 of the table, which applies unless one of the special circumstances listed in other items of the table apply.

538. Column 2 of the table sets out the information that an ordering institution must collect before passing on a transfer message for the transfer of value, or otherwise giving effect to the transfer of value. The ordering institution is required in all circumstances to collect payer information and the payee's full name for any value transfer service, whether domestic or international, unless the designated service is a merchant payment or a refund of a merchant payment. In these circumstances the ordering institution (i.e. the card issuer for a merchant payment and the merchant acquirer for the refund of a merchant payment) is not required to collect payer and payee's full name.

539. Column 3 of the table sets out information that an ordering institution must verify passing on a transfer message for the transfer of value, or otherwise giving effect to the transfer of value. In all circumstances, except those involving merchant payments, an ordering institution must verify payer information, i.e. information related to the ordering institution's own customer. The definition of 'payer information' provides a number of options for ordering institutions, allowing for some flexibility in which information an ordering institution verifies. 'Payer information' substantively reproduces the previous concept of 'complete payer information' in the former section 71 of the Act.

540. Column 4 of the table sets out the information that if the ordering institution and the beneficiary institution in the transfer of value are not the same person, the ordering institution must pass on to the next institution in the value transfer chain. Consistent with FATF recommendations 15 and 16, item 1 of the table requires that an ordering

institution must pass on payer information, the payee's full name and the tracing information to another institution in a value transfer chain, unless one of the special circumstances in the other items in the table applies. Those special circumstances recognise that certain payment systems have technical limitations that prevent the passing on of payer information and payee information:

- legacy payment systems such as BECS, which may be used for domestic payments or for a domestic 'link' in an incoming international value transfer chain—only tracing information needs to be passed on,
- lower risk limited purpose domestic payment systems such as BPAY and DEFT—only tracing information needs to be passed on,
- merchant payments, refunds of merchant payments and withdrawals of money from ATMs—only the card number needs to be passed on from the ordering institution to the beneficiary institution (which substantively maintains the requirement in the former section 67(2) of the Act).

541. The tracing information need not be unique to the payer/ordering institution or payee/beneficiary institution. If, for example, a single piece of information, such as a series of numbers, letters, symbols and characters, allows both the ordering institution and the beneficiary institution to identify the payer's account and the payee's account respectively, it could satisfy the requirement for 'tracing information'.

542. It should be noted that 'push payments' initiated by the issuer of the debit, credit or prepaid card on the instruction of the card holder are covered by the default requirement in item 1 of the table, unless they are a refund of a merchant payment.

543. Where an ordering institution transfers value to a self-hosted wallet, only the collection and verification requirements are engaged since there is no beneficiary institution to which to pass on information.

8-4—Obligations of beneficiary institutions – monitoring for receipt of information

544. Paragraph 65(2)(a) of the Act requires that a beneficiary institution must take reasonable steps to monitor whether it has received the information specified in the Rules relating to the transfer of value and whether the information received about the payee (that is, the beneficiary institution's customer) is accurate.

545. The Explanatory Memorandum to the *Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2024* at paragraph 643 makes clear that '[i]n recognition of the volume of value transfers, this obligation is restricted to "reasonable steps", which could include sampling of transfer messages and other assurance activities, as opposed to reviewing every transfer message individually'. The table in section 8-4 of the Rules must be read together with the definitions referred to in the notes on section 8-3 of the Rules, as well as the designated service in item 30 of table 1 in section 6 of the Act.

546. Column 1 of the table in section 8-4 of the Rules describes a range of circumstances in which beneficiary institutions provide value transfer services. These obligations to monitor for missing or inaccurate information will differ depending on the circumstance in which the ordering institution provides the value transfer service. The default circumstance is set out in item 1 of the table, which applies unless one of the special circumstances listed in other items of the table apply.

547. Column 2 of the table in section 8-4 of the Rules sets out the information that a beneficiary institution must take reasonable steps to monitor for. Consistent with FATF recommendations 15 and 16, item 1 of the table requires that beneficiary institutions take reasonable steps to monitor for payer information, the payee's full name and tracing information unless specified in one of the circumstances in items 2, 4, 5, 6 or 7 of the Table apply.

548. Those special circumstances recognise that certain payment systems have technical limitations that prevent the passing on of payer information and the payee's full name:
- legacy payment systems such as BECS, which may be used for domestic payments or for a domestic 'link' in an incoming international value transfer chain—a beneficiary institution is only required to take reasonable steps to monitor for tracing information,
- lower risk limited purpose domestic payment systems such as BPAY and DEFT—a beneficiary institution is only required to take reasonable steps to monitor for tracing information,
- merchant payments and refunds of merchant payments— a beneficiary institution is only required to take reasonable steps to monitor for the card number (which substantively maintains the requirement in the former section 67(2) of the Act).

549. It should be noted that 'push payments' using debit, credit or prepaid cards are covered by the default requirement in item 1 of the table unless they are a refund of a merchant payment.

550. Furthermore, it should be noted that under subsection 66A(6) of the Act, a beneficiary institution that receives a transfer of virtual assets must receive or otherwise obtain the payer, the payee's full name and tracing information before making the virtual assets available to the payee. The only exception is set out in subsection 66A(10) of the Act, which is only applicable in a value transfer chain scenario. For transfers received from self-hosted wallets, a beneficiary institution will necessarily be required to 'otherwise obtain' the payer information, the payee's full name, e.g. by requesting this information from its customer, the payee.

8-5—Obligations of intermediary institutions—monitoring for receipt of information and passing on information

551. Section 66 of the Act requires an intermediary institution to take reasonable steps to monitor whether it has received the information specified in the Rules relating to the

transfer of value, and to include information specified in the Rules when passing on a transfer message. The Explanatory Memorandum to the *Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2024* (accessible at https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query%3DId%3A%22legislation%2Fbillhome%2Fr7243%22;rec=0) at paragraph 650 makes clear that *'[i]n recognition of the volume of value transfers, this obligation is restricted to "reasonable steps", which could include sampling of transfer messages and other assurance activities, as opposed to reviewing every transfer message individually'*.

552. The table in section 8-5 of the Rules must be read together with the definitions of the following terms in section 1-4 of the Rules:
    - payer information
    - tracing information
    - merchant payment
    - BECS
    - BPAY
    - DEFT

    as well as the designated service in item 31 of table 1 in section 6 of the Act.

553. Column 1 of the table describes a range of circumstances in which intermediary institutions pass on transfer messages. The obligations to monitor for missing, and to pass on information, will differ depending on the circumstance in which the intermediary institution provides the value transfer service. The default circumstance is set out in item 1 of the table, which applies unless one of the special circumstances listed in other items of the table apply.

554. Column 2 of the table sets out the information that an intermediary institution must take reasonable steps to monitor for. Unlike a beneficiary institution, an intermediary institution is not required to monitor for the accuracy of information it receives (although obviously fictitious or false information, among other things, may give rise to a suspicious matter reporting obligation if detected). Consistent with FATF recommendations 15 and 16, item 1 of the table requires that intermediary institutions take reasonable steps to monitor for payer information, the payee's full name and tracing information unless one of the circumstances in items 2, 4, 5 or 6 of the Table apply.

555. Those special circumstances recognise that certain payment systems have technical limitations that prevent the passing on of payer information and the payee's full name:
    - legacy payment systems such as BECS, which may be used for domestic payments—an intermediary institution is only required to take reasonable steps to monitor for tracing information,

- lower risk limited purpose domestic payment systems such as BPAY and DEFT—an intermediary institution is only required to take reasonable steps to monitor for tracing information,
- merchant payments and refunds of merchant payments—an intermediary institution is only required to take reasonable steps to monitor for the card number.

556. 'Push payments' initiated by the issuer of the debit, credit or prepaid card on the instruction of the card holder are covered by the default requirement in item 1 of the table.

557. Item 6 of the table recognises that where an intermediary institution receives a transfer message related to an international value transfer, which it passes on through BECS to the beneficiary institution, it may be required to strip the payer information payee's full name off the transfer message and only pass on tracing information. The intermediary institution must still monitor for receipt of the payer information and the payee's full name in these cases and keep a record of it (section 107 of the Act). The intermediary institution must also make any information that it is required to pass on under column 2 to another institution in the value transfer chain (e.g. the beneficiary institution) as soon as practicable upon request (section 66(5) of the Act).

8-6—Payment transparency—transition to revised FATF Recommendations

558. Section 8-6 sets out an alternative way that an institution in a value transfer chain can fulfil obligations related to the collection, verification, passing on and monitoring of payer information and the payee's full name. In June 2025, the FATF revised recommendation 16 to change the content of 'travel rule' information in relation to the payer and the payee.

559. Global transition to the requirements of the revised recommendation 16 will take some years due to the cross-border nature of travel rule requirements and the necessity for amending standardised transfer message formats such as ISO20022 used by global messaging systems such as the Society for Worldwide Interbank Financial Telecommunication payment delivery system (Swift). For the financial sector, the FATF envisages this occurring in 2030.

560. However, given that some reporting entities (particularly remitters and VASPs newly subject to travel rule obligations) may operate within more contained payment ecosystems or even have bilateral arrangements with counterparties, they may wish to build new systems to the new standard.

561. Permitting implementation of the revised FATF recommendation 16 will also ensure that if financial institutions move at different rates to implement updated messaging formats that Australian financial institutions will not be required to treat incoming messages in the new format as lacking required information. For example, the revised

recommendation 16 removes the requirement for payer information to include both date *and place* of birth, replacing it instead with the payer's date of birth (if an individual) and business or residential address.

562. Section 8-6 does not, however, permit reporting entities to pick and choose between using the old standard for one element of the travel rule information and the revised standard for another. If a reporting entity chooses to use the revised recommendation 16 related to information about the payer, it must also use the revised recommendation 16 related to information about the payee.

Division 3—Exemptions from obligations relating to transfers of value

563. Division 3 of Part 8 of the Rules contains section 8-7 and section 8-8 of the Rules, which have been made for the purposes of paragraphs 67(1)(a) and 67(1)(b) of the Act respectively, to exempt certain transfers of value that occur in specified circumstances from the requirements in Part 5 of the Act.

8-7—Exemptions—designated services provided at or through foreign permanent establishments

564. Obligations relating to transfers of value under the AML/CTF Act apply to all reporting entities, including those providing designated services at or through a permanent establishment in a foreign country.

565. This will mean that some reporting entities will be involved in value transfer chains that related to transfers of value within the borders of a single foreign country and which may be subject to reduced domestic travel rule obligations (such as *de minimis* thresholds, reduced travel rule information requirements etc.) that nonetheless comply with the FATF standards. The FATF standards also recognise transfers within the European Economic Area as domestic transfers.

566. Section 8-7 seeks to reduce conflicts of laws by providing that the 'travel rule' obligations in Part 5 of the AML/CTF Act do not apply to transfers of value within a single foreign country, or within the European Economic Area, where the reporting entity complies with the applicable laws implementing the FATF recommendations in that place.

567. Transfer of virtual assets are not within the scope of this exemption. Such transfers are all to be treated as international transfers under recommendation 15, and subject to full travel rule obligations.

8-8—Exemptions –transfers of value occurring in specified circumstances

568. Subsection 8-8(1) of the Rules states that section 8-8 of the Rules is made for the purposes of paragraph 67(1)(b) of the Act.

569. Section 67 of the Act allows for Rules to specify exemptions to 'travel rule' obligations under Part 5 of the Act. A number of exceptions formerly in the Act prior to the 2024 amendments have been substantively reproduced in exemptions set out section 8-8 the Rules.

Inter-financial institution transfers

570. Subsection 8-8(2) of the Rules substantially reproduces the exemption which was in the former subsection 67(5) of the Act and exempts transfers of value from the travel rule where both the payer and payee are financial institutions acting on their own behalf. Such transfers, which include settlement payments, are internationally recognised as lower risk (see the Interpretive Note to FATF recommendation 16).

571. Subsection 8-8(3) of the Rules extends the exemption for transfers between financial institutions acting on their own behalf. Differences between the Act definition of 'financial institution' and a broader definition of 'supervised financial institution'—that applies to payments effected through Swift—has led to friction in Australian banks' implementation of the travel rule. Subsection 8-8(3) of the Rules recognises the broader Swift definition for transfers of value through Swift.

Cheques

572. Subsection 8-8(4) of the Rules substantively reproduces the exemption formerly in subsection 67(3) of the Act for instructions given by way of a cheque. However, given the AML/CTF Amendment Act 2024 extended the application of the travel rule beyond financial institutions to include remitters and VASPs, the exemption has been clarified to apply where the instruction for the transfer of value is given to the ordering institution by way of a cheque and the cheque is drawn on the ordering institution. This ensures, for example, that an instruction undertaken through a remitter or VASP that is funded by a cheque will not fall within the exemption and the travel rule will continue to apply.

Merchant payments —ordering institution obligations

573. Subsection 8-8(5) of the Rules exempts merchant payments and refunds of merchant payments from aspects of the travel rule, namely the requirement for the ordering institution to collect and verify payer information and to make such information available to another institution in the value transfer chain upon request.

574. 'Merchant payment' is defined in section 1-4 (Definitions) of the Rules and is the term is discussed in the notes on that definition.

575. This exemption supports items 4 and 5 in the table in section 8-3 of the Rules. It should be noted, however, that this exemption is restricted to travel rule obligations and all other AML/CTF obligations, including customer due diligence under Part 2 of the Act,

will apply in connection with any designated services related to debit cards, credit cards and stored value cards.

576. This 'merchant payment' exemption substantially replaces the exemptions that were in the former subsection 67(4A) (Merchant terminals) of the Act.

Pre commencement customers—ordering institution obligations

577. Subsection 8-8(6) exempts reporting entities from the obligation to verify payer information when accepting an instruction as an ordering institution from a pre-commencement customer. This recognises that reporting entities will not hold verified information about pre-commencement customers, who were customers of reporting entities before the commencement of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*. Pre-commencement customers are subject to special monitoring obligations under sections 30 and 36 of the Act.

578. This exemption is, however, conditional on there being no reasonable grounds to have doubts about the adequacy or veracity of the pre-commencement customer's payer information. If such reasonable grounds exist, this will trigger the requirement to review, update and, where appropriate, reverify KYC information about the pre-commencement customer under subparagraph 30(2)(c)(i) of the Act. Such reasonable grounds may also trigger the requirement to undertake initial CDD in relation to the pre-commencement if a suspicious matter reporting obligation arises.

Certain existing customers—ordering institution obligations

579. Subsection 8-8(7) exempts reporting entities from the obligation to verify payer information when accepting an instruction as an ordering institution from a customer that has been subject to the former Applicable Customer Identification Procedure or foreign equivalent before 31 March 2026. This is a transitional exemption, recognising that while reporting entities hold verified KYC information about such payers, many have not built systems to allow them to determine which elements of KYC information have been verified since the AML/CTF Act came into effect in 2007, nor to feed such information into their payments processing systems.

580. This exemption is, however, conditional on there being no reasonable grounds to have doubts about the adequacy or veracity of the customer's payer information. If such reasonable grounds exist, this will trigger the requirement to review, update and, where appropriate, reverify KYC information about the customer under subparagraph 30(2)(c)(i) of the Act.

581. This exemption will cease to operate from 1 July 2030, by which time reporting entities will need to have built the required systems to ensure that payer information passed on with value transfers is verified.

Transfers to a self-hosted virtual asset wallet

582. Subsection 8-8(8) of the Rules exempts transfers of virtual assets to self-hosted virtual asset wallets from certain obligations for the ordering institution to pass on and make available travel rule information. This exemption supports item 6 in the table in section 8-3 of the Rules.

583. It should be noted that exemptions to reports of IVTS under section 46 of the Act—as distinct from the travel rule obligations under Part 5 of the Act—will be considered as part of future Rules development.

584. A reconciliation of the exemptions in the former section 67 of the Act with the exemptions in section 76 of the Rules is contained in the table below:

Type of exemption	**Provision in the former section 67 of the AML/CTF Act** ***(only applied to electronic funds transfer (EFTI) instructions)***	**Approximate equivalent(s) provision(s) in the Rules** ***(more broadly now applies to 'transfers of value')***
Approved third-party bill payment systems	Subsection 67(1) of the AML/CTF Act ***Note:*** *this was an exemption from the requirements of Part 5 of the AML/CTF Act.*	• Item 2 in the table in section 8-3 of the Rules *(Obligations of ordering institutions – collecting, verifying and passing on information);* • Item 2 in the table in section 8-4 of the Rules *(Obligations of beneficiary institutions – monitoring for receipt of information);* • Item 2 in the table in section 8-5 of the Rules *(Obligations of intermediary institutions – monitoring for receipt of information and passing on information).* ***Note:*** *Rather than being an outright exemption, the Rules*

		clarify what information needs to be included in transfer messages passed on through one of the named third-party bill payment systems
Use of debit cards and credit cards, including at a branch of a financial institution	Subsection 67(2) of the AML/CTF Act	Some of these payments are more broadly covered by the "merchant payment" exemption in subsection 8-8(5) of the Rules • Items 4, 5 and 6 in the table in section 8-3 of the Rules *(Obligations of ordering institutions – collecting, verifying and passing on information);* • Item 4, 5 and 6 in the table in section 8-4 of the Rules *(Obligations of beneficiary institutions – monitoring for receipt of information);* • Item 4, 5 and 6 in the table in section 8-5 of the Rules *(Obligations of intermediary institutions – monitoring for receipt of information and passing on information).* ***Note:*** *Rather than being an outright exemption from all obligations, the Rules clarify what information needs to be verified (for ATM withdrawals), and included in transfer messages related to these kinds of transfers of value*
ATMs	Subsection 67(4) of the AML/CTF Act	
Merchant terminals	Subsection 67(4A) of the AML/CTF Act	

Cheques (where the cheque is drawn on the ordering institution)	Subsection 67(3) of the AML/CTF Act	Subsection 8-8(4) of the Rules
Inter-financial institution transfer	Subsection 67(5) of the AML/CTF Act	Subsections 8-8(2) and 8-8(3) (Swift) of the Rules

Division 4—International value transfer services

585. Part 8, Division 4 of the Rules contains the new section 8-9 of the Rules.

8-9—When is value in a country?

586. Section 8-9 of the Rules is made for the purposes of subsection 45(2) of the Act, which allows for Rules to be made specifying when value is in a country.

587. While such Rules will be most relevant to reports of IVTS reporting, the concept is also used in describing circumstances relevant to travel rule obligations for ordering institutions, beneficiary institutions and intermediary institutions in the tables in sections 8-3, 8-4 and 8-5 of the Rules.

588. The circumstances set out in section 8-9 of the Rules—prescribing when value is in a country—reflect the circumstances in which persons are ordering institutions and beneficiary institutions. In most circumstances, the country of the permanent establishment at or through which the ordering institution or beneficiary institution provides the value transfer service determines where the value is. Focusing on the permanent establishment of the service provider avoids the problem of many forms of value (for example, virtual assets), not having an inherent physical location.

589. Rules related to reports of IVTS will be developed in future.

Part 9—Reporting

590. Part 9 of the Rules provides detail in relation to various reporting obligations a reporting entity has under the Act.

Division 1—Suspicious matter reports

591. Subsection 41(1) of the Act provides that a suspicious matter reporting obligation arises for a reporting entity in the circumstances specified under that subsection. Subsection 41(2) of the Act requires that a reporting entity give the AUSTRAC CEO a report about the suspicious matter (SMR) within the time frames specified in that section.

592. Part 9, Division 1 of the Rules are made for the purposes of paragraph 41(3)(b) of the Act to prescribe the information that must be contained in a SMR made under subsection 41(2) of the Act. Sections 9-1 to 9-4 of the Rules will replace Chapter 18 of the former rules. Fundamentally, the types of information required to be included in a SMR remains similar.

593. The reportable details prescribed in Chapter 18 of the former rules have been reviewed and amended to better align them with the language and concepts used in the reformed AML/CTF regime – such as those relating to KYC information and the new CDD obligations. In addition, the prescribed reportable details for a SMR have been revised to recognise the new types of designated services which will be regulated under the Act, and updated to reflect technology and service delivery advancements.

594. Paragraph 41(3)(a) of the Act provides that a SMR given under subsection 41(2) must be in the approved form. Reportable details prescribed in sections 9-2 to 9-4 of the Rules will be incorporated into an 'approved form' referenced in paragraph 41(3)(a) of the Act, which a reporting entity must use when giving a SMR to AUSTRAC. Section 244 of the Act additionally prescribes that a report to the AUSTRAC CEO under the Act must be signed by the person or otherwise authenticated by the person in an approved way, or given to the AUSTRAC CEO either in the manner set out in section 28A of the *Acts Interpretation Act 1901* or in such other manner and form as is approved in relation to the person or a class of persons.

9-1—Purpose of this Division

595. Section 9-1 of the Rules states the purpose of Part 9, Division 1 of the Rules, which is to prescribe the reportable details for a SMR required to be made for the purposes of subsection 41(2) of the Act. The enabling power to prescribe the reportable details for a SMR is in paragraph 41(3)(b) of the Act.

596. The sections in Division 1 of Part 9 of the Rules are subject to Reportable details transitional arrangements in sections 12-1 and 12-2 of Part 12 of the Rules. Those sections apply as follows:
- new reportable details (contained in these Rules) don't commence until 1 July 2026, and
- any entity on the Reporting Entities Roll at 30 March 2026 can continue to report on the old reportable details (but can choose to report via the new reportable details) until 30 March 2029.

9-2—Reports of suspicious matters – general information

597. Section 9-2 of the Rules prescribes the general information that a reporting entity must include in a SMR made under subsection 41(2) of the Act. This includes:
- the reporting entity's full name and identifier assigned to it by AUSTRAC (paragraph 9-2(1)(a))

- the date the report is given to the AUSTRAC CEO (paragraph 9-2(1)(b))
- the date the SMR obligation arose for the reporting entity (paragraph 9-2(1)(c))
- whether paragraph 41(2)(aa) of the Act applies in relation to the report (whether the reporting entity availed themselves of the time extension applicable for certain circumstances relating to legal professional privilege) (paragraph 9-2(1)(d))
- the date any previous report was made to the AUSTRAC CEO which is relevant to the suspicious matter being reported (subparagraph 9-2(1)(e)(i)) and the identifier given to the previous report by AUSTRAC (if any) (subparagraph 9-2(1)(e)(ii))
- the full name, position and contact details of the individual completing the report (subsection 9-2(2))
- the full name, position and contact details of an individual who can provide information about the reporting entity forming the suspicion (subsection 9-2(3))
- information about any report the reporting entity has made to Commonwealth, State or Territory agencies which relates to the suspicious matter, and details of the part or unit and staff member within that agency the matter was reported to (subsection 9-2(4)).

598. The reference to 'a report it has previously given to the AUSTRAC CEO' in paragraph 9-2(1)(e) of the Rules includes any of the following: SMR, TTR, and reports of IVTS (or its predecessor, international funds transfer instruction report, if applicable). Reporting entities may exercise their discretion in assessing the relevance of previous reports. However, where a previous report involved a person that is either suspected or determined to be the first person in the impending SMR, that previous report should be referenced. Similarly, where a previous report includes the same account, property, product or instrument that is present in the impending SMR, that previous report should be referenced.

599. For the purposes of providing details for subsection 9-2(3) of the Rules (individual who can provide information about the reporting entity forming the suspicion), this should be taken to mean an individual who was centrally involved in the formation or substantiation of the suspicion. Although multiple people may be involved in the formation of a suspicion which is subsequently reported to AUSTRAC by the reporting entity, the information should only be provided on an individual who had a materially significant role in the formation of the suspicion, such as conducting enhanced due diligence measures on the relevant customer or reviewing transactions or behaviours identified through ongoing CDD. Where no one individual had a greater role than any other person in forming the suspicion, reporting entities should provide the details of the individual who is accountable for the business unit of the reporting entity that takes carriage of decision making in respect of SMR obligations.

9-3—Reporting of suspicious matters – information about persons

600. Section 9-3 of the Rules prescribes information a reporting entity must include in a SMR in relation to a person who is the subject of the suspicious matter, split by whether the person is an individual or non-individual. The information in both subsections 9-3(1) and 9-3(2) of the Rules is reportable to the extent they are applicable and known to the reporting entity (subsection 9-3(3) of the Rules).

601. Subsection 9-3(1) of the Rules prescribes the 'reportable information' in relation to a person who is an individual. This list of information is generally self-evident, however for the avoidance of doubt, paragraph (p) requires a physical description of the individual and a statement whether there are photographs or video (such as CCTV) held by the reporting entity of the individual, only where the identity of the individual had not been established by the reporting entity (such as if the individual was only a prospective customer making enquiries about designated services).

602. For the purposes of paragraphs 9-3(1)(b) and 9-3(2)(b) of the Rules (other names used by the person), other names of the person include:
    - business names that the individual is trading under in the capacity of a sole trader
    - previous given or surnames which may have legally changed (for example, through marriage or deed poll)
    - other names by which the person is commonly known, including anglicised names a person may use (for example, if a person from a culturally and linguistically diverse background adopts an anglicised name for day-to-day use).

603. For the purposes of paragraph 9-3(1)(d) of the Rules (the individual's gender), gender may be determined according to any identity documents the reporting entity has already collected, including where customers have indicated the title to prefix their name (for example, Mr, Mrs, Miss, Ms). If no information or identity documents are available which present this information, a reporting entity cannot be expected to know, or have knowledge about the individual's gender for reporting purposes.

604. Subsection 9-3(2) of the Rules prescribes the 'reportable information' in relation to a person who is a non-individual, such as a company or incorporated association, trust, government body, or partnership.

605. Subsection 9-3(3) of the Rules prescribes the information that a SMR must contain about a person in relation to whom a SMR obligation arose (referred to as 'the first person' in section 41(1) of the Act). The section specifies that a SMR must contain the 'reportable information' about the person (specified in subsection 9-3(1) or (2) of the Rules, as the case may be), to the extent it is applicable and known to the reporting entity, as well as information on that person's involvement in the matter (for example, 'subject of suspicion' or 'suspected victim'). The phrase 'the report must contain the following information, to the extent it is applicable and known to the reporting entity' recognises there is no absolute obligation to report any and all information that exists or is theoretically held by an entity. Passive possession of information is not the same as knowledge. If a reporting entity does not know whether the information exists and is

required to conduct extensive searches for them to be cognisant and aware of it, we consider the information is not 'known' to them at the time the reporting obligation arises. When considering whether information is 'known' there needs to be an element of a reporting entity being cognisant or aware of the existence of information, with clearness and certainty for the information to be 'known' for the purpose of this section.

606. Subsection 9-3(4) of the Rules prescribes 'reportable details' must be provided in an SMR in relation to another person, other than the person in relation to whom the SMR obligation arose. Examples of persons who may be captured under subsection 9-3(4) include a beneficiary of a trust, an agent of a body corporate, or a beneficial owner of a company. In particular, subsection 9-3(4) requires a SMR to include 'reportable information' not only about other persons, but additional persons for whom 'reportable details' are required by subsections 9-3(1) (for an individual) or 9-3(2) (for a non-individual) of the Rules in relation to that other person. Paragraph 9-3(4)(b) allows repeated operation of the provision. For example, if a person about whom the SMR obligation arises is a trust, paragraph 9-3(4)(b) provides that the 'reportable information' is to be given in relation to the beneficiaries of the trust, and if the beneficiary of the trust is a company, then the beneficial owner's 'reportable information' is also required to be included in the report to the extent that information is known to the reporting entity (if at all). Collection of this information will allow greater financial intelligence analysis of networks of connected persons, contributing to enhanced understanding and referrals to law enforcement agencies by AUSTRAC.

607. Subsections 9-3(5) to 9-3(7) of the Rules prescribe the SMR obligations in relation to 'involved persons'. Subsection 9-3(5) of the Rules defines that an 'involved person' is each of the following persons:
    - a person (other than the person in relation to whom the SMR obligation arose) who is involved in facilitating, funding, contributing to, or benefitting from, the matter the subject of the report (paragraph 9-3(5)(a))
    - a person who is adversely affected or impacted by the matter (paragraph 9-3(5)(b))
    - a person on whose behalf the customer is receiving the designated service (paragraph 9-3(5)(c))
    - a person acting on behalf of the customer in relation to the designated service (paragraph 9-3(5)(d)).

608. Subsections 9-3(6) and (7) of the Rules prescribe the information that must be contained in a SMR in relation to 'involved persons'. In particular, subsection 9-3(6) requires the SMR to contain 'reportable information' in subsections 9-3(1) (for individuals) and 9-3(2) (for non-individual) about the involved person to the extent that the information is applicable and known to the reporting entity and has not already been reported under subsections 9-3(3) or (4) of the Rules. Subsection 9-3(7) of the Rules requires the SMR to contain, to the extent it is known to the reporting entity, a

description of the relationship between the involved person and the person in relation to whom the SMR obligation arose.

9-4—Reports of suspicious matters – information about the matter

609. Section 9-4 of the Rules prescribes information about the suspicious matter that a reporting entity must include in a SMR made under subsection 41(2) of the Act.

610. As well as general information about the suspicious matter, and details required to be reported under section 41 of the Act (such as the matters in paragraphs 41(1)(a) to (c) of the Act), the other information required to be reported includes particular information about (as applicable, and to the extent the information is known):
- accounts involved
- each transaction in relation to the suspicious matter
- transfers of any property
- virtual assets
- any person, other than the reporting entity giving the report, involved in the provision or proposed provision of a designated service
- online activity by any person involved in the suspicious matter.

611. Paragraph 9-4(1)(a) of the Rules (which relates to matters prescribed in paragraphs 41(1)(a) to (c) of the Act) seeks to identify:
- if the designated service has commenced, or is proposed, to be provided by the reporting entity
- if the person who is the subject of the report has requested the designated service to be provided by the reporting entity, or
- if the person who is the subject of the report inquired whether the reporting entity would be willing or prepared to provide the designated service.

Division 2—Threshold transaction reports

612. Section 43 of the Act imposes an obligation on a reporting entity to give the AUSTRAC CEO a report about any 'threshold transaction' which occurs when commencing to provide, or providing, a designated service to a customer.

613. 'Threshold transaction' is defined in section 5 of the Act. Currently, it means a transaction involving the transfer of physical currency, where the total amount of physical currency transferred is not less than $10,000 (paragraph (a) of the definition). To date, no regulations have been made to trigger paragraphs (c) (money), (ca) (virtual asset) or (d) (property) of the definition, to include these types of transactions within the threshold transaction reporting obligation.

614. Subsection 43(2) of the Act requires that a reporting entity give the AUSTRAC CEO a report about the threshold transaction (TTR) within 10 days after the transaction takes place. Subsection 43(3) of the Act prescribes that a TTR given under subsection 43(2)

must be in the approved form (paragraph 43(3)(a)) and contain such information relating to the transaction as is specified in the Rules (paragraph 43(3)(b)).

615. Part 9, Division 2 of the Rules contains sections 9-5 to 9-8, which have been made for the purpose of paragraph 43(3)(b) of the Act to prescribe the information that must be contained in a TTR made under subsection 43(2) of the Act. Section 9-5 to 9-8 of the Rules will replace Chapter 19 of the former rules. Fundamentally, the type of information required to be included in a TTR remains similar.

616. The reportable details prescribed in Chapter 19 of the former rules have been reviewed and streamlined to better align them with the language and concepts used in the reformed AML/CTF regime—such as those relating to KYC information and the new CDD obligations. In addition, the prescribed reportable details for a TTR have been revised to recognise the new types of designated services and reporting entities which will be regulated under the Act, and updated to reflect technology and service delivery advancements.

617. Paragraph 43(3)(a) of the Act provides that a TTR given under subsection 43(2) must be in the 'approved form'. Reportable details prescribed in sections 9-5 to 9-8 of Rules will be incorporated into the updated approved form referenced in paragraph 43(3)(a) of the Act which a reporting entity will need to use when making a TTR.

9-5—Purpose of this Division

618. Section 9-5 of the Rules states the purpose of Part 9, Division 2 of the Rules, which is to prescribe the reportable details for a TTR required to be made for the purposes of subsection 43(2) of the Act.

619. The enabling power to prescribe the reportable details for a TTR is in paragraph 43(3)(b) of the Act.

Section 9-6—Reports of threshold transactions – general information

620. Section 9-6 of the Rules prescribes the general information that a reporting entity must include in a TTR made under subsection 43(2) of the Act, including the reporting entity's name and AUSTRAC identifier, and the full name, position and contact details of the individual completing the report.

9-7—Reports of threshold transactions – information about the customer and other persons

621. Section 9-7 of the Rules prescribes information a reporting entity must include in a TTR in relation to its customer and any other persons involved in, or related to, the threshold transaction. The information in both subsections 9-7(1) and 9-7(2) of the Rules is reportable as applicable and to the extent that the information is known to the reporting entity. The phrase 'the report must contain the following information, to the

extent it is applicable and known to the reporting entity' recognises there is known' recognises there is no absolute obligation to report any and all information that exists or is theoretically held by an entity. Passive possession of information is not the same as knowledge. If a reporting entity does not know whether the information exists and is required to conduct extensive searches for them to be cognisant and aware of it, we consider the information is not 'known' to them at the time the reporting obligation arises. When considering whether information is 'known' there needs to be an element of a reporting entity being cognisant or aware of the existence of information, with clearness and certainty for the information to be 'known' for the purpose of this section.

622. Subsection 9-7(1) of the Rules prescribes the 'reportable information' in respect of individuals, and subsection 9-7(2) prescribes the 'reportable information' in respect of persons who are not an individual, such as a company, trust, partnership, cooperative or incorporated association.

623. For the purposes of paragraphs 9-7(1)(b) and 9-7(2)(b) of the Rules (other names used by the person), other names of the person include:
- business names that the individual is trading under in the capacity of a sole trader
- previous given or surnames which may have legally changed (for example, through marriage or deed poll)
- other names by which the person is commonly known, including anglicised names a person may use (for example, if a person from a culturally and linguistically diverse background adopts an anglicised name for day-to-day use).

624. Subsection 9-7(3) of the Rules prescribes that a TTR must contain 'reportable information' to the extent it is applicable and known to the reporting entity about:
- the customer to whom the designated service was provided
- the transferor or transferee involved in the threshold transaction, if different to the customer
- if the customer received the designated service on behalf of another person—that other person.

625. In particular, a TTR is required to contain the same 'reportable information' (as applicable, and to the extent known to the reporting entity) that would be required by subsection 9-7(1) or (2) in relation to each of the above persons.

626. The transferor or transferee refers to a person who supplies, or ultimately obtains, the physical currency for, or from, a threshold transaction, but is not receiving the designated service in the capacity of a customer. For example:
- a third-party makes a cash deposit into the account of a customer at a branch of the customer's bank (designated service item 4, table 1 in section 6 of the Act). The third-party would be considered a transferor of the physical currency
- a third-party accompanies and supplies the customer with physical currency to facilitate one of the professional designated services listed in table 6, section 6 of

the Act, for example, to settle the bill with cash for professional fees for assisting to acquire a business. The third-party would be considered the transferor of the physical currency.

627. An example of a person which would be covered by paragraph 9-7(3)(c) of the Rules is a customer who is a trustee of a trust transacting AUD 15,000 cash for the equivalent value of gold bullion, on behalf of their family trust. In this example, the reporting entity is expected to provide information required by subsection 9-7(1) or (2) in relation to the family trust estate (not being the customer of the designated service).

628. Subsection 9-7(4) of the Rules relates to a TTR including information about other persons. In particular, subsection 9-7(4) applies where a TTR is required to contain the details of another person as part of the 'reportable information' in subsections 9-7(1) and 9-7(2) of the Rules. The example given is a beneficial owner or a trust. Subsection 9-7(4) of the Rules requires a TTR to also contain 'reportable information' about that other person, as well as information that is 'reportable information' about any other person for whom details must be included pursuant to the reportable information requirements in subsections 9-7(1) and 9-7(2) of the Rules. Paragraph 9-7(4)(b) provides that 'reportable information' is to be given in relation to the beneficiaries of the trust, and if the beneficiary of the trust is a company, then the beneficial owner's 'reportable information' is also required to be included in the report to the extent that information is known to the reporting entity (if at all).

629. Subsection 9-7(5) of the Rules prescribes that where there is another authorised person acting on behalf of the customer, a TTR must contain the 'reportable information' about that person (in accordance with subsections 9-7(1) or 9-7(2), whichever is applicable) and a description of the following:
- the relationship between the other person and the customer, and
- the authority of the person to act on behalf of the customer.

630. Subsection 9-7(6) of the Rules prescribes that subsection 9-7(5) of the Rules does not apply in the following circumstances:
- the threshold transaction was a deposit in circumstances where there was no personal contact (such as using an automated teller machine or express deposit facility) (paragraph 9-7(6)(a))
- the transaction did not involve a virtual asset (paragraph 9-7(6)(b))
- the authorised person was acting in the course of a business of collecting, holding or delivering physical currency (such as payroll or cash courier services, but not including collection of donations for a registered charity) (paragraph 9-7(6)(c)).

631. Subsection 9-7(7) of the Rules prescribes that where subsection 9-7(5) does not apply because the designated service occurred in the circumstances mentioned in subsection 9-7(6), the report must include a statement as to the circumstances of the designated service.

9-8—Reports of threshold transactions – information about the transaction

632. Section 9-8 of the Rules prescribes details about the threshold transaction itself that a reporting entity must include in a TTR made under subsection 43(2) of the Act.

633. Subsection 9-8(1) of the Rules prescribes the 'standard information' that must be included in a TTR. For the purposes of paragraph 9-8(1)(f) of the Rules (the reporting entity's reference number), a reference number could, for example, be a transaction or invoice number, or a serial number unique to the documents associated with the designated service.

634. Subsections 9-8(2), (3), (4), (5) and (7) of the Rules require TTRs to include information, as applicable and to the extent that the information is known, about the following:
- an account provided by the reporting entity or another person (subsection 9-8(2))
- products or instruments involved in the threshold transaction (subsection 9-8(3))
- transfers of property (subsection 9-8(4))
- virtual assets (subsection 9-8(5))
- online activity (subsection 9-8(7)).

635. Subsection 9-8(6) of the Rules requires a TTR to include information about any other person providing a designated service relating to the threshold transaction, including the full name of the person, the place where the person was involved in the provision of the designated service, and a description of the designated service provided by the person. Practically this would mean that where a real estate agent accepts a deposit from a buyer in physical currency and the buyer has provided details of their solicitor who will conduct conveyancing on their behalf so the agent can send the contract, the real estate agent would provide the details of the solicitor to the extent that it has them. Such increased ability for AUSTRAC to identify linkages will result in enhanced financial intelligence analysis to combat financial crime.

Meaning of 'products and instruments'

636. Subparagraph 9-4(4)(d)(i) of the Rules requires a description of products or instruments, if these have been involved in a transaction being reported in a SMR. Subsection 9-8(3) of the Rules requires a description of products or instruments, if these have been involved in the transaction being reported in a TTR.

637. A product or instrument refers to the (monetary or non-monetary) article specified within the description of each designated service in the various tables in section 6 of the Act. A product or instrument is an article which enables the provision of the respective designated service, either by way of holding a monetary value and/or being able to be exchanged for money.

638. The examples below present some of the products or instruments which can be involved in a designated service and references the relevant designated service item listed in section 6 of the Act. The examples are not exhaustive:
    - cheque (items 14, 15, 16 from Table 1)
    - stored value card (items 21, 22, 23, 24 from Table 1)
    - precious metals, stones or products (item 2 from Table 2)
    - chips or tokens, for the purpose of gambling (items 7 and 8 from Table 3)
    - virtual asset (items 46A, 50A, 50B, 50C from Table 1; items 7, 8 from Table 3; and item 3 from Table 6)
    - real estate (items 1, 2 from Table 5; item 1 from Table 6).

Meaning of 'full name'

639. Divisions 1 and 2 of Part 9 of the Rules require that the 'full name' of an individual must be contained in a SMR or TTR. Full name in this context should be taken to mean the person's first and last name, and any middle name(s), written in full.

640. For a non-individual, 'full name' should be taken to mean the full legal name of the non-individual, such as that specified in legal documentation establishing, or involving the non-individual.

Division 3—AML/CTF compliance reports

9-9—Reporting and lodgement periods for AML/CTF compliance reports

641. Section 47 of the Act imposes an obligation on a reporting entity to periodically give the AUSTRAC CEO a report (compliance report) in relation to the reporting entity's compliance with the Act, the regulations and the Rules during a 'reporting period' (subsection 47(2) of the Act).

642. The application of section 47 of the Act is triggered if there are Rules which provide that:
    - a specified period is a reporting period; and
    - a specified period beginning at the end of the reporting period is the lodgement period for that reporting period (subsection 47(1) of the Act).

643. Both the reporting period and the lodgement period may be a recurring period.

644. If there are Rules which specify a 'reporting period' and 'lodgement period', a reporting entity must, within the lodgement period, provide a compliance report in relation to the reporting period to the AUSTRAC CEO (subsection 47(2) of the Act).

645. Subsection 47(3) of the Act requires a compliance report to:
    - be in the approved form; and
    - contain such information as is required by the approved form.

646. Section 9-9 of the Rules provides the same 'reporting period' and 'lodgement period' as is contained in the former rules:
    - each calendar year is a reporting period (that is, 1 January to 31 December, inclusive); and
    - the period of 3 months beginning at the end of a reporting period is the lodgement period for that reporting period (that is, 1 January to 31 March of the following calendar year).

Division 4—Registered remittance affiliates

9-10—Reporting obligations of registered remittance affiliates

647. Section 9-10 of the Rules is made for the purposes of section 49A of the Act.

648. Section 49A of the Act allows for the making of Rules in relation to reports required to be lodged by registered remittance affiliates.

649. Subsection 9-10(2) of the Rules allows a RNP to give a SMR to the AUSTRAC CEO on behalf of a registered remittance affiliate, and discharge the affiliate's obligation to give such a report if there is a written agreement between the affiliate and the network provider that provides for the network provider to do so.

650. Subsection 9-10(3) of the Rules alters the default legal obligation for a registered remittance affiliate to give a:
    - TTR under subsection 43(2) of the Act; and
    - report of an international funds transfer instruction under subsection 46(2) of the Act.

651. The obligation falls on the RNP to give such reports to the AUSTRAC CEO where there is a remittance affiliate.

Division 5—Cross-border movement reports

9-11—Purpose of this Division

652. Division 5 of Part 9 of the Rules sets out:
    - the information to be contained in a report about movement of monetary instruments into or out of Australia, submitted by a person moving the monetary instrument (the traveller)– for the purposes of paragraph 53(7)(b) of the Act
    - the timing rule for the submission of a report about movement of monetary instruments into or out of Australia—for the purposes of paragraph 53(7)(d) of the Act
    - the information to be contained in a report about movement of monetary instruments moved into Australia, submitted by a person receiving or sending the monetary instrument—for the purposes of paragraph 54(4)(b) of the Act

- the form and content of notices about reporting obligations that can be affixed in ports to inform travellers of reporting obligations, and the location of such notices—for the purposes of paragraph 61(1)(b) and 61(2)(b) of the Act.

9-12—Reports about moving monetary instruments into or out of Australia

653. Section 9-12 of the Rules prescribes that that a report under section 53 of the Act (reports about movements of monetary instruments into or out of Australia) must contain the information specified in subsection 9-12(2) (to the extent the information is known) and be given in accordance with the applicable timing rules specified in subsection 9-12(3) of the Rules.

654. The timing rules in subsection 9-12(3) of the Rules for reports made under section 53 of the Act are as follows:
    - if the person brings the monetary instrument into Australia, no later than when the person reaches the place at which customs officers examine baggage, or if there is no such place, at the first opportunity after arrival in Australia
    - if the person moves the monetary instrument by sending it into Australia, before the movement takes place
    - if the person takes the monetary instrument out of Australia, no later than when the person reaches the place at which customs officers examine baggage, or if there is no such place, before the last opportunity to give the report before leaving Australia, and
    - if the person sends the monetary instrument out of Australia by consignment, before the time when the instrument is irrevocably committed to a postal service or other person (as the case may be).

655. Reports for the purposes of section 53 of the Act must be given in the approved form.

9-13—Reports about receiving monetary instruments moved into Australia

656. Section 9-13 specifies the information required for a report under section 54 of the Act (reports about receipts of monetary instruments moved into Australia), including prescribed details that need to be reported if the monetary instrument is a bearer negotiable instrument.

657. Reports for the purposes of section 54 of the Act must be given in the approved form.

9-14—Affixing of notices about cross-border movement reporting obligations

658. Section 61 of the Act provides a power to affix written notices about reporting obligations under Part 4 of the Act. Paragraph 61(1)(b) of the Act allows for the making of Rules which specify the form and contents of the written notices. Subsection 61(2) of the Act allows for such written notices to be affixed to any part of an aircraft or ship, or any other place specified in the Rules.

659. Paragraph 9-14(2)(a) of the Rules prescribes that the written notices can be in one of three forms:
    - a self-standing sign
    - a digital or electronic sign
    - a sign in any other material form.

660. Paragraph 9-14(2)(b) of the Rules prescribes the wording content of the written notices (which may include other additional words).

661. Subsection 9-14(3) of the Rules (made for the purposes of paragraph 61(2)(b) of the Act) prescribes, by reference to the provisions of the *Customs Act 1901*, that the written notices may be affixed at the following places:
    - any port, airport, wharf, or boarding station that is appointed under section 15 of the *Customs Act 1901*; or
    - a place to which section 234AA of the *Customs Act 1901* applies that is not a place, or a part of a place, referred to in paragraph (a).

662. The incorporation by reference to the *Customs Act 1901* is permitted by paragraph 14(1)(a) of the *Legislation Act 2003*.

Part 10—Secrecy and access

Section 10-1—Disclosure of AUSTRAC information to foreign countries or agencies

663. Section 10-1 of the Rules is made for the purposes of paragraph 127(2)(a) of the Act to prescribe the Commonwealth, State or Territory agencies—the heads of which may disclose AUSTRAC information to the government of a foreign country, or to a foreign agency.

664. Safeguards around the sharing of AUSTRAC information are contained in subsection 127(2) of the Act. This includes requiring the agency head to be satisfied that:
    - the government of the foreign country, or the foreign agency, has given an undertaking for:
        - protecting the confidentiality of the information and controlling the use that will be made of the information; and
        - ensuring that the information will be used only for the purpose for which it is disclosed to the government of the foreign country or to the foreign agency; and
        - it is appropriate, in all the circumstance of the case, to make such a disclosure to the government of the foreign country, or the foreign agency.

Part 11—Other matters

Section 11-1—False or misleading information or documents

665. Section 11-1 prescribes the provisions of the Rules that are subject to the false or misleading information and documents offences under sections 136 and 137 of the Act respectively.

666. These offences apply where:
- a person gives information or produces a document to the AUSTRAC CEO, an authorised officer, a customs officer, a police officer, a reporting entity or a person acting on a reporting entity's behalf, and
- the person does so knowing that the information or document is false or misleading or, when giving information, knowing that the information omits any matter or thing without which the information is misleading, and
- the information or document is given or produced, or purportedly given or produced, under the Act or a provision of the regulations or of the Rules, if the regulations or Rules (as applicable) state that section 136 or 137 of the Act applies to this provision.

667. Section 11-1 provides that these offences apply to information or a document given or produced, or purportedly given or produced, under the following provisions of the Rules:
- Part 3—Enrolment.
- Part 4—Registration
- Part 6—Customer due diligence
- Part 8—Transfers of value
- Part 9—Reporting

668. The effect of section 11-1 is that, where a person gives information or provides documents, or purports to do so, under these provisions of the Rules in breach of one of the false or misleading offences mentioned above, they will face a maximum penalty of 10 years' imprisonment or 10,000 penalty units, or both.

669. Strict liability applies to the physical element that the information or document was given or produced, or purportedly given or produced, under a provision of the Rules. Under subsection 6.1(2) of the *Criminal Code Act 1995*, this means that no fault elements apply to this physical element and the defence of mistake of fact is available.

Part 12—Application, saving and transitional provisions

Sections 12-1 and 12-2 —Transitional requirements in relation to reports of suspicious matters

670. Sections 12-1 and 12-2 of the Rules prescribe transitional requirements for the reporting of SMRs during the following periods:
    - the period between commencement of these Rules (31 March 2026) and 30 June 2026 (section 12-1); and
    - the period starting 1 July 2026 and ending on 29 March 2029 (or such other day specified in an instrument made under subsection 12-2(3)) (section 12-2).

671. In essence, section 12-1 of the Rules prescribes that for the period between 31 March 2026 and 30 June 2026, all reporting entities will need to report SMRs using the existing approved form for the purposes of paragraph 41(3)(a) of the Act and include the reportable details prescribed in Chapter 18 of the former rules (the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)*). SMRs submitted in this manner during this period are deemed to comply with the new requirements in Division 1 of Part 9 of the Rules under subsection 12-1(3).

672. For SMRs given to the AUSTRAC CEO from 1 July 2026, different requirements apply depending on whether or not a reporting entity is enrolled with AUSTRAC as at 30 March 2026:
    - Under section 12-2 of the Rules, reporting entities enrolled with AUSTRAC as at 30 March 2026 will have the option to:
        - submit SMRs using the existing approved form for the purposes of paragraph 43(3)(a) of the Act, and include the reportable details in Chapter 18 of the existing Rules—in which case such a report is taken to comply with the new requirements under Division 1 of Part 9 of the Rules (subsection 12-2(2)); or
        - submit SMRs in accordance the new requirements in Division 1 of Part 9 of the Rules.

673. Reporting entities not enrolled with AUSTRAC as at 30 March 2026 will need to submit SMRs in accordance with the new requirements in Division 1 of Part 9 of the Rules.

674. The ability for reporting entities enrolled as at 30 March 2026 to continue reporting SMRs from 1 July 2026 in accordance with the existing requirements and Chapter 18 of the existing Rules will continue until 29 March 2029 or an earlier date specified under a notifiable instrument made by the AUSTRAC CEO pursuant to subsection 12-2(3) of the Rules.

Sections 12-3 and 12-4—Transitional requirements in relation to reports of threshold transactions

Transitional requirements for reports of threshold matters from 31 March 2026

675. Sections 12-3 and 12-4 of the Rules prescribe transitional requirements for the reporting of TTRs during the following periods:
    - the period between commencement of these Rules (31 March 2026) and 30 June 2026 (section 12-1); and
    - the period starting 1 July 2026 and ending 29 March 2029 (or such other day specified in an instrument made under subsection 12-2(3)) (section 12-2).

676. In essence, section 12-3 of the Rules prescribes that for the period between 31 March 2026 and 30 June 2026, all reporting entities will need to report TTRs using the existing approved form for the purposes of paragraph 43(3)(a) of the Act and include the reportable details prescribed in Chapter 19 of the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)*. TTRs submitted in this manner during this period are deemed to comply with the new requirements in Division 2 of Part 9 of the Rules (subsection 12-3(3)).

677. For TTRs given to the AUSTRAC CEO from 1 July 2026, different requirements apply depending on whether or not a reporting entity is enrolled with AUSTRAC as at 30 March 2026:
    - Under section 12-3 of the Rules, reporting entities enrolled with AUSTRAC as at 30 March 2026 will have the option to:
        - submit TTRs using the existing approved form for the purposes of paragraph 43(3)(a) of the Act, and include the reportable details in Chapter 19 of the existing Rules—in which case such a report is taken to comply with the new requirements under Division 2 of Part 9 of the Rules (subsection 12-2(2)); or
        - submit TTRs in accordance the new requirements in Division 2 of Part 9 of the Rules.
    - Reporting entities not enrolled with AUSTRAC as at 30 March 2026 will need to submit TTRs in accordance with the new requirements in Division 2 of Part 9 of the Rules.

678. The ability for reporting entities enrolled as at 30 March 2026 to continue reporting TTRs from 1 July 2026 in accordance with the existing requirements and Chapter 19 of the existing Rules will continue until 30 March 2029 or an earlier date specified under a notifiable instrument made by the AUSTRAC CEO pursuant to subsection 12-4(3) of the Rules.

Section 125-35—Transitional—keep open notices

679. Section 12-3 5 of the Rules prescribes transitional requirements in relation to exemptions granted to reporting entities under Chapter 75 of the former Rules prior to 31 March 2026, and which continue in force beyond this date.

680. Subsection 125-35(2) of the Rules prescribes that an exemption issued under Chapter 75 of the former Rules, and which continues in force after 31 March 2026 may be dealt with as if it were a keep open notice issued under subsection 39B(1) of the Act by a senior member of the eligible agency that requested the (Chapter 75) exemption. In these cases, the expiry of the (Chapter 75) exemption is to be determined in accordance with subsection 125-35(3) of the Rules.

681. Furthermore, subsection 125-35(4) of the Rules prescribes that any further extensions of Chapter 75 exemptions that continue in force after 31 March 2026 are to be done in accordance with subsections 39B(7) and 39B(8) of the Act which otherwise apply to keep open notices.

Schedule 1—Forms

682. This schedule prescribes, and contains, forms for the purposes of the 'keep open notice' framework.

683. The prescribed forms have been developed to strike a balance between operational practicalities of specified agencies and the need to contain a sufficient amount of information for a reporting entity to identify the customer or customers to which the exemption applies and promote a consistent manner of presenting information by issuing agencies to reporting entities and AUSTRAC.

684. The prescribed forms are not designed to form a basis for deciding to issue such a notice by a senior officer, they only represent the outcome of a decision to issue a notice. Specified agencies are required to keep records of their administrative decision making underpinning the issuing of a notice.

Form 1—Keep open notice

685. Form 1 in Schedule 1 to the Rules is the prescribed form for the purpose of paragraph 39B(5)(a) of the Act for use when a senior member issues a keep open notice pursuant to subsection 39B(1) of the Act.

686. It is noted that section 6-38 of the Rules provides that Form 1 in Schedule 1 is prescribed as the form for a keep open notice, while section 6-39 of the Rules prescribes the information and documents required to be contained in, or to accompany, a keep open notice, and mirrors the information and documents specified in Form 1.

Form 2—Extension notice

687. Form 2 in Schedule 1 to the Rules is the prescribed form for the purpose of subsection 39B(7) of the Act, for use when a senior member decides to extend the period that a keep open notice remains in force for a further period of 6 months.

688. It is noted that section 6-40 of the Rules provides that Form 2 in Schedule 1 is prescribed as the form for an extension notice.

Form 3—Application to issue extension notice

689. Form 3 in Schedule 1 to the Rules is the prescribed form for the purpose of paragraph 39B(8)(b) of the Act, for use by a senior member when making an application to the AUSTRAC CEO to further extend the period that a keep open notice remains in force after two previous extension notices have been issued in relation to the same keep open notice.

690. Section 6-41 of the Rules provides that Form 3 in Schedule 1 is prescribed as the form of an application to the AUSTRAC CEO for a notice under paragraph 39B(8)(d) of the Act.

ATTACHMENT B

Anti-Money Laundering and Counter-Terrorism Financing Rules Amendment (Consequential Amendments) Instrument 2025

Explanation of provisions in the *Anti-Money Laundering and Counter-Terrorism Financing Rules Amendment (Consequential Amendments) Instrument 2025*

Part 1—Preliminary

Item 1—Name

1. This item provides that the name of the Instrument is the *Anti-Money Laundering and Counter-Terrorism Financing Rules Amendment (Consequential Amendments) Instrument 2025*

Item 2—Commencement

2. This section provides for the commencement of the Instrument, as set out in the table in subsection 2(1).

3. Schedule 1 to this Instrument commences at the same time as the *Anti-Money Laundering and Counter-Terrorism Financing Rules 2025* commence.

4. Schedule 2 to this Instrument commences on 31 March 2031.

Item 3—Authority

5. This section provides that the Instrument is made under section 229 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.

Item 4—Schedules

Schedule 1—Amendments

Item 1—Section 1

6. This item renames the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)* as the *Anti-Money Laundering and Counter-Terrorism Financing (Class Exemptions and Other Matters) Rules 2007*.

Item 2—Section 2

7. This item repeals section 2 which consisted of the name of the instrument and a statement that the Anti-Money Laundering and Counter-Terrorism Financing Rules are set out in this Instrument.

Item 3—Part 1.2

8. This item sets out the key terms and concepts used in the *Anti-Money Laundering and Counter-Terrorism Financing Rules Amendment (Consequential Amendments) Instrument 2025*.

Item 4—Chapters 2 to 20

9. This item repeals Chapters 2-20 inclusive. Chapters 3, 7, 11, 12, 13, 16, 17, 18 and 19 have been replaced by provisions in the Rules.

10. Chapters 2, 4, 8, 9, and 15 have been repealed as the matters set out in those Chapters are contained in the amended Act and the Rules

11. The matters in Chapter 6 and the exemptions set out in Chapters 10 and 14, are now dealt with by provisions in the Act.

12. Chapters 5 and 20 have been repealed because the provisions in the Act that they were made for, have been repealed.

Item 5—Chapter 21

13. This item replaces the term "prescribed financial market" with the term "declared financial market" in subparagraph 21.3(1)(a), following similar amendments to the section 9 of the *Corporations Act 2001*.

Item 6—Chapter 21

14. Item 6 replaces the reference to Division 4 of Part 2 of the Act in subparagraph 21.3(1)(b)(ii) with an updated reference to section 28 of the Act.

Item 7—Chapter 21

15. This item replaces the term "prescribed financial market" with the term "declared financial market" in subparagraphs 21.3(2) and (3) following amendments to the section 9 of the *Corporations Act 2001*.

Item 8—Chapter 21

16. Item 8 replaces the term "prescribed financial market" in subparagraph 21.3(4)(a)(i)(A) with the term "declared financial market", following amendments to section 9 of the *Corporations Act 2001*.

Item 9—Chapter 21

17. This item replaces the obsolete term "the applicable customer identification procedure" in subparagraphs 21.3(4)(d)(ii) and (iii), with the term "initial customer due diligence" consistent with the terms and concepts in the Act.

Item 10—Chapter 21

18. Item 10 replaces the obsolete term "the applicable customer identification procedure" in subparagraph 21.3(4)(e) with the term "initial customer due diligence", consistent with the terms and concepts in the Act.

Item 11—Chapter 21

19. This item defines "declared financial market" to have the meaning given by section 9 of the *Corporations Act 2001*, and inserts the definition after subparagraph 21.4(1).

Item 12—Chapter 21

20. Item 12 updates the reference to Chapter 19 of the ASX Rules in subparagraph 21.4(2) to reflect that the current version of that Chapter was issued on 1 December 2019.

Item 13—Chapter 21

21. This item replaces the term "prescribed financial market" with the term "declared financial market" in subparagraph 21.4(3), following similar amendments to the section 9 of the *Corporations Act 2001*.

Item 14—Chapter 21

22. This item repeals subparagraph 21.4(5) to remove the definition of "managed investment scheme" as the term is defined in section 5 of the Act, therefore that definition applies to Chapter 21.

Item 15—Chapter 21

23. Item 15 amends subparagraphs 21.4(6)(b) and (c) by replacing the obsolete term "the applicable customer identification procedure" with the term "initial customer due diligence", consistent with the terms and concepts in the Act.

Item 16—Chapter 21

24. Item 16 updates the *Corporations Act 2001* reference in subparagraph 21.4(7)

Item 17—Chapter 21

25. This item repeals subparagraph 21.4(8) to remove the obsolete term "prescribed financial market" from the Chapter.

Item 18—Chapter 22

26. Item 18 replaces the reference to "Wholesale Electricity Market Rules" in subparagraph 22.3(1)(c) with an updated reference to the renamed "Electricity System and Market Rules".

Item 19—Chapter 22

27. This item amends subparagraph 22.3(1)(f) to replace the term "AFS licence" with the term "Australian financial services licence", a defined term in section 5 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.

Item 20—Chapter 22

28. Item 20 replaces the reference to "Wholesale Electricity Market Rules" in subparagraphs 22.3(2)(c) and 22.5(1)(c) with an updated reference to the renamed "Electricity System and Market Rules".

Item 21—Chapter 22

29. This item amends subparagraph 22.5(1)(f) to replace the term "AFS licence" with the term "Australian financial services licence", a defined term in section 5 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.

Item 22—Chapter 22

30. Item 22 replaces the reference to "Wholesale Electricity Market Rules" in subparagraph 22.5(2)(c) with an updated reference to the renamed "Electricity System and Market Rules".

Item 23—Chapter 22

31. Item 23 repeals subparagraph 22.6(1) to remove the obsolete defined term "*AFS licence*".

Item 24—Chapter 22

32. This item removes the obsolete term "Wholesale Electricity Market Rules" and its definition and defines the term "Electricity System and Market Rules" by reference to the renamed *Electricity Industry (Electricity System and Market) Regulations 2004* (WA).

Item 25—Chapters 23 to 30

33. This item repeals Chapters 23 to 30 inclusive. Chapter 23 has been repealed as amendments to the AML/CTF Act removed the term "*non-financier*" from the Act rendering Chapter 23 obsolete.

Items 26, 27 and 29—Chapter 31

34. These items amend subparagraphs 31.3(1), 31.3(2) and 31.4(1) to replace the defined term "traveller accommodation" with the term "short-term accommodation for travellers" which has its ordinary meaning.

Item 28—Chapter 31

35. Subparagraph 31.3(5) previously made reference to Chapter 32 of the AML/CTF Rules. This Instrument repeals Chapter 32 and item 28 amends subparagraph 31.3(5) to reflect that repeal.

Items 30 and 31—Chapter 31

36. These items amend subparagraph 31.4(1) and repeal subparagraph 31.4(2) to remove the term "traveller accommodation" from Chapter 31.

Item 32—Chapters 32 to 38

37. This item repeals Chapters 32 to 38 inclusive. Chapter 32 is no longer required because item 47 of table 1 in section 6 of the AML/CTF Act was amended to exclude providing a safe deposit box or similar facility in the course of carrying on a business that provides short-term accommodation for travellers.

38. The exemptions previously provided by Chapters 33 and 35 to 38 have been moved into the Act.

39. The matters dealt with in Chapter 34 are now covered in Division 6 of Part 8 of the Rules.

Items 33 and 34—Chapter 39

40. These items amend the heading to Chapter 32 and update the wording in paragraph 39.2 to make it consistent with the terms and concepts in the amended Act.

Item 35—Chapters 40 and 41

41. Item 35 repeals Chapters 40 and 41. Chapter 40 is no longer required as the term it defined has been removed from the Act. The exemptions contained in Chapter 41 relating to the cashing out of low value superannuation funds are now contained in section 39E of the Act.

Item 36—Chapter 43

42. Item 36 amends the reference in paragraph 43.1 to a subsection of section 247 of the Act.

Item 37—Chapter 45

43. This item amends Chapter 45 to update the scope and references used in the Chapter for consistency with the provisions and concepts of the amended Act.

Item 38—Chapter 46

44. This item repeals Chapter 46 as the matters set out in the Chapter are dealt with in Part 5 of the Rules.

Items 39 to 41—Chapter 48

45. Item 39 amends subparagraph 48.2(1) to remove obsolete references to items 31 and 32 of table 1 in section 6 of the Act following the inclusion of section 63A into the Act.

46. Item 40 updates the scope and references used in paragraph 48.3 for consistency with the provisions and concepts of the amended Act.

47. Item 41 repeals subparagraphs 48.4(1) and 48.4(3) to remove the definitions of "*payroll*" and "*superannuation clearance*" as a result of the amendment to paragraph 48.3.

Items 42—Chapter 49

48. Item 42 replaces the reference in paragraph 49.2 to Division 4 of Part 2 of the AML/CTF Act with an updated references to section 28 of the Act

Item 43—Chapter 49

49. This item updates the *Corporation Act 2001* references in subparagraphs 49.4(1), (2) and (3).

Item 44—Chapters 50 to 66

50. Item 44 repeals Chapters 50 to 66 inclusive. Because of amendments to the Act, Chapters 50 and 66 have been replaced by deemed compliance provisions in Part 5 of the Rules.

51. Chapter 51 has been repealed as it is no longer required because of amendments to the Act.

52. The exemption set out in Chapter 52 has been moved into section 233K of the Act.

53. Chapters 53 to 61 relate to the registration of providers of remittance services. These matters are now dealt with in Part 3 of the Rules.

54. Chapters 62 to 65 relate to the enrolment of reporting entities. These matters are now dealt with in Part 2 of the Rules.

Items 45 —Chapter 67

55. Item 45 replaces the references in paragraphs 67.2 to 67.6 to Division 4 of Part 2 of the AML/CTF Act with updated references to section 28 of the Act.

Item 46—Chapter 67

56. Item 46 replaces the term "prescribed financial market" with the term "declared financial market" in subparagraphs 67.8(2), (3) and (6), following similar amendments to the section 9 of the *Corporations Act 2001*.

Item 47—Chapters 68 to 81

57. This item repeals Chapters 68 to 81 inclusive. Chapter 68 has been replaced by section 111 of the Act. Because of the exclusion of casinos from the definition of "registrable remittance service" in the Act, Chapter 69 is no longer required.

58. Chapter 70 is no longer required as the renewal of registrations is now dealt with in Part 3 of the Rules.

59. Chapter 71 is no longer required due to amendments of items 1 to 3 of table 1 in section 6 of the AML/CTF Act.

60. Because of value transfer amendments to the Act, Chapters 72 and 78 are no longer required to enable reporting of international value transfers.

61. The matters dealt with in Chapter 73 now fall within the provisions of section 63A of the Act.

62. The exemption contained in Chapter 75 is now contained in sections 39A, 39B and 39C of the Act, with notice requirements set out in Division 8 of Part 5 of the Rules.

63. Chapter 76 relates to the registration of virtual asset service providers (formerly Digital Currency Exchanges). These matters are now dealt with in Part 3 of the Rules.

64. Chapter 77 has been repealed because it is obsolete.

65. The matters set out in Chapter 79 are now dealt with in Part 5 of the Rules.

66. Chapter 80 is no longer required as the definitions of "*stored value card*" in the Act has been amended.

67. Due to the exclusion of financial institutions from the definition of "*registrable virtual asset service*" in the Act, Chapter 81 is no longer required.

Schedule 2—Amendments commencing on 31 March 2031

Item 1—Chapters 21, 22, 31, 39, 42, 43, 45, 47, 48, 49 and 67

68. This item repeals Chapters 21, 22, 31, 39, 42, 43, 45, 47, 48, 49 and 67 on 31 March 2031. These Chapters provide exemptions from various provisions of the AML/CTF Act.

69. During this 5-year timeframe AUSTRAC will undertake a review including public consultation, and reassessment of each of the exemptions to determine whether they should continue to operate.

ATTACHMENT C

Statement of Compatibility with Human Rights

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

Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2025

Anti-Money Laundering and Counter-Terrorism Financing Rules Amendment (Consequential Amendments) Instrument 2025

The *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2025* and *Anti-Money Laundering and Counter-Terrorism Financing Rules Amendment (Consequential Amendments) Instrument 2025* (the Rules Instruments) are compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview

1. The Rules Instruments supplement various overarching requirements prescribed in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (the Act), which was amended in 2024 by the *Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2024* (the Amendment Act).
2. The amendments to the AML/CTF Act expanded the regulatory scope of the anti-money laundering and counter-terrorism financing (AML/CTF) regime to cover additional services that are globally recognised by the Financial Action Task Force (FATF) as posing high money laundering and terrorism financing risk. Consequently, from 2026, the following industries (known as 'Tranche 2 entities') will commence having obligations under the expanded AML/CTF regime:
    - real estate professionals
    - dealers in precious stones, metals and products
    - certain professional service providers (such as lawyers, accountants, trust and company service providers), and
    - virtual asset service providers.
3. To give effect to, and supplement, the Amendment Act, the AUSTRAC CEO is creating a new AML/CTF Rules framework:

    (a) the making of the *Anti-Money Laundering and Counter-Terrorism Financing Rules 2025* (the Rules), which replaces many of the provisions in the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007* and operationalises the amended AML/CTF Act; and

    (b) the *Anti-Money Laundering and Counter-Terrorism Financing Rules (Class Exemption and Other Matters) 2007* (the Class Exemption Rules) formerly titled the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007*—which has historically supplemented the AML/CTF Act—has been

amended and renamed. The only chapters preserved are Chapters 1, 21, 22, 31, 39, 42, 43, 45, 47, 48, 49, and 67.

32. The AML/CTF Rules 2025 is set out in a topically-structured format that reflects the order of engagement a reporting entity will have with the AML/CTF regime. It supports the amended AML/CTF Act by:

- providing reporting entities with finer detail on fundamental AML/CTF obligations set out in the AML/CTF Act, for example, reporting groups, AML/CTF programs and customer due diligence (CDD) obligations
- specifying information required to meet specific obligations—particularly for enrolment, registration, suspicious matter reporting, threshold transaction reporting, keep open notices, and the transfer of value
- re-writing in simpler terms, existing measures that have not substantively changed such as correspondent banking relationships and AML/CTF compliance reporting requirements.

4. The reforms to the AML/CTF regime do not fundamentally change the central tenets of the existing regime, which align with international obligations. These are:

- persons providing designated services—known as 'reporting entities' – must enrol (and, in certain circumstances, register) with AUSTRAC
- reporting entities must develop, maintain and comply with an AML/CTF program that appropriately identifies, mitigates and manages the money laundering/terrorism financing (ML/TF) risks associated with the provision of designated services
- reporting entities must identify their customers, verify their customers' identity, understand the associated ML/TF risk of the customer before providing a designated service, and undertake ongoing CDD
- reporting entities must report certain transactions and suspicious matters to the AUSTRAC CEO, and
- reporting entities must make and retain certain records and ensure they are available to law enforcement and the AUSTRAC CEO.

5. In particular, the Rules contains details in relation to the following requirements in the Act:

- revised information required for enrolment and registration applications
- AML/CTF programs
- reporting groups
- CDD, including delayed CDD in a wider range of circumstances and simplified beneficial owner due diligence for certain low risk customers
- travel rule
- updated reportable details for threshold transaction reports (TTRs) and suspicious matter reports (SMRs)
- compliance reports

- keep open notices (formerly ‘Chapter 75 notices’)
- correspondent banking relationships.

Human rights implications

6. The Rules Instruments may engage, directly or indirectly, the following human rights:
    - protections against arbitrary or unlawful interference with privacy, and unlawful attacks on honour or reputation, in Article 17 of the International Covenant on Civil and Political Rights (ICCPR)
    - right to life and freedom from torture or cruel, inhuman or degrading treatment or punishment, in Articles 6 and 7 of the ICCPR
    - right to equality and non-discrimination, in Article 2, 16, and 26 of the ICCPR
    - right to freedom of association, in Article 22 of the ICCPR, and
    - right to work, in Article 6 of the International Covenant on Economic, Social and Cultural Rights (ICESCR).

Protections against arbitrary or unlawful interference with privacy, and unlawful attacks on honour or reputation—Article 17 of the ICCPR

7. Article 17 of the ICCPR provides that no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence. Article 17 of the ICCPR also provides that a person must not be subjected to unlawful attacks on his or her honour or reputation.

8. The protection for privacy under Article 17 can be permissibly limited to achieve a legitimate objective and where the limitations are lawful and not arbitrary. The term ‘*unlawful*’ in Article 17 of the ICCPR means no interference can take place except as authorised under domestic law.

9. The terms ‘*arbitrary*’ means that any interference with privacy must be in accordance with the provisions, aims and objectives of the ICCPR and should be reasonable in particular circumstances. The United Nations Human Rights Committee (UNHRC) has interpreted ‘*reasonableness*’ to mean that any limitation must be proportionate and necessary in the circumstances. In this case, the legitimate end is the protection of public safety, addressing crime and protecting the rights and freedoms of individuals by requiring certain personal information to be collected, retained and disclosed to support relevant investigations.

10. Measures in the Rules that may engage the protection against arbitrary and unlawful interference with privacy in Article 17 of the ICCPR include:
    - enrolment requirements (Part 3)
    - registration requirements (Part 4)
    - the changes to CDD requirements (Part 6)
    - transfer of value requirements for ordering and beneficiary institutions (Part 8)
    - the reporting obligation requirements (Part 9), and
    - the ability to disclose ‘AUSTRAC information’ to foreign countries or agencies (Part 10).

Enrolment requirements

11. The Reporting Entities Roll, maintained by the AUSTRAC CEO, contains details about all reporting entities regulated by AUSTRAC. Before commencing to provide a designated service, a reporting entity must apply to AUSTRAC for enrolment on the Reporting Entities Roll. The Reporting Entities Roll provides AUSTRAC with essential information to:

    - identify businesses subject to AML/CTF obligations and appropriately monitor and supervise those reporting entities for compliance with the Act, Rules and Regulations
    - understand the nature, size and complexity of businesses subject to regulation
    - communicate effectively with these entities, including developing appropriate guidance and education materials
    - provide access to AUSTRAC online reporting systems
    - identify what designated service each reporting entity provides.

12. In complying with the requirement to apply for enrolment and keeping enrolment details up to date, reporting entities are required to provide personal information. The following are examples of the types of personal information reporting entities are required to provide in an enrolment application, as included in section 3-3 of the Rules:

    - the names of any beneficial owners of the applicant
    - the full name, and any former names, of each director, including the date of birth of each director
    - if the applicant is a partnership, and the partner is an individual who has, or is a member of a group of individuals who have, primary responsibility for the governance and executive decisions of the partnership, that individual's full name, and any former names of the individual, including the individual's date of birth
    - associations the applicant is a member of that represent the interests of a particular industry, profession or trade
    - the full name of the individual completing the application
    - full name, job title or position and email address of a person AUSTRAC can communicate with.

13. Not all enrolment information required to be provided by a reporting entity is necessarily personal information about a reporting entity or its employees. To the extent that such enrolment information is not of a personal nature, nor identify a particular individual, no human rights are engaged.

14. Any information, including personal information, provided to AUSTRAC as part of the enrolment process would be considered to be 'AUSTRAC information'. As such, it would be subject to the secrecy and access provisions outlined in Part 11 of the Act, which restrict access, use or disclosure of AUSTRAC information to a limited range of legitimate purposes.

15. To the extent the provisions that relate to enrolment with AUSTRAC in Part 3 of the Rules would constitute an impact or limitation on the protection against arbitrary or unlawful interference with privacy, any interference is reasonable, necessary and proportionate for AUSTRAC to fulfil its role as AML/CTF regulator which, in turn, necessitates AUSTRAC to know and understand its regulated population.

Registration requirements

16. Parts 6 and 6A of the Act require remittance service providers (RSPs) and virtual asset service providers (VASPs) to apply to AUSTRAC for registration on the Remittance Sector Register (RSR) and the Virtual Asset Service Provider Register (VASP Register). These Parts of the Act implement FATF recommendation 26 which requires countries to take the necessary legal or regulatory measures to prevent criminals or their associates from holding, being the beneficial owner of, or holding a significant or controlling interest in, or holding a management function in a remittance service provider (RSP) or virtual asset service provider (VASP).

17. FATF recommendation 26 provides that, at a minimum, countries must ensure that a business providing a value transfer service or virtual asset service should be licensed or registered and subject to effective systems for monitoring and ensuring compliance with national AML/CTF requirements.

18. FATF recommendation 27 also requires countries to empower supervisors to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the financial institution's license.

19. Part 4 of the Rules represents a more transparent and robust entry process to registration, bolstering Australia's regulatory framework for RSPs and VASPs by broadening the range of information AUSTRAC collects and considers when assessing an application for registration. Additionally, and to address regulatory gaps, the amendments to the Act capture additional virtual asset services. By extending AML/CTF regulation to additional virtual asset-related services for VASPs, this will result in an increased number of businesses in relation to whom information is collected by AUSTRAC for the purposes of registration.

20. Division 2 of Part 4 of the Rules sets out the information required for registration applications. The information that must be contained in a registration application made under subsections 75B(1) and (2), and 76D(1) of the Act, includes personal information such as:

    - information relating to the key personnel of the candidate (such as their full name, criminal and civil penalty history, date and place of birth and residential address)
    - information about beneficial owners of the candidate (such as their full name, residential address, date and place of birth, and a unique identifier given to them by an Australian government body or foreign government)
    - information about the individual completing the application (such as their full name, job title, date of birth, telephone number, email address and postal address)

- information about directors of candidates that are a body corporate (such as their full names, date and place of birth)
- information about partners in a candidate that is a partnership, or certain individuals such as trustees and beneficiaries relating to a trust (such as their full name, residential address, date and place of birth and a unique identifier).

21. The increased standard and level of information required for registration applications is to assist with mitigating and managing the risk of money laundering, the financing of terrorism, and other serious crime that are inherent to these sectors. Remittance services and virtual asset services were assessed in AUSTRAC's 2024 Money Laundering National Risk Assessment of Australia (ML NRA) as high and medium-high vulnerability for money laundering. Both were assessed in AUSTRAC's 2024 Terrorism Financing National Risk Assessment of Australia (TF NRA) as highly vulnerable to misuse for terrorism financing. This is because, in part, remittance and virtual asset service providers are subject to less oversight and regulation than other financial sub-sectors.

22. The nature of RSPs and VASPs, which deal with the transfer of funds and transfers of value and often operate across borders, inherently carries a high risk of being exploited for illicit activities. Therefore, a comprehensive understanding of the proposed RSP or VASP, its owners, key personnel, and customers is necessary for AUSTRAC's effective regulation and ML/TF risk mitigation.

23. The information to be collected by AUSTRAC as part of the registration application is considered a necessary and proportionate measure to achieve AUSTRAC's legitimate regulatory objectives. This is because the information requested by AUSTRAC is directly relevant to assessing the proposed RSP or VASP's suitability and its ability to comply with its AML/CTF obligations should it be registered as a RSP or VASP on the RSR or VASP Register, respectively.

24. Any information, including personal information, provided by RSPs or VASPs to AUSTRAC as part of their registration application process would be considered to be 'AUSTRAC information'. As such, it would be subject to the secrecy and access provisions outlined in Part 11 of the AML/CTF Act, which restrict access, use or disclosure of AUSTRAC information to a limited range of legitimate purposes.

25. To the extent the provisions in Part 4 of the Rules in relation to registration applications would constitute a limitation on the protection against arbitrary or unlawful interference with privacy, any interference is reasonable, necessary and proportionate.

Changes to CDD requirements

26. Part 2 of the Act prescribes requirements in relation to CDD, which are supplemented by Part 6 of the Rules. The CDD framework requires reporting entities to identify their customer(s) and certain other people (including individuals) through initial CDD and monitor them on an ongoing basis.

27. For example, Part 6 of the Rules set out:

- requirements for a reporting entity to establish the source of funds and source of wealth for particular customers
- circumstances where providing designated services before initial CDD is complete is permissible
- circumstances where alternative identity verification is permissible, and
- specific enhanced CDD requirements for foreign politically exposed persons (PEPs), high-risk domestic and international organisation PEPs, and designated services provided as part of nested service relationships, consistent with international standards.

28. Combined, the provisions in the Act and Rules clarify the focus on effective risk mitigation in the AML/CTF regime. That is, reporting entities are required to collect personal information that enables them to establish the identity of its customers and certain other individuals on reasonable grounds and identify their customer's ML/TF risk, and to apply appropriate measures to manage and mitigate the risks they may be exposed to, such as by seeking further customer information.

29. Personal information will only be collected to fulfil these requirements and the type of information collected will be appropriate to the customer's identified ML/TF risk. In some cases, such as where enhanced CDD is required, a reporting entity may need to collect additional personal information about a customer.

30. In addition to AML/CTF obligations, reporting entities under the AML/CTF Act are responsible entities under the *Privacy Act 1988* (even where other exemptions may usually apply—see section 6E of that Act), and are required to comply with the Australian Privacy Principles including the requirement to implement data protection policies, systems and controls in place where they collect and handle personal information.

31. To the extent the CDD requirements in Part 6 of the Rules constitute a limitation on the protection against arbitrary or unlawful interference with privacy, the legislative requirements and other safeguards ensure that any interference is reasonable, necessary and proportionate.

Transfer of value requirements for ordering and beneficiary institutions

32. Part 5 of the Act contains requirements to require information, including limited personal information, to 'travel' with the transfer of value for financial institutions, remittance providers and VASPs, for both domestic and cross-border transfers.

33. Part 8 of the Rules supplement the requirements in Part 5 of the Act to prescribe the types of information which an ordering and beneficiary institution needs to, depending on the circumstances:

- collect
- verify, and
- if applicable, pass on to the next institution in the value transfer chain.

34. Such information includes ‘payer information’ and ‘tracing information’ (both defined in section 1-4 of the Rules) or ‘card number of the card’.

35. In particular:

    - section 8-3 of the Rules prescribes the obligations of ordering institutions in relation to the collection, verification and passing on of different types of information in different circumstances
    - section 8-4 of the Rules prescribes the obligations of beneficiary institutions to monitor the receipt of particular information from an ordering institution in different circumstances
    - section 8-5 of the Rules prescribes the obligations of intermediary institutions to monitor the receipt of particular information and pass on information in different circumstances.

36. The types of personal information collected by ordering, beneficiary and intermediary institutions as required by sections 8-3 to 8-6 of the Rules include:

    - payer information, which includes the payer’s full name, and if that payer is an individual, the payer’s date of birth, place of birth and residential address, and
    - tracing information, which includes the address of a custodial wallet if the transfer of value is for a transfer of a virtual asset from a custodial wallet or the address of a self-hosted virtual asset wallet if the transfer of value is for a transfer of a virtual asset from a self-hosted virtual asset wallet.

37. Consistent with FATF recommendation 16, the inclusion of limited personal information travelling with transfers of value would ensure that basic information is immediately available to:

    - law enforcement agencies to assist them to detect or investigate terrorists or other criminals, and trace their assets
    - AUSTRAC, for analysing suspicious or unusual activity and disseminating as necessary, and
    - financial institutions, remitters and VASPs to facilitate the identification and reporting of suspicious transactions and take appropriate actions.

38. Reporting entities under the AML/CTF Act are responsible entities under the *Privacy Act 1988* (even where other exemptions may usually apply—see section 6E of that Act), and are required to comply with the Australian Privacy Principles including the requirement to implement data protection policies, systems and controls in place where they collect and handle personal information.

39. To the extent that transfer of value provisions would constitute a limitation on the protection against arbitrary or unlawful interference with privacy, any interference is reasonable, necessary and proportionate.

Suspicious matter reports and threshold transaction reports

40. As part of a reporting entity complying with its AML/CTF obligations, it must report certain transactions and suspicious matters to AUSTRAC. These reports include:

    - a suspicious matter report (SMR) if it suspects on reasonable grounds that a customer is not who they claim to be, or the provision of a designated service to a customer relates to any one of the following:
        i. financing of terrorism
        ii. money laundering
        iii. an offence against a Commonwealth, State or Territory law
        iv. proceeds of crime
        v. tax evasion.
    - a threshold transaction report (TTR) if it provides a designated service that involves the transfer of physical currency (cash) of $10,000 or more (or the foreign currency equivalent). A transfer can include receiving or paying cash.

41. The following are examples of the types of personal information reporting entities are required to provide to AUSTRAC in a SMR in relation to a person whom the suspicion relates:

    - the individual's full name, date of birth, gender, residential address, telephone number and email address
    - the country or countries of which the individual is a citizen
    - information on the individual's occupation, business or principal activity
    - a unique identifier for the individual
    - a description of the data used to verify a customer's identity
    - if the person's identity was not established, a description of the individual
    - if the matter involves virtual assets, the full name of any person who controls, or controlled, the virtual asset, and the full name of any person in whose name the assets are, or were, held
    - if the matter involves online activity by any person involved in the matter, information about the online activity, including unique network identification numbers for the networks used by the person, such as an Internet Protocol (IP) address.

42. Similar information is required to be provided to AUSTRAC in a TTR.

43. This personal information includes (if applicable and to the extent known by the reporting entity): full name, other names the individual is commonly known by, the individual's date of birth, their gender, residential address, telephone number, email address used by the person,

44. Any personal information provided to AUSTRAC as part of these reports will be considered to be 'AUSTRAC information'. As such, this 'AUSTRAC information' will be subject to the secrecy and access provisions outlined in Part 11 of the Act, which

restrict access, use or disclosure of AUSTRAC information to a limited range of legitimate purposes.

45. As for the types of information collected in these reports, Divisions 1 and 2 of Part 9 of the Rules prescribe the information that must be contained in a SMR and TTR respectively. SMRs provide AUSTRAC with essential information, including:

    - information about the person in relation to whom the SMR obligation arises for the reporting entity
    - information about the suspicious matter that a reporting entity must include in a SMR.

    TTRs provide AUSTRAC with key data, including:

    - information about the customer to whom the designated service was provided; and
    - information about the threshold transaction, including the amounts and persons involved, or affected by, the transaction.

46. The information AUSTRAC receives within SMRs play a crucial role in identifying illegal activity and assists in the detection and prevention of the flow of illegal funds through Australia's financial system. The information received from TTRs provide AUSTRAC with insights into transaction activity that involve large sums of cash within the reporting entity population. This assists AUSTRAC with a broader understanding on the flows of physical currency around Australia. Additionally, the information collected in both SMRs and TTRs allows AUSTRAC to receive more granular, specific, and useful information that enables AUSTRAC to more accurately and, with a level of degree of certainty, identify the person to whom the reports relate.

47. Although the provision of personal information by reporting entities to AUSTRAC in SMRs and TTRs limits the right to privacy of the individuals to whom are the subject of those reports, the limitation is reasonable, necessary and proportionate in achieving the legitimate objectives of Australia's AML/CTF regime. Requiring reporting entities to provide timely information in relation to the suspected commission of an offence is crucial for detecting and preventing crimes like money laundering and the financing of terrorism. Appropriate safeguards exist to ensure that any use of an individual's personal information is reasonable and proportionate. To the extent the reporting obligation requirements in Part 9 of the Rules constitute a limitation on the protection against arbitrary or unlawful interference with the privacy of a person, any interference is reasonable, necessary and proportionate.

48. In addition to safeguards within the AML/CTF Act, both reporting entities and AUSTRAC also have Australian privacy law obligations in relation to the collection, storage and disclosure of personal information.

Right to life; freedom from torture or cruel, inhuman or degrading treatment or punishment

49. Article 6 of the ICCPR recognises and protects the right to life of all persons. The right to life provides that no one shall be arbitrarily deprived of life and that this right shall be protected by law. It is a non-derogable right that cannot be suspended.

50. Article 7 of the ICCPR recognises the freedom from torture and other cruel, inhuman or degrading treatment or punishment. This is an absolute right that cannot be limited.

51. Section 127 of the Act permits certain government entities to disclose 'AUSTRAC information' to foreign governments. Section 10-1 of the Rules prescribes the Commonwealth, State and Territory agencies that are permitted to share AUSTRAC information to foreign governments.

52. Consequently, these provisions may engage the right to life and freedom from torture and other cruel, inhuman or degrading treatment or punishment if information is disclosed to foreign governments and entities, particularly information about alleged criminal activity, that may expose a person to a risk of the death penalty or to torture or other cruel treatment.

53. There are safeguards in place to ensure these rights are not limited. Section 127 of the Act provides that the AUSTRAC CEO, or the head of a prescribed agency or department as set out in the Rules, may disclose AUSTRAC information to a foreign country or agency where it is appropriate, in all the circumstances of the case, to do so. Further, the government of the foreign country, or the foreign agency, must give an undertaking for:

    - protecting the confidentiality of the information
    - controlling the use that will be made of the information, and
    - ensuring that information will be used only for the purpose for which it is disclosed to the government of the foreign country or to the foreign agency.

54. Section 10-1 of the Rules limits the agencies that are permitted to share AUSTRAC information with foreign countries. Prior to the reform of the AML/CTF Act in 2024, the list of agencies was contained in the AML/CTF Act.

55. Information can only be disclosed to a foreign government if it is appropriate to do so in all the circumstances of the case. For example, it would not be appropriate to share information if it would result in limitations to a person's right to life, or freedom from torture or cruel, inhuman or degrading treatment or punishment.

56. Australia's *Strategy for Abolition of the Death Penalty* (the Strategy) (accessible at: *https://www.dfat.gov.au/sites/default/files/australia-strategy-abolition-death-penalty.pdf*) does not consider government-to-government assistance or international police cooperation in death penalty matters. However, it sets out that Australia opposes the death penalty in all circumstances for all people. The AML/CTF Rules do not contradict this position, and instead only permits information sharing with foreign countries if it is appropriate to do so in all circumstances of the case.

57. Government-to-government assistance or police cooperation is governed by the *Mutual Assistance in Criminal Matters Act 1987* (the Mutual Assistance Act), the *Extradition*

Act 1988 (the Extradition Act), section 8 of the *Australian Federal Police Act 1979* and the *AFP National Guideline on International Police-to-Police Assistance in Death Penalty Situations* (the AFP National Strategy). These frameworks contain safeguards to prevent information sharing from limiting the right to life and freedom from torture or cruel, inhuman or degrading treatment or punishment.

58. AUSTRAC is retaining its existing practices with regard to its foreign disclosures framework.

59. The agencies prescribed in section 10-1 of the Rules will likewise have an obligation to protect people from being killed, or from identified risks by virtue of Article 6 of the ICCPR.

Right to equality and non-discrimination, in Article 2, 16, and 26 of the ICCPR

60. Articles 2, 16, and 26 of the ICCPR provide for the right of equality and non--discrimination. All persons are equal before the law and are entitled without any discrimination to the equal protection of the law. Discrimination is prohibited, and laws should guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

61. Part 6 of the Rules relate to initial CDD, enhanced CDD and politically exposed persons (PEPs). Some provisions in this Part may indirectly limit this right by requiring reporting entities to apply additional measures to customers because of their occupation, place of residence within a country and their property. These measures may have a disproportionate impact on particular persons and groups, such as politically exposed persons (PEPs). The Rules require these individuals to be treated differently to manage and mitigate the higher ML/TF risk associated with providing them with designated services.

62. For example, before a reporting entity provides a designated service to a foreign PEP or high-risk domestic or international organisation PEP, they must establish their source funds and source of wealth. They must also seek senior manager approval to provide them with designated services. If a reporting entity has a business relationship with a customer, and the customer, their beneficial owner, or a person on whose behalf the customer is receiving a designated service, becomes a foreign PEP or a high-risk domestic or international organisation PEP, they must also review and, where appropriate, update and reverify the "Know Your Customer" information.

63. PEPs are individuals entrusted with significant public responsibilities and power. Their family members and close business associates are also considered PEPs under the FATF framework and the AML/CTF Act. The ML NRA indicated that PEPs can be an attractive target for bribery and corruption given their capacity to influence government spending and decision making. As such, they present a higher risk of ML/TF and require additional measures be applied to manage and mitigate these risks.

64. The provisions in the Rules do not restrict the ability for PEPs to receive designated services, unless, for example, they cannot establish their source of funds or source of wealth on reasonable grounds during initial CDD. A reporting entity may decide not to provide a designated service to any customer if it is unable to manage and mitigate the ML/TF risk of a customer.

65. Part 6 of the Rules supplements the requirements in Part 2 of the Act, and together ensure that CDD is applied in a way that is proportionate and appropriate to manage the ML/TF risk of a customer. This includes ensuring a reporting entity has enough information to identify the ML/TF risk of a customer, including inherently higher-risk customers like PEPs. This helps reporting entities to then apply appropriate measures to manage and mitigate the customer's ML/TF risks when providing them with a designated service. Further, approval from senior managers is an important way of ensuring that senior management has oversight of the business' ML/TF risks and can make informed decisions about how to manage and mitigate those risks. The Rules do not require a service to be denied because it involves a PEP.

66. The United Nations Human Rights Committee recognises that 'not every differentiation of treatment will constitute discrimination, if the criteria for such differentiation are reasonable and objective'. While the Rules may require additional measures to be applied to persons because of their occupation or country of residence, these measures are reasonable, necessary and proportionate to ensure a reporting entity can manage and mitigate the ML/TF risks associated with providing a customer with a designated service.

Right to Work—Article 6 of the ICESCR

67. Article 6 of the ICESCR recognises the right to work as a fundamental human right. It affirms that everyone has the right to the opportunity to gain their living by work which they freely choose or accept.

68. The following provisions in the Rules may engage the right to work enumerated in Article 6 of the ICESCR:

- the provisions in Division 4 of Part 5 of the Rules (relating to AML/CTF compliance officers); and
- section 5-8 of the Rules (relating to undertaking due diligence in relation to persons who are, or will be, employed or otherwise engaged by the reporting entity)
- the provisions in Divisions 2-5 of Part 4 of the Rules (relating to key personnel of those required to be registered with AUSTRAC on particular rolls).

AML/CTF compliance officers

69. For the purposes of Division 5 of Part 1A of the Act, an AML/CTF compliance officer must be a resident of Australia, be a fit and proper person, and meet any further requirements specified in the Rules. Division 4 of Part 5 of the Rules gives effect to the provisions in the Act by specifying the matters that a reporting entity must have regard to

in determining whether an individual is a fit and proper person for the purposes of paragraph 26J(3)(b) of the Act.

70. The requirement for an AML/CTF compliance officer of a reporting entity to be a 'fit and proper' person may engage the right to work in Article 6 of the ICESCR, but does not necessarily violate the right. 'Fit and proper' is intended to be understood with its ordinary meaning, including concepts of honesty and competency.

71. The role of the AML/CTF compliance officer in a reporting entity involves ensuring that an entity complies with its AML/CTF obligations. This position requires a high level of integrity and trustworthiness. As such, requiring an individual in this role to meet 'fit and proper' requirements is a legitimate and proportionate safeguard, especially within the context and objectives of the AML/CTF regime—which is, ultimately, to detect, deter and disrupt money laundering, the financing of terrorism, and other serious financial crimes (section 3 of the Act).

Personnel due diligence

72. Subsection 5-8(2) of the Rules require the AML/CTF policies of a reporting entity to include due diligence procedures that assess:

- the person's skills, knowledge and expertise relevant to the particular responsibilities of the person under the AML/CTF policies, and
- the person's integrity.

73. This due diligence needs to occur both before a person's employment or engagement and during a person's employment or engagement.

74. A reporting entity's personnel are the frontline for identifying, managing and mitigating the risks of money laundering, terrorism financing and other serious crime. Without suitably-qualified and trustworthy personnel, a reporting entity cannot adequately comply with its obligations under the AML/CTF regime and, indeed, could put themselves in a position where they are facilitating serious and organised crime. This could be in the context of a person not properly performing their duties because they do not have the requisite skills. At worse, and without adequate due diligence procedures, a reporting entity could engage a person who themselves is a criminal or terrorist, or has active connections to such individuals, and the activities of the reporting entity are used to further these illegal activities, or shroud illegal activity.

75. Requiring a reporting entity to have personnel due diligence polices in place and undertake due diligence prior to the engagement of personnel and on an ongoing basis could be seen as engaging the right to work in that certain individuals——because of their lack of experience, previous criminal history or criminal associations——may be denied employment with a reporting entity.

76. However, requiring a reporting entity to have personnel due diligence policies in place is a legitimate and proportionate safeguard, especially within the context and objectives of

the AML/CTF regime—which is, ultimately, to detect, deter and disrupt money laundering, the financing of terrorism, and other serious financial crimes (section 3 of the Act).

Key personnel

77. Key personnel are individuals who would be the governing body or senior manager of the reporting entity once registered, the beneficial owner of the reporting entity, and the AML/CTF compliance officer of the reporting entity.

78. Section 4-9 sets out information regarding key personnel of the candidate that must be included in a registration application. Sections 4-15, 4-17 and 4-25 of the Rules allows the AUSTRAC CEO, in deciding whether to register a person, or to suspend or cancel a person's registration respectively, to have regard to:

- any offences of which key personnel have been charged or convicted under the law of the Commonwealth, a State or Territory or a foreign country
- whether key personnel have experience that is appropriate, having regard to the nature, size and complexity of the candidate's business and the risks of money laundering, financing of terrorism and proliferation financing that the candidate may reasonably face in providing its registrable services.

79. Additionally, suspension and cancellation decisions can involve consideration of whether the person or key personnel:

- have been found by a court to have contravened the Act, the regulations or the AML/CTF Rules
- have been the subject of civil or criminal proceedings, or a regulatory or disciplinary process in Australia or a foreign country that:
    i. related to the management of an entity, or commercial or professional activity; and
    ii. involved an adverse finding as to the competence, diligence, judgement, honesty or integrity of the person or the key personnel (as applicable); or
- are committing, continuing or repeating a contravention of the Act, the regulations or the AML/CTF Rules.

80. The key personnel provisions may engage the right to work in that certain individuals—— because of their lack of experience, previous criminal history or criminal associations—— may be excluded from being a key personnel of a reporting entity who is seeking to be obtain or maintain registration.

81. A reporting entity is required to identify, manage and mitigate the risks of money laundering, terrorism financing and other serious crime while meeting their other obligations under the Act and Rules. Key personnel have influence and power in and over a reporting entity that provides registrable services. As such it is appropriate that the

relevant criminal history, integrity and skill of key personnel is taken into consideration when making registration decisions.

82. To the extent that the provisions of the Rules may reduce a person's right to work, these limitations are reasonable, necessary and proportionate to address the risks of money laundering, and financing of terrorism, proliferation financing and other serious financial crime.

Conclusion

83. The Rules Instruments engage with a number of human rights and, to the extent the Rules limits some rights, those limitations would be reasonable, necessary and proportionate, and facilitate the overarching legitimate objectives of the AML/CTF regime. To the extent the Rules engage with other rights, there are safeguards in place to avoid those rights being limited.

Dr John Moss AIM

Acting Chief Executive Officer

Australian Transaction Reports and Analysis Centre