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: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation
FATF methodology	Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT/CPF Systems
IVTS	International value transfer services
ML/TF	Money laundering and terrorism financing
PEP	Politically exposed person
RNP	Remittance network provider
RSP	Remittance service provider
RSR	Remittance service register
SMR	Suspicious matter report given to the AUSTRAC CEO under section 41 of the AML/CTF Act

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

Section 1-1—Name

6. Section 1-1 provides that the title of the instrument is the *Anti-Money Laundering and Counter Terrorism Financing Rules 2025* (the Rules).

Section 1-2—Commencement

7. Section 1-2 provides that the Rules commence on 31 March 2026.

Section 1-3—Authority

8. Section 1-3 provides that the authority that the Rules are made under is the *Anti-Money Laundering and Counter Terrorism Financing Act 2006.*

Section 1-4—Definitions

9. 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.

10. 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.

11. 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.

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

13. 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.

14. 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.

15. ***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 to maintain status as a participant.

16. ***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.

17. The definition of ***card based pull 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.

18. 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.

19. ***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).

20. **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.

21. 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.

22. ***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).

23. The definition of ***foreign company*** provides that the meaning of the term given by 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.

24. ***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).

25. The definition of ***independent evaluation report*** is given by paragraph ^4 7(2)(d) 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.

26. 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.

27. The definition of ***passport*** defines the term to include an Australian passport issued under the *Australian Passports Act 2005*, as well as passports or similar international travel documents that contain contains a photograph and the signature of the person in whose name the document is issued; and is issued by a foreign government, the United Nations or an agency of the United Nations.

28. The definition of ***payable-through accounts*** refers to section ^6-1(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.

29. The definition of ***payee information*** sets out information about the payee in a transfer of value which is ordinarily required to be 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 beneficiary information' in FATF recommendation 16.
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. The definition of ***registrable services*** is:
    - 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.

32. The definition of ***super agent*** is given by subsection 3-13(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.

33. 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 that FATF recommendation 16 indicates should be included with domestic transfers of value in certain circumstances.

34. 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.

35. 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.

36. A unique identifier given to the person by an organisation accredited by the Global Legal Entity Identification Foundation, 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 are 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.

37. 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 7 of the Rules.

38. 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 Fie Number) Rule 2015* prohibits collection, use or disclosure of tax file number information unless this is permitted under taxation, personal assistance or superannuation law.

39. 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.

Sections 1-5 -- Domestic politically exposed person

40. 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 offices 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.

41. Paragraphs (a) to (f) are straightforward on the text of the Rules.

42. 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

43. 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.

44. 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.

45. Paragraph (i) specifies that heads, regardless of the title of the position, of Departments of State of a State or Territory 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.

46. Paragraph (j) specifies heads (however described) and members 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.

47. Paragraph (k) specifies the head (however described), or member of the governing body, whose staff can be investigated for corruption or other integrity issues by a State or Territory anti-corruption or integrity body. At present those bodies are:
    - the Independent Commission Against Corruption formed under the *Independent Commission Against Corruption Act 1988 (NSW)*
    - the Independent Broad-based Anti-corruption Commission formed under the *Independent Broad-based Anti-corruption Commission Act 2011 (Vic)*
    - the Crime and Corruption Commission formed under the *Crime and Corruption Act 2001 (Qld)*
    - the Independent Commission Against Corruption formed under the *Independent Commission Against Corruption Act 2012 (SA)*
    - the Corruption and Crime Commission formed under the *Corruption and Crime Commission Act 2003 (WA)*
    - the Integrity Commission formed under the Integrity Commission Act 2009 (Tas)
    - the Independent Commissioner Against Corruption formed under the *Independent Commissioner Against Corruption Act 2017 (NT)*
    - the ACT Integrity Commission formed under the *Integrity Commission Act 2018.*

48. Each integrity or anti-corruption body publishes information on the bodies over which it has oversight. They are generally bodies that are publicly funded and have decision making authority with respect to the rights of individuals or funding. Examples include State and Territory Departments of State, police forces, statutory bodies, and regulators.

49. 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 rights of individuals, valuable

contracts, law enforcement operations as well as decision making on potentially lucrative matters such as infrastructure development and access rights to local resources.

50. 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 website.

51. 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.

52. 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.

Section 1-6—Enrolment details

53. Section 1-6 specifies that enrolment details for the purpose of section 5 of the Act are the information mentioned in section 2-2 and 2-3 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.

Section 1-7—Registrable details

54. Section 1-6 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.

Section 1-8—Transfer of value—excluded transfers

55. 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)-(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.

Sections 1-9 and 1-10—Reporting groups

Reporting Groups

56. The amendments to the AML/CTF Act relating to reporting groups are set out in Part 1 of the Act. The amendments replace the existing 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 (if any) 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.

57. The intention behind the establishment of reporting groups is to require management and mitigation of ML/TF risk, and AML/CTF compliance management, at the group level, 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 reflects how 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 without the need for authorisation under the principles of agency. 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 10-2 and 10-3 of the Rules are satisfied.

58. Reporting groups are mandatory where there is control between persons, but in all other circumstances are optional.

Reporting group that is a business group

59. For the purposes of a reporting group to which paragraph 10A(1)(a) of the Act applies, subsection 1-9(1) outlines the requirements which must be satisfied if the members agree on a member being the lead entity. In addition to the members of the group reaching an agreement as to which member is to be the lead entity, that member must also satisfy the requirements outlined in paragraphs 1-9(1)(a) to (c) of the Rules.

60. The requirement in paragraph 1-9(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.

61. The requirement in paragraph 1-9(1)(b) is that the member who is to be the lead entity must have capacity to determine AML/CTF policies of other members in the group. This may be by virtue of the lead entity owning other members 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.

62. The requirement in paragraph 1-9(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.

63. Subsection 1-9(2) of the Rules specifies who the lead entity is in the reporting group that is a business group if the members of the group do not agree on a lead entity that meets the requirements in subsection 1-9(1) of the draft Rules (or do not turn their mind to nominating a lead entity). In circumstances where subsection 1-9(2) of the Rules is inapplicable due to 2 or more persons in the group who satisfy paragraph 1-9(2)(a) and control an equal number of members of the group who provide a designated service, paragraph 1-9(3) provides tie-breaker mechanisms to prescribe who the lead entity of the reporting group is.

64. Subsection 1-9(4) of the Rules specifies that a reporting group to which paragraph 10A(1)(a) of the Act applies is ineligible to be a reporting group if the person in the group who controls each other person only has that control by reason of the person's capacity roles and functions outlined in paragraphs 1-9(4)(a) to (h). It is not the intention of the provisions in the AML/CTF Rules that pertain to reporting groups to make an insolvency practitioner/ administrator a lead entity of a reporting group, or a member of a reporting group, due to the control they obtain when appointed as any of the positions in paragraphs 10-9(4)(a)-(h).

Reporting group formed by election

65. Subsection 1-10 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.

66. 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 1-10(2)(a) to (c) of the Rules.

67. The requirement in paragraph 1-10(2)(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.

68. The requirement in paragraph 1-10(2)(b) 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.

69. The requirement in paragraph 1-10(2)(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.

70. Subsection 1-10(3) requires that where a person wants to join an existing reporting group, the lead entity of the reporting group must provide consent.

71. Subsections 1-10(4) and (5) deal with the conditions for a member to leave a reporting group. Under subsection 1-10(4), an ordinary members (a member that is not the lead entity) may leave a reporting group if it gives the lead entity notice in writing. Under subsection 1-10(5), a lead entity may leave a reporting group if it gives the other members notice in writing.

72. Subsection 1-10(6) sets the conditions for the continual operation of a reporting group formed by election. Paragraph 1-10(6)(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 1-10(6)(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 1-10(6) 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.

Part 2—Enrolment

73. Part 2 of the Rules deals with the Reporting Entities Roll established under Part 3A of the Act.

74. 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

75. 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.

76. 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.

Section 2-1—Purpose of this Division

77. Section 2-1 provides the purpose of Part 2, 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.

Section 2-2—Information about applicant's designated services

78. Section 2-2 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.

79. Paragraphs 2-2(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 2-2(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 2-2(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 2-2(1)(d).

80. Paragraph 2-2(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.

81. Paragraphs 2-2(2)(a)-(c) requires the applicant to advise whether it is registered, or intends to register on the RSR for VASPR.

82. Subsection 2-2(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 certain gambling services in circumstances where the entity and any related entity that is a reporting entity are entitled to operate no more than 15 gaming machines under State or Territory licences.

83. Subsection 2-2(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 a designated service. Reporting entities who provide only designated services of that kind are subject to fewer obligations under the Act (see sections 26T, 30(10), 39(7), 44(6), 47(5)).

Section 2-3—Information relating to the applicant

84. Section 2-3 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.

85. Information provided by an applicant under subsections 2-3(1)-(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.

86. Some of the information, such as that required under 2-3(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.

87. Paragraph 2-3(1)(g) 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 affiliates with the applicant.

88. Paragraph 2-3(1)(m) 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).' Accordingly, if a reporting entity named Dazzling Bullion Pty Ltd sold bullion through two website domains: dazzlingbullion.com.au and dazzlingbullionoutlet.com.au, it would provide both of those domain names. If Dazzling Bullion had another website domain dazzlingbulliongallery.com.au which it used to showcase a gallery of products, but through which no sales or purchases were conducted, it would not need to provide that website domain name.

89. Subsections 2-3(2) to (7) are straightforward on the face of the text.

90. Paragraph 2-3(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, and information about the lead entity if the applicant is a member of a reporting group but not the lead entity.

Section 2-4—Information about the person completing the application and declaration

91. Section 2-4 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

92. Division 2 of Part 2 of the Rules contain the sections 2-5 – 2-7, 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 mechanical provisions allow the AUSTRAC CEO to maintain an accurate up-to-date Reporting Entities Roll.

Section 2-5—Correction of entries in the Reporting Entities Roll

93. Section 2-5 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.

Section 2-6—Removal of name and enrolment details on AUSTRAC CEO's own initiative

94. Section 2-6 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.

Section 2-7—Request to remove entry from Reporting Entities Roll—required information

95. Section 2-7 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 Rill if he or she is satisfied that it is appropriate to do so, having regard to the matters in paragraphs 51G(3)(a)-(c) of the Act.

Division 3—Changes in enrolment details

Section 2-8—Changes in enrolment details

96. Section 2-8 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 section 2-8 is that any change to enrolment details set out in section 2-2 and section 2-3 of the Rules must be advised to the AUSTRAC CEO in the approved form within 14 days of the change arising.

Part 3—Registration

97. 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, they should be licensed or registered and subject to effective systems for monitoring and ensuring compliance with national AML/CTF requirements.

98. 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.

99. 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 persons 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 reflect parliament's intent to fill the gap by subjecting remitters and VASPs to registration with the AUSTRAC CEO.

100. 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.

101. 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.

102. 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.

103. 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.

104. Part 3 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.

105. The additional information collected in an application for registration will be a component of an effective mechanism to identity and prevent ML/TF risks in the financial system by preventing registration of, or imposing conditions on 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; and
- do not have the required capability or competency to be registered, within its existing resources.

106. Part 3 of the Rules streamlines the requirements for the RSR and VASP Register for reporting entities and AUSTRAC, further advancing the AML/CTF reform objectives of simplification and modernisation.

Division 1—Management of the RSR and VASP Register

Section 3-1—Correction of entries

107. 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.

108. 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 3-1(2) permits the AUSTRAC CEO to correct information which the AUSTRAC CEO reasonably believes is incorrect or incomplete.

109. Where the AUSTRAC CEO makes a correction of an entry under subsection 3-1(2), subsection 3-1(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.

Section 3-2—Publication of register information

110. Section 3-2 requires the AUSTRAC CEO to publish the following information from each entry on the RSR and the VASP register:

- the name of the person;
- any conditions to which the registration of the person is subject;
- 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.

111. 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.

112. 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.

Division 2—Information requirements for registration applications

113. Information required for registration applications in this Division represents the information the AUSTRAC CEO requires to make a decision under 75C and 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, being:
  - the candidate's ML/TF risk exposure and management of ML/TF risks;
  - the candidate's capability to meet AML/CTF obligations; and

114. Commonalties between 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.

Section 3-3—Purpose of this Division

115. Section 3-3 provides the purpose of Part 3, 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).

Section 3-4—Application—general information

116. Subsections 3-4(1) to 3-4(7) of the Rules prescribes the general identifying, ownership, operating structure information about the candidate proposed to be registered that must be included in a registration application made for the purposes of subsections 75B(1), 75B(2) and 76D(1) of the Act

3-5—Information relating to ML/TF risks

117. Section 3-5 sets out information relating to ML/TF risks a candidate faces in providing its proposed designated services which that be provided in a registration application. This information allows the AUSTRAC CEO to consider the ML/TF risks of the candidate, as well as the candidate's processes to undertake, review and keep up to date its ML/TF risk assessment.

3-6—Information relating to AML/CTF policies

118. Section 3-6 sets out the information relating to the candidate's AML/CTF policies required under the Act which must be provided in a registration application. This information allows the AUSTRAC CEO to consider the candidate's policies, procedures, systems and controls to manage ML/TF risks it may reasonably face, as well as the candidate's ability to meet its AML/CTF obligations.

3-7—Information relating to accounts with financial institutions

119. Section 3-7 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 designated 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 database 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.

3-8—Information relating to other persons assisting

120. Section 3-8 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 designated services.

3-9—Information relating to key personnel and past unlawful activity etc.

121. Section 3-9 sets out information regarding key personnel of the candidate that must be included in a registration application. This includes whether the candidate or any of its key personnel have has 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;
- fraud (including scams);

- a serious offence (as defined in the Act) of any other kind.

122. Information about the candidate and its key personnel relating to contraventions under the Act, and other civil proceedings or enforcement action related to the commercial or professional activity is also required.

123. Information under 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.

3-10—Additional requirements for application by a remittance network provider for registration of an affiliate

124. Section 3-10 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 risks of ML/TF and proliferation financing that the provider may reasonably face. Subsection 3-10(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.

3-11—Additional requirements for application by independent remittance dealer for registration as a remittance affiliate

125. Section 3-11 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.

3-12—Additional requirements for application for registration as an independent remittance dealer or a remittance affiliate of network provider

126. Section 3-12 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.

3-13—Additional requirements for application for registration as a remittance affiliate of remittance network provider

127. Section 3-13 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.

3-14—Additional requirements for application for registration as a virtual asset service provider

128. Section 3-14 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

129. 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 AML/CTF Rules. Similarly, subsection 76E(2) of the AML/CTF Act sets out the same requirements for VASP registration although people smuggling risk is not a named risk factor.

130. 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.

131. 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.

Section 3-15—Registration decisions—matters to which AUSTRAC CEO must have regard

132. Section 3-15 of the Rules provide the matters to which the AUSTRAC CEO must have regard to in an application for registration. Section 3-15 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.

Division 4

133. The ability to suspend registrations is an important regulatory tool for AUSTRAC and complements the power to cancel or impose conditions on registration. The suspension powers give the AUSTRAC CEO the ability to respond to a wide range of operational circumstances and provide for the stopping of remittance or virtual asset services while matters are investigated.

Section 3-16—Purpose of this Division

134. Section 3-16 provides the purpose of Part 3, Division 4 of the Rules, which is prescribe requirements relating to suspension of registration for the purpose of section 75H and 76K of the Act.

Section 3-17—Suspension of registration

135. Section 3-17 specifies the grounds on which the AUSTRAC CEO may suspend a person's registration. The grounds specified are based on the matters that the AUSTRAC CEO must have regard to when determining whether it is appropriate to register a person.

136. Suspension of a person's registration will allow 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 registration.

137. The AUSTRAC CEO may suspend a registration if the AUSTRAC CEO has a reasonable suspicion of one of the matters in paragraphs 3-17(a)-(h) apply. This is an intentionally 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 further evidence or make further enquiries to inform whether to take further action.

Section 3-18—Effect of suspension—renewal and advising of certain matters

138. While a reporting entity cannot provide a registrable services while their registration is suspended, the effect of section 3-18 of the Rules is that the renewal of registration provisions set out in Division 6 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 3, Division 7 of the Rules.

Section 3-19—Period of suspension

139. Subsection 3-19(1) provides that suspension of registration has effect for a period of up to 3 months. Subsection 3-19(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 3-17 applies.

Section 3-20—Notice of suspension decision

140. Section 3-20 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 3-20(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 designated remittance services.

141. 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.

142. 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.

Section 3-21—Notice of extension of suspension

143. Following a decision by the AUSTRAC CEO under sections 3-17 and 3-19 to extend the suspension of a person's registration for a further period of time, section 3-21 of the Rules requires that the AUSTRAC CEO give to the person a written notice containing the information specified in subsection 3-21(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 designated remittance services.

144. 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.

145. 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 continue to be suspended.

Section 3-22—Register entry in relation to suspension of registration

146. Section 3-22 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 3-2 to be published on the AUSTRAC website.

147. The AUSTRAC CEO must remove the information from the register following the end of the suspension.

Division 5—Cancellation of registration

148. 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).

149. 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.

Section 3-23—Cancellation of registration

150. Section 3-23 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 replacing it with more detailed provisions that allow the AUSTRAC CEO to have regard to, among other matters;

- 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 sufficient experience in functions relevant to the person's obligations under the AML/CTF regime or functions relevant to providing registrable services.

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

152. The AUSTRAC CEO's requirement 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.

Section 3-24—Publication of cancellation information

153. 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.

154. The effect of section 3-24 of the Rules is that publication of the list of names and dates will be on the AUSTRAC website.

155. Publication of details of cancellation decision by the AUSTRAC CEO will inform reporting entities, foreign remittance service providers and VASPs and other persons regulated for AML/CTF when considering on the basis of ML/T risk whether to enter commercial relationships with another entity.

Division 6—Renewal of registration

156. 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, because the registration has been suspended or cancelled).

157. Renewal of registration provides ongoing and regular assessment by the AUSTRAC CEO of a RSP or VASPs suitability to maintain registration. Division 6 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. Previously registered persons will need to meet the new renewal of registration standards as prescribed in Part 3, Division 6 of the Rules when having a renewal application decided by the AUSTRAC CEO.

Section 3-25—Purpose of this Division

158. Section 3-25 provides the purpose of Part 3, 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.

Sections 3-26 to 3-31

159. These sections set out:

- the application process for the renewal of a person's registration (section 3-26);
- the period within which a renewal of application may be made (section 3-27);
- 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 3-28);
- the period for which renewed registrations have effect, being 3 years (section 3-29);
- 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 3-30); 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 3-31).

Division 7—Matters registered persons required to advise

160. 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.

161. 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.

Section 3-32—Matters registered persons required to advise

162. Section 3-32 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.

163. The matters specified at subsection 3-32(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

Section 3-33—Spent convictions

164. Section 3-33 preserves the primacy of the Commonwealth Spent Convictions Scheme in Part VIIC of the *Crimes Act 1914*. The provisions of Part 3 of the Rules do not override the Commonwealth Spent Convictions Scheme.

165. 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.

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

167. 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 3 of the Rules does not constitute such an exception.

Part 4—AML/CTF programs

Division 1—ML/TF risk assessment

Section 4-1 – Review of ML/TF risk assessment

168. 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.

169. The Act is largely self-contained in relation to ML/TF risk assessments. Section 4-1 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 independent evaluation report will contain adverse findings in relation to its ML/TF risk assessment where the report identifies or indicates instances of non-compliance with a reporting entity's ML/TF risk assessment obligations under Part 1A, Division 2 of the Act. For example, if the independent evaluation report identifies that the reporting entity has not adequately assessed its risks of ML, TF and proliferation financing that it reasonably faces in providing designated services, this would be an example of an adverse finding. 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.

170. 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

Section 4-2—Prevention of tipping off

171. 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.

172. Section 4-2 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.

173. The requirement in section 4-2 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.

174. 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 reduce the risk of tipping off when engaging with customers
- personnel training to enable them to understand the tipping off offence.

Section 4-3—Provision of information to governing body

175. 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.

176. 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
- that the reporting entity is complying with its AML/CTF policies.

177. Section 4-3 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 reporting entity and its governing body so it can exercise appropriate, ongoing oversight to fulfil its responsibilities under the Act.

Section 4-4—Reporting from AML/CTF compliance officer to governing body

178. 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 4-4 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.

179. '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 4-4 nonetheless requires that such reporting occur with a frequency of at least once every 12 months.

180. The Act contemplates that the distinction between a governing body, senior manager and AML/CTF compliance officer may be redundant for a sole trader, Accordingly, subsection 4-4(3) exempts a reporting entity from section 4-4 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..

181. Sections 4-3 and 4-4 are also intended to reinforce the important roles of the governing body and the AML/CTF compliance officer in the effectiveness of a reporting entity's AML/CTF program. Section 4-4 seeks to ensure a direct line of communication between the AML/CTF compliance officer and the governing body.

Section 4-5—Undertaking personnel due diligence

182. Paragraph 26F(4)(d) of the Act and section 4-5 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.

183. 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 4-5 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.

184. 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 thorough 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

identify personnel who might be involved in money laundering or other illicit activities, allowing for early intervention and prevention.

185. 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 to under the entity's AML/CTF Program.

186. 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.

187. 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 a higher risk role, the due diligence should be more rigorous than persons in lower risk roles.

188. 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.

189. 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 leveraged or used to supplement personnel due diligence checks for the purpose of fulfilling personnel due diligence requirements under the AML/CTF regime where the protocols are relevant to the reporting entity's personnel due diligence obligations and they are adequately documented within 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.

Section 4-6—Providing personnel training

190. 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.

191. Section 4-6 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.

192. 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 as relevant to the roles and responsibilities of the person.

193. The extent of the reporting entity's AML/CTF policies in relation to the provision of personnel training must reflect the nature, size, and complexity of the entity.

194. A reporting entity must ensure that training is provided to, and obtained by, a reporting entity's personnel or persons otherwise engaged by its relevant personnel. 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 have measures in place 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 for which such training is required. A reporting entity is required to keep records of providing training to employees in a way that demonstrates that the training ensures that the reporting entity complies with its obligations under the AML/CTF regime.

Section 4-7—Independent evaluations

195. 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. Section 26F(7)(a) provides the relevant head of power for the AML/CTF Rules to specify requirements that must be complied with in relation to section 26F(4).

196. Section 4-7 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.

197. 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 subsection 4-7(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.

198. 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 (subsection 4-7(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.

199. Under subsection 4-7(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 intended outcome of ML/TF risk mitigation and management in practice.

200. Subparagraphs 4-7(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), regarding the design and operational effectiveness of the reporting entity's AML/CTF policies.

201. Subparagraph 4-7(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 subparagraph 4-7(2)(d).

202. Paragraph 4-7(3) is provided to require that the reporting entity must document their approach to responding to the report described in paragraph 4-7(2)(d).

203. The word 'test' in paragraphs 4-7(2)(c) and (d) reflects FATF recommendation 18.

Section 4-8—Reviewing and updating AML/CTF policies following independent evaluation

204. Section 4-8 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/CTFC policies.

205. 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.

Section 4-9—Fulfilling reporting obligations

206. Section 4-9 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 charge. 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 AML/CTF 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).

207. Reports submitted to AUSTRAC that are complete, accurate and free from unauthorised charge 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.

208. Section 4-9 requires that in its AML/CTF policies, a reporting entity must provide policies, systems, procedures and controls which provide the reporting entity assurance that reports it gives to AUSTRAC under the Act are complete, accurate and free from unauthorised charge.

Section 4-10—Assessment of potential suspicious matters

209. Section 4-10 of the Rules requires that a reporting entity's AML/CTF policies must deal with timely review and determination of potential suspicious matters.

210. 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' have lessened the utility of SMRs to AUSTRAC and partner agencies in detecting and disrupting criminal activity. Section 4-10 will require AML/CTF policies to ensure such determination as soon as practicable.

Section 4-11—Actions requiring approval or that senior manager be informed

211. Section 4-11 deals with the requirement for reporting entities' policies to deal with decisions about accepting or continuing to provide designated services in higher ML/TF risk circumstances.

212. Subsection 4-11(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 5-24), 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.

213. Subsection 4-11(2) deals with circumstances where a reporting entity is providing designated services at or through a permanent establishment in a foreign country, requiring senior manager approval under subsection 4-11(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. 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.

214. Subsection 4-11(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 buy 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.

215. Subsection 4-11(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.

Section 4-12—Policies relating to financial sanctions

216. Section 4-12 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, 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.

217. Reporting entity's AML/CTF policies relating to targeted financial sanctions will enable a reporting entity to respond appropriately if or when they have a customer who is designated for targeted financial sanctions or is associated with a designated person or entity. It will also assist reporting entities in determining what to do with any value, virtual assets or property already held on behalf of the customer or subject to transactions being assisted by the reporting entity, to avoid their designated services being abused for sanctions-related ML/TF or proliferation financing offences. This will assist reporting entities from inadvertently dealing with frozen assets, or returning frozen assets to a sanctioned person in the mistaken belief that this will reduce risk.

Section 4-13—Policies relating to the obligations of ordering institutions relating to virtual asset transfers

218. Section 4-13 of the Rules sets out the requirements for a reporting entity who is an ordering institution for the transfer of a virtual asset (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 4-13(a) to (d).

219. 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 payee information which apply to all ordering institutions (whether transferring money, property or digital currency).

220. 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.

221. The AML/CTF policies of a reporting entity to which subsections 4-13(a) to (d) applies are required to deal with how relevant reporting entities will fulfil their obligations under Part 5 of the Act.

Section 4-14—Policies relating to the obligations of beneficiary institutions

222. Subsection 4-14(1) 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 4-14(1)(a) to (c) of the Rules in relation to the transfers of value to a payee.

223. 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 payee information (paragraph 16.13 of the FATF Methodology); and
- having risk-based policies and procedures for determining:
    - 223..1. when to execute, reject or suspend a wire transfer lacking required payer or required payee information; and
    - 223..2. the appropriate follow-up action (paragraph 16.15 of the FATF Methodology).

224. Under subsection 65(2) of the Act, beneficiary institutions are required to take reasonable steps to identify missing payer and payee information in a transfer of value (consistent with criterion 16.13 of the FATF methodology), and inaccurate payee information (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).

225. Paragraphs 4-14(1)(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 travel rule risk mitigation measures.

226. Subsection 4-14(2) of the Rules specifies that 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 4-14(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.

227. 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.

228. The FATF methodology requires beneficiary institutions who are virtual asset service providers to obtain and hold:

- required payer information; and
- required and accurate payee information

for virtual asset transfers and make it available on request to appropriate authorities (paragraph 15.9(b)(ii) of the FATF Methodology).

Section 4-15—Polices relating to the obligations of intermediary institutions

229. Section 4-15 of the Rules sets out the requirements for an intermediary institution that is 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 4-15(a) to (c) of the Rules.

230. 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 require 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:
  - 230..1. when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information, and
  - 230..2. the appropriate follow-up action (paragraph 16.12 of the FATF Methodology).

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

232. The matters specified in subsections 4-15(a) to (c) give effect to the above-mentioned FATF Methodology by requiring the AML/CTF policies of the reporting entity to which subsection 4-15 of the Rules applies to, to:

- take reasonable steps monitor whether the reporting entity has received the information specified in section 7-5 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.

Section 4-16—Policies relating to customer due diligence for real estate transactions

233. Section 4-16 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 section 5-15(e) of the Rules.

234. 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 necessary information to meet that verification obligation by way of that information sharing arrangement. Section 4-16 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 subsection 5-15(g) of the Rules.
- has verified the customer in accordance with its responsibilities allocated under the arrangement pursuant to subsection 5-15(g) of the Rules, but the level 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 subsection 5-15(g) of the Rules but does not share the KYC information or associated verification data with the relying reporting entity.

235. 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. Accordingly, an example of what a relying reporting entity may have in its AML/CTF policies to address the requirements under this rule in relation to such circumstances may be identifying alterative reliance and independent data sources that can be adopted to address this information gap. The intent of this section is to ensure that the relying reporting entity is prepared and can appropriately respond if such circumstances arise.

Section 4-17—Record keeping by lead entity of a reporting group

236. Section 4-17 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 1-9(1) to (3) of the Rules;
- forming a reporting group by election pursuant to subsection 1-10(1) of the Rules;
- a member of the reporting group satisfying the requirements prescribed in subsection 1-10(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 subsections 1-10(4) and (5) of the Rules

Division 3—AML/CTF compliance officers

Section 4-18—AML/CTF compliance officer requirements—matters to have regard to in determine whether a fit and proper person

237. Section 4-18 of the Rules outlines a number of matters which a reporting entity must consider in conducting fit and proper assessments of a 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 4-18(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 with regard to other fit and proper regimes. Such attributes are essential to the AML/CTF compliance officer functions, as the AML/CTF compliance officer is in a unique position to undermine the effectiveness of a reporting entity's AML/CTF regime if they have a lack of willingness to comply with legal obligations or is deceitful.
- whether the individual has been convicted of a serious offence, as defined in the Act.
- whether the individual was the subject of regulatory proceedings or administrative action 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.
- 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.

238. Subsection 4-18(2) confirms that paragraph 4-18(1)(c) does not affect the operation of the Commonwealth Spend 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 3-33 of the Rules.

Division 4—AML/CTF program documentation

Section 4-19—Time period for AML/CTF program documentation

239. Section 24 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.

240. 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 it 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.

241. The AML/CTF 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 AML/CTF 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.

242. 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.

243. Section 4-19 of the AML/CTF Rules only relates to the requirement to document updates to a reporting entity's ML/TF risk assessment and AML/CTF policies. Section 4-19 of the AML/CTF Rules does not relate to the time in which it takes a reporting entity to assess the impacts of the trigger for update, 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.

244. The requirement to '*document*' for the purposes of section 4-19 of the AML/CTF 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.

Part 5—Customer Due Diligence

Division 1— Matters to be established in initial customer due diligence

Section 5-1—Establishing the identity of the customer

245. Section 5-1 of the Rules sets out specific requirements for establishing the identity of customers under paragraph 28(2)(a) of the Act. The requirements relate to customers that are:

- not individuals, or
- receiving designated services in relation to the customer's business.

246. The requirements are to establish on reasonable grounds:

- the full name for a customer and any business names of the customer,
- a unique identifier (note that this term is defined in section 1-4),
- the customer's registered office address (if any), and
- the address of the customer's principal place of business or operations (if any).

247. This section applies to all designated service types.

248. The matters described in section align with the requirement under FATF recommendation 10 to verify the identity of legal persons and legal arrangements.

Section 5-2—Additional matters for initial customer due diligence

249. FATF recommendation 10 sets out a range of specific matters that should be included in CDD obligations for specific kinds of customers. In some cases, these go beyond the default 'matters' specified for customer in s 28(2) of the Act and are of a level of specificity that they are best dealt with through the Rules.

250. Section 5-2 of the Rules specifies these additional matters that a reporting entity must establish in accordance with its obligation under subsection 28(1) of the Act, for designated services provided at or through Australian permanent establishments. The scope of this section is confined to Australia 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 should comply with relevant foreign laws relating the CDD when providing services at or through foreign permanent establishments, while ensuring that they still meet the broad outcomes set out in subsections 28(1) and (2) of the Act.

251. Subsection 5-2(2) requires that reporting entities understand the nature of their customer's business. This is a separate concept from understanding 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. Understanding the nature of a customer's business is essential to effective ongoing CDD as it allows reporting entities to understand the kinds of designated services, and the types of transactions and behaviours to expect, as part of its dealings with the customer.

252. Subsection 5-2(3) sets out requirements related to establishing the ownership and control structure of non-individual customers. Understanding the ownership and control structure of a customer is essential to understanding the ML/TF risk of the customer and reinforces customer due diligence requirements related to beneficial owners in paragraph 28(2)(d) of the Act. Complex ownership and control structures are a well-known method used in efforts to obfuscate money laundering and proliferation financing activities. Together with subsection 5-2(2), subsection 5-2(3) addresses FATF recommendation 10 (specifically 10.8 in the FATF methodology).

253. Subsection 5-2(4) requires reporting entities to establish on reasonable grounds the legal or official documentation that sets out how the customer is governed, for example its constitution, partnership agreement or trust deed, unless one of the exceptions applies. Such documentation assists in proving the existence of a body corporate, trust or other legal arrangement and assists with establishing who the beneficial owners are for private companies, partnerships, trusts etc. The exceptions reflect that:

- individuals acting on their own behalf will not have such documents,
- control of government bodies is usually readily apparent in public information,
- the risks of providing designated services to listed public companies are reduced where disclosure requirements ensure transparency regarding the identity of any beneficial owner.

254. Subsection 5-2(5) requires reporting entities to establish the full name and director identification number, if any, of each eligible officer within the meaning of the *Corporations Act 2001*, which supplements the requirement in subsection 5-2(3) with respect to Australian bodies corporate and registered foreign companies.

255. Subsection 5-2(6) sets out the requirement to establish a range of matters in relation to a trust where the customer is a trustee, including the kind of trust, the full name of any settlor, and the identity of any appointor, guardian or protector of the trust. The subsection also applies to equivalents of trusts under foreign legal systems. This implements FATF recommendation 10 (10.11 in the FATF methodology).

256. Subsection 5-2(7) provides a fall back where a non-individual customer has no beneficial owner, requiring reporting entities to instead establish the identity of the individual, or each member of the group of individuals, with primary responsibility for the governance and executive decisions. This implements FATF recommendation 10 (10.10(c) in the FATF methodology).

Section 5-3—Establishing the identity of agents, beneficial owners, trustees etc

257. Section 5-3 of the Rules relates to circumstances where a reporting entity must establish the identity of a person other than the customer, such as a person acting on behalf of the customer (e.g. an agent or a person appointed under a power of attorney) or a beneficial owner of a customer. In such circumstances, the reporting entity must treat that person in the same manner as it would a customer in order to meet the relevant obligation under subsections 28(1) and (2) of the Act. This means that where a beneficial owner, for example, would qualify for simplified due diligence if they were the direct customer, then the beneficial owner will qualify for simplified due diligence under Rule 5-4.

Division 2—Simplified and enhanced customer due diligence

Section 5-4—Simplified customer due diligence requirements

258. The purpose of section 5-4 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 5-4 specifies that a reporting entity's AML/CTF policies must deal with simplified due diligence before it can undertake simplified measures.

Section 5-5—Customers for whom enhanced customer due diligence is required

259. 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 5-5 implements this requirement.

260. The Act nor Rules are prescriptive about what enhanced CDD measures require, but where enhanced CDD is to be applied to due the operation of section 5-5, enhanced measures may include:

- seeking additional independent, reliable sources to verify KYC information,
- 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
- increasing the monitoring of the customer, including greater scrutiny of transactions.

261. Enhanced CDD under this section may arise from monitoring undertaken as part of ongoing CDD 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.

Division 3—Exemptions from initial customer due diligence

262. Division 3 of Part 5 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 to after commencing to provide a designated service, despite its obligation under subsection 28(1) of the Act to do so beforehand.

263. 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.

264. 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.

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

Section 5-6—Delayed verification for certain identification requirements—service provided in Australia

266. 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 generally for any designated service provided at or through a permanent establishment in Australia for up to 30 days about:

- the identity of any person on whose behalf the customer is receiving the designated service, e.g. beneficiaries of an express trust;
- the identity of the beneficial owners of the customer; and
- any other matter relating to the customer that is specified in the Rules made under paragraph 28(2)(g) of the Act.

267. Section 5-6 allows for delayed verification of these matters, but reporting entities must still collect the KYC information about the identity of any person on whose behalf the customer is receiving the designated service, any beneficial owners of the customer, and any additional matters contained in Rules made under paragraph 28(2)(g) of the Act.

268. The option to delay verification under this section does not extend to:
- the identity of the customer,
- the identity of any person acting on behalf of the customer and their authority to act,
- 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 a PEP or a person designated for targeted financial sanctions (but see section 5-21, or 5-9 relating to delayed verification relating to PEPs and sanction screening)
- the nature and purpose of the business relationship or occasional transaction.

Section 5-7—Delayed initial due diligence—real estate transactions

269. Section 5-7 permits delayed initial CDD for the specified designated services involving sales, purchases or other transfers of real estate in some 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 (a such as a legal practitioner or conveyancer) acting for the buyer or transferee may delay initial CDD in relation to their client.

270. In all of these circumstances, initial CDD must be completed as soon as practicable but no later than the settlement of the sale, purchase or transfer of the real estate. This recognises that the ML/TF risk associated with the sale, purchase or transfer of real estate manifests at settlement, at which the purchase funds and the real estate change hands.

271. To benefit from delayed initial CDD under this section, the settlement of the sale, purchase or transfer of the real estate must be conditional on completion of initial CDD in relation to the customer.

272. This section recognises that in the circumstances set out above, it can disrupt the ordinary course of business to require initial CDD to be completed 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.

273. 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.

274. 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.

275. These delayed verification provisions are intended to operate alongside section 5-15 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, section 5-7 is not restricted to such arrangements.

Section 5-8—Delayed initial due diligence—service provided in foreign country

276. 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 5-8 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.

277. Section 5-8 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.

278. Consistent with FATF recommendation 10, delayed initial CDD under section 5-8 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,
- meets the reporting requirements in relation to managing and mitigating associated ML/TF risk, etc.

Section 5-9—Delayed initial due diligence for certain matters (politically exposed persons and sanctions)—service provided in Australia

279. Section 5-9 permits a reporting entity, where they have established all of the matters in subsection 28(2) of the Act, except in relation to whether the customer or associated person is a PEP to subject to targeted financial sanctions, to delay PEP and sanctions screening where the conditions in section 29 of the Act are met, including that the delay is essential to avoid interrupting the ordinary course of business and appropriate risk mitigations are implemented. In these circumstances, PEP and sections checks must be carried out as soon as reasonably practicable per section 29 of the Act. The permitted delayed verification applies to designated service provided at or through a permanent establishment in Australia (see section 5-8 for delayed verification in relation to services provided at or through foreign permanent establishments).

Section 5-10—Delayed verification—opening an account and deposit

280. Section 5-10 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 only to delayed verification of KYC information and not the collection 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.

281. 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). Transferring funds out of the account is not permitted until initial CDD is completed.

Section 5-11—Delayed verification—certain financial markets transactions

282. Section 5-11 substantively reproduces the delayed verification rules in Chapter 46 of the former rules. The section permits delayed verification of KYC information as part of initial CDD when specific kinds of designated services are provided on prescribed financial markets. The section requires that the verification must be completed as soon as reasonably practicable and no later than 5 business days after the day on which it first provided those relevant designated services to the customer. The intent is to address circumstances where the transaction must be performed rapidly due to financial market conditions relevant to the transaction. This section relates only to delayed verification of KYC information and does not extend to the collection of KYC information which must still be done before commencing to provide a designated service.

Division 4—Circumstances in which reporting entity taken to comply with requirements

283. Division 4 of Part 5 of the Rules provides regulatory relief to reporting entities where appropriate to the ML/TF risk by providing that reporting entities are taken to comply with initial or ongoing CDD obligations. The rules are made for the purpose of either:

- paragraph 28(6)(b) of the Act in relation to the initial CDD, or
- paragraph 30(3)(b) of the Act in relation to the ongoing CDD.

Section 5-12—Initial customer due diligence—previous carrying out of applicable customer identification procedure

284. Section 5-12 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 ACIP in relation to the customer prior to the commencement of these Rules.

Section 5-13—Initial customer due diligence—previous compliance in a foreign country

285. Section 5-1 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.

286. 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.

Section 5-14—Initial customer due diligence—establishing the identity of any person on whose behalf the customer is receiving the designated service

287. Section 5-14 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.

288. The principal situation under which a customer receives a designated service on behalf of another person under Australian law arises where a trustee receives designated services of behalf of beneficiaries of the trust (beneficiaries ordinarily do not 'control' the trustee 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 for 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.

289. Section 5-14 also sets out what a reporting entity must do to comply with section 28(2)(b) for trusts whose nature means it is not possible to identify each beneficiary.

Section 5-15—Initial customer due diligence—identity of beneficial owners of certain customers

290. Section 5-15 alters the requirement for reporting entities to establish the beneficial owners of the customer for certain kinds of customers that are generally considered lower ML/TF risk. This includes bodies corporate or legal arrangements that are, or are controlled by:

- a government body,
- an entity that is subject to oversight by a prudential, insurance, or investor protection regulator through registration or licensing requirements,
- a corporation or association of homeowners in a strata title or community title scheme, or
- a listed public company that is subject to public disclosure requirements (however imposed) that ensure transparency regarding the identity of any beneficial owners.

291. Where the ML/TF risk of the customer is low and enhanced customer due diligence is not triggered, it is sufficient for the purpose establishing the beneficial owners under paragraph 28(2)(d) of the Act that the reporting entity establishes on reasonable grounds that the customer is one of these kinds of customer.

Section 5-16—Initial customer due diligence—real estate transactions

292. Real estate transactions will ordinarily involve multiple reporting entities, each of which will be required to undertake initial customer due diligence under section 28 of the Act. AUSTRAC has received a number of proposals by industry bodies and businesses to provide services and platforms that:

- reduce duplication of CDD by facilitating reliance among the reporting entities involved in various stages of real estate transactions, and
- allow, where appropriate, for more complex aspects of customer due diligence (e.g. verification of PEP status, beneficial ownership of the customer, etc.) to be carried out by legal practitioners, conveyancers, financial institutions etc. rather than real estate agents—given legal practitioners, conveyancers and financial institutions are likely to better placed to undertake such due diligence despite potentially entering into a business relationship with the customer after the real estate agent has done so.

293. Section 5-15 of the Rules is designed to enable such arrangements. In relation to the specified kinds of designated services, a real estate agent or professional services provider will be taken to have complied 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.

294. 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. 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.

295. For a real estate agent or professional services provider to use this section, they must implement the safeguards specified in the section.

296. 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.

297. Further, initial CDD must be completed before settlement of the sale, purchase or transfer of the real estate. As it may not always be guaranteed that there will be another participating reporting entity in the same arrangement as the real estate agent, the real estate agent or professional services provider must also develop and maintain AML/CTF policies dealing with completing initial CDD before settlement where they do not receive the required verification data under the arrangement (see section 4-16).

298. The section is technology and platform neutral. This approach ensures that the flexibility afforded by this section is not limited to specific technologies or platforms.

5-17—Initial customer due diligence—individual cannot provide satisfactory evidence

299. Section 5-17 allows for alternative verification requirements for customers if:

- the customer is an individual, and
- is unable to provide information or evidence of identity because:
    - the customer is unable to obtain the information or evidence, or
    - the customer is unable to access the information or evidence due to circumstances beyond the customer's control.

300. These circumstances are intended to encompass customers who may not have access to standard verification methods, as they are:

- 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.

301. In these circumstances, the reporting entity may 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. 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 customer's identity.

5-18—Initial customer due diligence—transferred customer

302. Section 5-18 provides regulatory relief for initial CDD where a customer is transferred from one reporting entity to another as a result of:

- One reporting entity (the prior reporting entity) assigning, conveying, selling or transferring the whole of a part of its business to another reporting entity,
- One reporting entity (the prior reporting entity) being subject to a voluntary transfer under the *Financial Sector (Transfer and Restructure) Act 1999*,
- All or part of the assets and liabilities of another reporting entity (the reporting entity) become the assets and liabilities of another reporting entity as a result of a compulsory transfer under statute.

if the prior reporting entity also provides copies of the records kept by the prior reporting entity under sections 107, 108, 111 and 114 of the Act in relation to the customer.

303. A note is included with this section to remind reporting entities that where ongoing customer due diligence is still required, which most relevantly includes the requirement to review, and where appropriate, update and reverify 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.

Section 5-19—Ongoing customer due diligence—transferred pre-commencement customer

304. Section 5-19 of the Rules operates to allow reporting entities to benefit from the relief provided by section 36 of the Act where a reporting entity has customers who are customers of the reporting entity because of:

- One reporting entity (the prior reporting entity) assigning, conveying, selling or transferring the whole of a part of its business to the reporting entity,
- All or part of the assets and liabilities of one reporting entity (the prior reporting entity) being transferred to another reporting entity as a result of a voluntary transfer under the *Financial Sector (Transfer and Restructure) Act 1999*,
- All or part of the assets and liabilities of another reporting entity (the reporting entity) become the assets and liabilities of another reporting entity as a result of a compulsory transfer under statute.

305. In such circumstances, the reporting entity's ongoing CDD obligations are varied by section 5-19 of the Rules to only require monitoring for significant changes in the nature and purpose of the business relation with the customer which results in the ML/TF risk of the customer being high or medium.

Section 5-20—Ongoing customer due diligence—monitoring of transactions and behaviours

306. 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.

307. *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.

308. Section 5-20 of the Rules specifies that a reporting entity is taken to comply with paragraph 30(2)(a) 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) (other than subparagraph 41(1)(f)(iii) of the Act) 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 5-20(b)(i)-(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.

309. The offences listed in subparagraphs 5-20(b)(ii)-(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(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.

310. The effect of section 5-20 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.

311. 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 5—Politically exposed persons

312. AUSTRAC's 2024 money laundering national risk assessment (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.

Section 5-21—Matters for initial customer due diligence—politically exposed person

313. Section 5-21 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.

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

315. 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,

316. Subsection 5-21(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. Section 5-21(3) therefore allows reporting entities to treat such 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.

Section 5-22— Delayed initial due diligence for certain matters (politically exposed persons)—service provided in Australia

317. Section 5-22 allows for a reporting entity to commence to provide a designated service to a customer where it has:
    - established that the customer is a PEP
    - established all other matters set out in section 28(2) of the Act in relation to the customer, and
    - not yet established the customer's source of wealth or source of funds.

318. Given this section is made under section 29 of the Act, the requirements of section 29 must also be met, including the risk mitigation requirements associated with delayed verification of matters for initial CDD.

319. The effect of section 5-22 is that once a customer's status as a PEP has been established on reasonable grounds, the customer's source of wealth and source of funds must be established 'as soon as reasonably practical' under the reporting entity's AML/CTF policies.

Section 5-23—Ongoing customer due diligence—politically exposed person

320. Section 5-23 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.

321. As with subsection 5-21(3) above in relation to initial customer due diligence, subsection 5-23(3) allows reporting entities to apply the requirements for domestic PEPs where they provide designated services to a foreign PEP at or through a permanent establishment in the foreign country for which the customer is a PEP.

Division 6—Nested service relationships

322. 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.

323. 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 6 of the Rules.

324. 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.

325. 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.

326. 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.

327. 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.:

- they provide 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

- they provide 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).

328. 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.

329. 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. Nested services relationship enhanced due diligence does automatically not extend to 'know your customer's customer' (KYCC) requirements for each service provided by the foreign counterpart, but sets our risk mitigation measures related to the relationship itself.

330. Division 6 should be read together with section 4-11 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.

Section 5-24—Matters for initial customer due diligence—nested services relationship

331. Section 5-24 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.

332. 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 and Financial Crime Compliance Questionnaire as part of meeting nested services enhanced due diligence requirements under the Act and Rules.

333. The matters to be established in section 5-24 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.

Section 5-25— Ongoing customer due diligence—nested services relationship

334. Subsections 5-25(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:

- the reporting entity must review and, where necessary, update its identification and assessment of the ML/TF risk of the customer at least once every 2 years, and

- the reporting entity must review and, where necessary, update and reverify KYC information about the customer no less than once every 2 years.

335. Subsection 5-25(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 nested services relationship. In such cases, the reporting entity must review and, if necessary, update and reverify the KYC information about the customer.

336. 5-25(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—Reliance on collection and verification of KYC information

337. Division 7 of Part 5 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.

338. 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).

339. 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.

340. 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) 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 5-13 in relation to initial CDD carried out under the laws of a foreign country.

Section 5-26—Requirements for agreement or arrangement on collection and verification of KYC information

341. Section 5-26 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 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

- Paragraph (e)—that the responsibilities of each party to the CDD arrangement be documented in the arrangement, including in relation to record-keeping.

Section 5-27—Requirements for reliance on collection and verification of KYC information

342. Section 5-27 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 but, 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 5-27 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 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,
- Subsection (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 AML/CTF Rules made under section 29 of the AML/CTF Act related to delayed initial CDD),
- Subsection (d)—the requirement for the relying reporting entity to 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 8—Keep open notices

343. Sections 39A, 39B and 39C of the Act prescribe the requirements for the 'keep open notice' framework. Sections 5-28 to 5-32 of the Rules further prescribe the form and content of the various notices which form part of this framework.

344. 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 Act obligations.

345. 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.

346. Section 39B of the Act allows a 'senior member' (defined in subsection 39B(3) of the Amended AML/CTF Act) of an agency (specified in subsection 39B(4) of the Amended AML/CTF 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).

347. 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.

348. 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).

349. 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.

Section 5-28—Senior member of agency—superintendent

350. 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.

351. Section 5-28 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.

352. Accordingly, section 5-28 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.

Section 5-29 – Form of keep open notice

353. 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.

354. Section 5-29 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 prescribed as the form to be used when issuing keep open notices pursuant to subsection 39B(1) of the Act.

Section 5-30 – Information and documents required to be contained in or to accompany keep open notice

355. Section 5-30 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.

Section 5-3—Extension notices

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

357. 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'.

358. 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.

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

360. Section 5-31 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.

Section 5-32—Further extension application

361. 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.

362. Section 5-32 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.

Part 6—Correspondent Banking

363. Part 6 of the Rules deals with the entry of a financial institution into a correspondent banking relationship and ongoing due diligence assessments. Part 6 replaces Chapter 3 of the former rules and is substantially the same.

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

Section 6-1 – Requirements for due diligence assessment

364. 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.

365. Subsection 6-1(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.

366. Subsection 6-1(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.

Section 6-2 – Matters to which a senior officer must have regard before giving approval

367. Subsection 96(1)(b) of the Act prohibits a financial institution 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.

368. Subsection 6-2(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.

369. 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 6-3(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

Section 6-3 – Requirements for ongoing due diligence assessments

370. 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 6-3 of the Rules requires out that the correspondent must carry out the ongoing due diligence assessments 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 6-1(3).

Section 6-4 – Timing of ongoing due diligence assessments

371. Section 6-4 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.

372. Subsection 6-4(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 7—Transfers of value

373. 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'.

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

375. Part 7 of the Rules:

- prescribes circumstances for determining whether a person is an ordering institution or a beneficiary; 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

376. Division 1 of the Rules comprises:

- Section 7-1 – Determination of who is an ordering institution; and
- Section 7-2 – Determination of who is a beneficiary institution.

377. Section 7-2 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.

Section 7-1 – Determination of who is an *ordering institution*

378. Section 7-1 of the Rules provides for the determination of who is an ordering institution under the enabling power of subsection 63A(1) of the Act for the purposes of a transfer of value.

379. Subsection 7-1(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.

380. Subsection 7-1(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).

381. Paragraphs 7-1(3)(a) – (d) of the Rules set out non-exhaustive circumstances in which a person may be an ordering institution.

382. Subsection 7-1(4) of the Rules clarifies that these circumstances do not affect the fundamental requirement for a person to satisfy subsection 7-1(2) of the Rules to be an ordering institution.

Circumstances in which a person may be an ordering institution under subsection 7-1(2) of the Rules

383. Paragraph 7-1(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.

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

Example 1: A customer provides cash or virtual assets 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).

385. Paragraph 7-1(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).

386. 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.

387. Paragraph 7-1(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.

388. 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).

389. 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 under the preceding circumstance because it accepts the instruction to transfer value from a credit card account.

390. Paragraph 7-1(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.

391. 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.

Section 7-2 – Determination of who is a *beneficiary institution*

392. Section 7-2 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.

393. Subsection 7-2(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.

394. Subsection 7-2(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).

395. Subsection 7-2(3) of the Rules prescribes the circumstances in which a person may be a beneficiary institution under subsection 7-2(2).

396. Subsection 7-2(4) of the Rules prescribes that the circumstances identified in paragraphs 7-2(3)(a)-(d) do not affect the requirement for a person to satisfy subsection 7-2(2) to be a beneficiary institution.

Circumstances in which a person may be a beneficiary institution under subsection 7-2(2) of the Rules

397. Paragraph 7-2(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

398. Non-exhaustive examples of this circumstance include:

Example 1: A remitter, financial institution or VASP provides cash or virtual assets 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).

399. Paragraph 7-2(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.

400. 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.

401. Paragraph 7-2(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.

402. 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).

403. Paragraph 7-2(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.

404. 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

405. The requirements in Part 7 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.

406. The new sections 7-3 – 7-5 of the Rules establish the minimum information that is required to be collected, verified and passed on in a transfer of value.

Section 7-3 – Obligations of ordering institutions – collecting, verifying and passing on information

407. 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.

408. 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.

409. 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.

410. The table in section 7-3 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.

411. The table in section 7-3 of the Rules must also be read together with the definitions of the following terms in section 1-4 of the Rules:

- payer information
- payee information
- tracing information
- card-based pull payment
- BECS
- BPAY
- DEFT.

412. Column 1 of the table in section 7-3 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 circumstance listed in other items of the table apply.

413. 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 payee information for any value transfer service, whether domestic or international, unless the designated service is a card-based pull payment or a refund of a card-based pull payment. In these circumstances the ordering institution (i.e. the card issuer for a card-based pull payment and the merchant acquirer for the refund of a card-based pull payment) is not required to collect payer and payee information.

414. 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 card-based pull 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.

415. 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 both payer and payee 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,
- card-based pull payments and refunds of card-based pull payments—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).

416. 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'.

417. 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.

418. 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 the payer and payee information.

Section 7-4 – Obligations of beneficiary institutions – monitoring for receipt of information

419. 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.

420. 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 7-4 of the Rules must be read together with the definitions referred to in the notes on section 7-3 of the Rules, as well as the designated service in item 30 of table 1 in section 6 of the Act.

421. Column 1 of the table in section 7-4 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 circumstance listed in other items of the table apply.

422. Column 2 of the table in section 7-4 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 both payer and payee information unless specified in one of the circumstances in items 2, 4, 5 or 6 of the Table apply.

423. 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—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,
- card-based pull payments and refunds of card-based pull 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).

424. 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.

425. 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 and payee 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 and payee information, e.g. by requesting this information from its customer, the payee.

Section 7-5 - Obligations of intermediary institutions—monitoring for receipt of information and passing on information

426. 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* 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'.*

427. The table in section 7-5 of the Rules must be read together with the definitions of the following terms in section 1-4 of the Rules:

- payer information
- payee information
- tracing information
- card-based pull payment
- BECS
- BPAY
- DEFT

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

428. 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.

429. 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 both payer and payee information unless one of the circumstances in items 2, 4 or 5 of the Table apply.

430. 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—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,
- card-based pull payments and refunds of card-based pull payments—an intermediary institution is only required to take reasonable steps to monitor for the card number.

431. '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.

432. 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 and payee information off the transfer message and only pass on tracing information. The intermediary institution must still monitor for receipt of the payer and payee information 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).

Division 3—Transfers of value exemptions

433. Division 3 of Part 7 of the Rules contains section 7-6 of the Rules, which has been made for the purpose of paragraph 67(1)(b) of the Act to exempt certain transfers of value that occur in specified circumstances from the requirements in Part 5 of the Act.

Section 7-6 – Transfer of value exemptions

434. Subsection 7-6(1) of the Rules states that section 7-6 of the Rules is made for the purposes of paragraph 67(1)(b) of the Act.

435. 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 7-6 the Rules.

Inter-financial institution transfers

436. Subsection 7-6(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).

437. Subsection 7-6(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 the Society for Worldwide Interbank Financial Telecommunication payment delivery system (Swift) - has led to friction in Australian banks' implementation of the travel rule. Subsection 7-6(3) of the Rules recognises the broader Swift definition for transfers of value through Swift.

Cheques

438. Subsection 7-6(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.

Card-based pull payments

439. Subsection 7-6(5) of the Rules exempts card-based pull payments and refunds of card-based pull 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.

440. 'Card-based pull payment' is defined in section 1-4 (Definitions) of the Rules and is the term is discussed in the notes on that definition.

441. This exemption supports items 4 and 5 in the table in section 7-3 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.

442. This 'card-based pull payment' exemption substantially replaces the exemptions that were in the former subsection 67(4) (ATMs) and subsection 67(4A) (Merchant terminals) of the Act.

Transfers to a self-hosted virtual asset wallet

443. Subsection 7-6(6) 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 7-3 of the Rules.

444. 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.

445. 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 7-3 of the Rules *(Obligations of ordering institutions – collecting, verifying and passing on information);* • Item 2 in the table in section 7-4 of the Rules *(Obligations of beneficiary institutions –*

		monitoring for receipt of information); • Item 2 in the table in section 7-5 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 a third-party bill payment*
Use of debit cards and credit cards, including at a branch of a financial institution	Subsection 67(2) of the AML/CTF Act	More broadly covered by the "card – based pull payment" exemption in subsection 7-6(5) of the Rules
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 7-6(4) of the Rules
Inter-financial institution transfer	Subsection 67(5) of the AML/CTF Act	Subsections 7-6(2) and 7-6(3) (Swift) of the Rules

Division 4—International value transfer services

446. Part 7, Division 4 of the Rules contains the new section 7-7 of the Rules.

Section 7-7 – When is value in a country

447. Section 7-7 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.

448. 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 7-3, 7-4 and 7-5 of the Rules.

449. The circumstances set out in section 7-7 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.

450. Rules related to reports of IVTS will be developed in future.

Part 8—Reporting

451. Part 8 of the Rules provides detail in relation to various reporting obligations a reporting entity has under the Act.

Division 1—Suspicious matter reports

452. 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). A reporting entity must give the AUSTRAC CEO a report about the suspicious matter within the time frames specified by subsection 41(2) of the Act.

453. Paragraph 41(3)(b) of the Act prescribes that a SMR given under subsection 41(2) must contain such information relating to the matter as is specified in the Rules.

454. Part 8, Division 1 of the Rules contain the new sections 8-1, 8-2, 8-3 and 8-4, which have been 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 8-1 to 8-4 of the Rules will replace Chapter 18 of the former rules. Fundamentally, the type of information required to be included in a SMR remains unchanged.

455. 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 other new sections of the Rules and the Act – 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.

456. 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 8-1 to 8-4 of the Rules will be incorporated into the updated 'approved form' referenced in paragraph 41(3)(a) of the Act, which a reporting entity will need to use when giving a SMR to AUSTRAC.

Section 8-1 - Purpose of this Division

457. Section 8-1 of the Rules states the purpose of Part 8, 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 suspicious matter report is in paragraph 41(3)(b) of the Act.

Section 8-2 - Reports of suspicious matters – general information

458. Section 8-2 of the Rules prescribes the general details that a reporting entity must include in a SMR made under subsection 41(2) of the Act. These details include:

- the reporting entity's full name and identifier assigned to it by AUSTRAC (paragraph 8-2(1)(a)
- the date the report is given to the AUSTRAC CEO (paragraph 8-2(1)(b)).
- the date the suspicious matter reporting obligation arose for the reporting entity (paragraph 8-2(1)(c)).

- whether paragraph 41(2)(aa) of the Act applies to the report (dealing with the timeframe for giving a report in certain circumstances relating to legal professional privilege)
- the identifier given by the reporting entity to the report (if any) (paragraph 8-2(1)(e)).
- details about previous reports made to the AUSTRAC CEO which are relevant to the suspicious matter being reported (paragraph 8-2(1)(f)
- the full name, position and contact details of the individual completing the report (subsection 8-2(2)).
- the full name, position and contact details of an individual who can provide information about the reporting entity forming the suspicion (subsection 8-2(3)).
- information about a report made to Commonwealth, State or Territory agencies which relates to the suspicious matter (subsection 8-2(4)).

459. For 'identifying number', a reporting entity should use the identifying number assigned to it when it enrols with AUSTRAC.

460. The reference to 'previous reports made to the AUSTRAC CEO' in paragraph 8-2(1)(e) of the Rules includes any of the following: SMR, TTR, and reports of IVTS. 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, product or instrument that is present in the impending SMR, that previous report should be referenced.

461. For the purposes of providing details for subsection 8-2(3) of the Rules (individual who can provide information about the reporting entity forming the suspicion), this should be taken to mean any individual, other than the individual giving the report to AUSTRAC, who was involved in the formation or substantiation of the suspicion. This information recognises that 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.

Section 8-3 - Reporting of suspicious matters – information about the person in relation to whom the suspicious matter reporting obligation arises for the reporting entity

462. Section 8-3 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.

463. Subsection 8-3(1) of the Rules prescribes the details which must be reported in relation to a person who is an individual.

464. Subsection 8-3(2) of the Rules prescribes details which must be reported in relation to a person who is a non-individual, such a company or incorporated association. The information in both subsections 8-3(1) and 8-3(2) of the Rules is reportable as applicable and to the extent that the information is known to the reporting entity.

465. For the purposes of paragraphs 8-3(1)(b) and 8-3(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);
- 'nicknames' or colloquial names by which the person is commonly known instead of their given name (for example, an abbreviation of the individual's given name, or an anglicised version of their given name).

466. For the purposes of paragraph 8-3(1)(e) of the Rules (the person's gender), gender should be determined according to any identity documents the reporting entity has already collected. If no identity documents are available which present this information, a reporting entity cannot be expected to know, or have knowledge about, this information for reporting purposes.

467. Subsection 8-3(3) of the Rules prescribes reportable details which must be provided in a SMR where the person involved in a suspicious matter is acting as an agent or authorised representative of another person in relation to the provision or proposed provision of the designated service to which the suspicious matter relates.

468. The reportable details requirements for SMRs in section 8-3 of the Rules are summarised in the table below:

TYPE OF PERSON	**Is the person a customer of the reporting entity?**	
	Yes	**No**
Individual	***As applicable and to the extent the information is known:*** • Information listed in subsection 8-3(1)	***As applicable and to the extent the information is known:*** • Information listed in subsection 8-3(1)
Non-individual	***As applicable and to the extent the information is known:*** • Information listed in subsection 8-3(2)	***As applicable and to the extent the information is known:*** • Information listed in subsection 8-3(2)
Authorised person acting on behalf of another person	• Information listed in subsection 8-3(3)	

Section 8-4 - Reports of suspicious matters – information about the matter

469. Section 8-4 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.

470. 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, involved in the provision or proposed provision of a designated service;
- online activity by any person involved in the suspicious matter;

471. Paragraph 8-4(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; or
    - 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

472. 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.

473. '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.

474. Subsection 43(2) of the Act requires that a reporting entity give the AUSTRAC CEO a report about the threshold transaction within 10 days after the transaction takes place (TTR). 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)).

475. Part 8, Division 2 of the Rules contains sections 8-5 to 8-8, 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 8-5 to 8-8 of the Rules will replace Chapter 19 of the former rules. Fundamentally, the type of information required to be included in a TTR remains unchanged.

476. 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 other new sections of the Rules and the Act – 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.

477. 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 8-5 to 8-8 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.

Section 8-5 - Purpose of this Division

478. Section 8-5 of the Rules states the purpose of Part 8, 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.

479. The enabling power to prescribe the reportable details for a TTR is in paragraph 43(3)(b) of the Act.

Section 8-6 - Reports of threshold transactions – general information

480. Section 8-6 of the Rules prescribes the general details that a reporting entity must include in a TTR made under subsection 43(2) of the Act.

481. The 'identifier' for a reporting entity is the identifying number assigned by AUSTRAC when the reporting entity is enrolled on the Reporting Entities Roll. This is the number which should be included in a TTR.

Section 8-7 - Reports of threshold transactions – information about the customer and other person

482. Section 8-7 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.

483. Subsection 8-7(1) of the Rules prescribes the details which must be reported in relation to a customer who is an individual.

484. Subsection 8-7(2) of the Rules prescribes details which must be reported in relation to a person who is a non-individual, such a company or incorporated association. The information in both subsections 8-7(1) and 8-7(2) of the Rules is reportable as applicable and to the extent that the information is known to the reporting entity.

485. For the purposes of paragraphs 8-7(1)(b) and 8-7(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);
- 'nicknames' or colloquial names by which the person is commonly known instead of their given name (for example, an abbreviation of the individual's given name, or an anglicised version of their given name).

486. Subsection 8-7(3) of the Rules prescribes the information that must be contained in a TTR where there is a transferor or transferee involved in the threshold transaction, other than the customer. In particular, a TTR is required to contain the same information (as applicable, and to the extent known) that would be required by subsection 8-7(1) or (2) of the Rules if the transferor or transferee were the customer. 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 the person engaging with the reporting entity, nor 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.

487. In both examples, the reporting entity is expected to provide information required by subsection 8-7(1) or (2) on that third-party who is the transferor (not being the customer of the designated service).

488. Subsection 8-7(4) of the Rules prescribes that the information required to be reported under subsection 8-7(1) or (2) must be contained in a TTR where the customer is receiving the designated service on behalf of another person.

489. For example, a customer who is a trustee transacts 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 8-7(1) or (2) in relation to the family trust estate (not being the customer of the designated service).

490. Subsection 8-7(5) of the Rules prescribes that the reportable information required by subsection 8-7(1) or (2) must be provided in a TTR where the customer was represented by another person authorised to act on behalf of the customer, subject to subsections 8-7(6) and (7).

491. Subsection 8-7(6) of the Rules prescribes that subsection 8-7(5) of the draft Rules does not apply in either of the following circumstances:

(a) 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);

(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).

492. Subsection 8-7(7) of the Rules prescribes that where subsection 8-7(5) does not apply because the designated service occurred in the circumstances mentioned in paragraphs 8-7(6)(a) or (b), the report must include a statement as to the circumstances of the designated service.

493. The reportable details requirements in section 8-7 of the draft Rules are summarised in the table below:

TYPE OF PERSON	**Is the person a customer of the reporting entity?**	
	Yes	**No**
Individual	• Information listed in subsection 8-7(1)	N/A
Non-individual	• Information listed in subsection 8-7(2)	N/A
Transferor or transferee of the physical currency, other than the customer	N/A	• Information listed in subsection 8-7(3) *(the information in subsection 8-7(1) (individual) or 8-7(2) (non-individual) as if the transferor or transferee*

		were a customer of the reporting entity).
Customer receiving designated service involving the threshold transaction on behalf of another person	N/A	• Information listed in subsection 8-7(4) *(the information in subsection 8-7(1) (individual) or 8-7(2) (non-individual) as if the other person were a customer of the reporting entity).*
Authorised person acting on behalf of the customer	• Information listed in subsection 8-7(5) ***unless the exceptions in subsection 8-7(b)apply:*** o *Deposit made in circumstances where there was no person contact (such as using an automated teller machine or express deposit facility);* o *The authorised person was acting in the course of a business of collecting, holding or delivering physical currency (such as payroll or courier services, but not including collection of donations for a registered charity).* • ***If the exceptions in subsection 8-7(5)do not apply:*** a statement as to the circumstances of the designated service.	

Section 8-8 - Reports of threshold transactions – information about the transaction

494. Section 8-8 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.

495. Subsection 8-8(1) of the Rules prescribes the 'standard information' that must be included in a TTR. For the purposes of paragraph 8-8(1)(e) 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.

496. Subsection 8-8(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 8-8(2)).
- products or instruments involved in the threshold transaction (subsection 8-8(3)).
- transfers of property (subsection 8-8(4)).
- virtual assets (subsection 8-8(5)).
- online activity (subsection 8-8(7)).

497. Subsection 8-8(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'

498. Paragraph 8-4(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 8-8(3) of the Rules requires a description of products or instruments - if these have been involved in the transaction being reported in a TTR.

499. A product or instrument should be taken to mean 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.

500. The examples below present some of the products or instruments which can be involved in a designated service and references the source 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'

501. Divisions 1 and 2 of Part 8 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.

502. Divisions 1 and 2 of Part 8 of the Rules require that the 'full name' of a non-individual must be contained in a SMR or TTR. Full name in this context 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 4—compliance reports

503. 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).

504. 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).

505. Both the reporting period and the lodgement period may be a recurring period.

506. 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.

507. 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.

508. Section 8-9 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 each reporting period is the lodgement period for that reporting period (that is, 1 January to 31 March of the following calendar year).

Division 5—Registered remittance affiliates

509. Section 8-10 of the Rules is made for the purposes of section 49A of the Act.

510. Section 49A of the Act allows for the making of Rules in relation to reports required to be lodged by registered remittance affiliates.

511. Subsection 8-10(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.

512. Subsection 8-10(3) of the Rules alters the default legal obligation to give a:
- TTR under subsection 43(2) of the Act; and
- report of an international funds transfer instruction under subsection 45(2) of the Act.

from the registered remittance affiliate to the registered RNP, meaning obligation falls on the RNP to give such reports to the AUSTRAC CEO where there is a remittance affiliate.

Division 6—Cross-border movement reports

Section 8-11 – Purpose of this Division

513. Division 6 of Part 4 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) (including the timing rule) – 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.

Section 8-12 – Reports about moving monetary instruments into or out of Australia

514. Section 8-12 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 8-12(2) (to the extent the information is known) and be given in accordance with the applicable timing rules specified in subsection 8-12(3) of the Rules.

515. The timing rules in subsection 8-12(3) of the Rules for reports made under section 53 of the Act are as follows:
    (a) 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;
    (b) If the person moves the monetary instrument by sending it into Australia, before the movement takes place;
    (c) 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
    (d) 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).

516. Reports for the purposes of section 53 of the Act must be given in the approved form.

Section 8-13 – Reports about receiving monetary instruments moved into Australia

517. Section 8-13 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.

518. Reports for the purposes of section 54 of the Act must be given in the approved form.

Section 8-14 – Affixing of notices about cross-border movement reporting obligations

519. 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.

520. Paragraph 8-14(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.

521. Paragraph 8-12(2)(b) of the Rules prescribes the wording content of the written notices (which may include other additional words).

522. Subsection 8-14(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:

(a) any port, airport, wharf, or boarding station that is appointed under section 15 of the *Customs Act 1901*; or

(b) 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).

Part 9—Secrecy and access

Section 9-1 – Disclosure of AUSTRAC information to foreign countries or agencies

523. Section 9-1 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.

524. 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:

(a) the government of the foreign country, or the foreign agency, has given an undertaking for:
  (i) protecting the confidentiality of the information and controlling the use that will be made of the information; and
  (ii) 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

(b) 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 10—Other matters

Section 10-1—False or misleading information

525. Section 10-1 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.

526. 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.

527. Section 10-1 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 2 – enrolment.
- Part 3 – registration
- Part 5 – customer due diligence

- Part 7 – transfers of value
- Part 8 – reporting

528. The effect of section 10-1 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.

529. 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 AML/CTF 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.

Section 10-2—Conditions for discharge of obligations by members of a reporting group

530. Section 10-2 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 10-2 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.

Section 10-3—Discharge of obligations by members of a reporting group

531. Section 10-3 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.

532. Subsections 10-3(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 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 for the purposes of paragraph 26F(4)(e) of the Act.

533. 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 10-3(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.

Schedule 1—Forms

534. This schedule prescribes, and contains, forms for the purposes of the 'keep open notice' framework.

535. 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.

536. 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**

537. 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.

538. It is noted that section 5-29 of the Rules provides that Form 1 in Schedule 1 is prescribed as the form for a keep open notice, while section 5-30 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

539. 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.

540. It is noted that section 5-31 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

541. 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.

542. Section 5-32 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.