

CHAPTER 4

Part 4.1 Introduction

4.1.1 These Rules are made pursuant to section 229 of the AML/CTF Act for the purposes of paragraphs 36(1)(b), 84(2)(c), 84(3)(b), 85(2)(c) and 85(3)(b), and sections 106, 107 and 108 of the AML/CTF Act. Sections 136 and 137 of the AML/CTF Act apply to each paragraph of this Chapter. They specify the requirements with which Part A or Part B of a reporting entity's standard AML/CTF program or Part A or Part B of a reporting entity's joint AML/CTF program must comply. The primary purpose of Part A of a standard or joint AML/CTF program is to identify, manage and mitigate money laundering or terrorism financing (ML/TF) risk a reporting entity may reasonably face in relation to the provision by the reporting entity of designated services at or through a permanent establishment in Australia. The sole or primary purpose of Part B is to set out the reporting entity's applicable customer identification procedures.

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

4.1.2 This Chapter does not apply to:

- (1) a pre-commencement customer; or
- (2) a customer who receives a designated service covered by item 40, 42 or 44 of table 1 in section 6 of the AML/CTF Act.

Note: Subparagraph 4.1.2(1) relates to pre-commencement customers referred to in sections 28 and 29 of the AML/CTF Act.

4.1.3 For the purposes of these Rules, in identifying its ML/TF risk a reporting entity must consider the risk posed by the following factors:

- (1) its customer types; including:
 - (a) beneficial owners of customers; and
 - (b) any politically exposed persons;
- (2) its customers' sources of funds and wealth;

- (3) the nature and purpose of the business relationship with its customers, including, as appropriate, the collection of information relevant to that consideration;
- (4) the control structure of its non-individual customers;
- (5) the types of designated services it provides;
- (6) the methods by which it delivers designated services; and
- (7) the foreign jurisdictions with which it deals.

Different requirements with respect to different kinds of customers

4.1.4 These Rules specify different requirements for AML/CTF programs in relation to different kinds of customers. An AML/CTF program must comply with such requirements to the extent that a reporting entity has a customer of a particular kind. These Rules make provision in respect of the following kinds of customers:

- (1) Individuals – Part 4.2 of these Rules;
- (2) Companies – Part 4.3 of these Rules;
- (3) Customers who act in the capacity of a trustee of a trust – Part 4.4 of these Rules;
- (4) Customers who act in the capacity of a member of a partnership – Part 4.5 of these Rules;
- (5) Incorporated or unincorporated associations – Part 4.6 of these Rules;
- (6) Registered co-operatives – Part 4.7 of these Rules;
- (7) Government bodies – Part 4.8 of these Rules.

Requirements in respect to Beneficial Owners and Politically Exposed Persons

4.1.5 These Rules specify different requirements for AML/CTF programs in relation to beneficial owners and politically exposed persons:

- (1) Beneficial Owners – Part 4.12 of these Rules;
- (2) Politically Exposed Persons – Part 4.13 of these Rules.

4.1.6 A reporting entity is only required to apply the requirements specified in subparagraphs 4.4.3(5) and 4.4.5(5), and in Part 4.12 and Part 4.13 of these

Rules to a person who becomes a customer after the commencement of those provisions on 1 June 2014.

Verification

- 4.1.7 These Rules also require an AML/CTF program to comply with the requirements of Part 4.9 of these Rules relating to document-based verification and with the requirements of Part 4.10 of these Rules relating to verification from electronic data.

Agents of customers

- 4.1.8 An AML/CTF program must comply with the requirements of Part 4.11 of these Rules in relation to any agent who is authorised to act for or on behalf of a customer in relation to a designated service.

Part 4.2 Applicable customer identification procedure with respect to individuals

- 4.2.1 In so far as a reporting entity has any customer who is an individual, an AML/CTF program must comply with the requirements specified in Part 4.2 of these Rules.
- 4.2.2 An AML/CTF program must include appropriate risk-based systems and controls that are designed to enable the reporting entity to be reasonably satisfied, where a customer is an individual, that the customer is the individual that he or she claims to be.

Collection of information

- 4.2.3 An AML/CTF program must include a procedure for the reporting entity to collect, at a minimum, the following KYC information about an individual (other than an individual who notifies the reporting entity that he or she is a customer of the reporting entity in his or her capacity as a sole trader):
- (1) the customer's full name;
 - (2) the customer's date of birth; and
 - (3) the customer's residential address.
- 4.2.4 An AML/CTF program must include a procedure for the reporting entity to collect at a minimum, the following KYC information about a customer who notifies the reporting entity that he or she is a customer of the reporting entity in his or her capacity as a sole trader:
- (1) the customer's full name;

-
- (2) the customer's date of birth;
 - (3) the full business name (if any) under which the customer carries on his or her business;
 - (4) the full address of the customer's principal place of business (if any) or the customer's residential address; and
 - (5) any ABN issued to the customer.

4.2.5 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine whether, in addition to the KYC information referred to in paragraph 4.2.3 or 4.2.4 above, any other KYC information will be collected about a customer.

Verification of information

4.2.6 An AML/CTF program must include a procedure for the reporting entity to verify, at a minimum, the following KYC information about a customer:

- (1) the customer's full name; and
- (2) either:
 - (a) the customer's date of birth; or
 - (b) the customer's residential address.

4.2.7 An AML/CTF program must require that the verification of information collected about a customer be based on:

- (1) reliable and independent documentation;
- (2) reliable and independent electronic data; or
- (3) a combination of (1) and (2) above.

4.2.8 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine whether, in addition to the KYC information referred to in paragraph 4.2.6 above, any other KYC information collected about the customer should be verified from reliable and independent documentation, reliable and independent electronic data or a combination of the two.

Responding to discrepancies

- 4.2.9 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to respond to any discrepancy that arises in the course of verifying KYC information collected about a customer so that the reporting entity can determine whether it is reasonably satisfied that the customer is the person that he or she claims to be.

Documentation-based safe harbour procedure where ML/TF risk is medium or lower

- 4.2.10 Paragraph 4.2.11 sets out one procedure for documentation-based verification which a reporting entity may include in an AML/CTF program to comply with its obligations under paragraphs 4.2.3 to 4.2.8, and 4.9.1 to 4.9.3 of these Rules where the relationship with the customer is of medium or lower ML/TF risk. Paragraph 4.2.11 does not preclude a reporting entity from meeting the requirements of paragraphs 4.2.3 to 4.2.8, and 4.9.1 to 4.9.3 of these Rules in another way where the relationship with the customer is of medium or lower ML/TF risk.
- 4.2.11 An AML/CTF program that requires the reporting entity to do the following will be taken to meet the requirements of paragraphs 4.2.3 to 4.2.8 and 4.9.2 to 4.9.3 of these Rules in respect of a customer, where a reporting entity determines that the relationship with that customer is of medium or lower risk:
- (1) collect the KYC information described in paragraph 4.2.3 or 4.2.4 (as the case may be);
 - (2) verify the customer's name and either the customer's residential address or date of birth, or both, from:
 - (a) an original or certified copy of a primary photographic identification document; or
 - (b) both:
 - (i) an original or certified copy of a primary non-photographic identification document; and
 - (ii) an original or certified copy of a secondary identification document; and
 - (3) verify that any document produced about the customer has not expired (other than in the case of a passport issued by the Commonwealth that expired within the preceding two years).

Electronic-based safe harbour procedure where ML/TF Risk is medium or lower

4.2.12 Paragraph 4.2.13 sets out one procedure for electronic verification which a reporting entity may follow to comply with its obligations under paragraphs 4.2.3 to 4.2.8, and 4.10.1 of these Rules where the relationship with the customer is of medium or lower ML/TF risk. Paragraph 4.2.13 does not preclude a reporting entity from meeting the requirements of paragraphs 4.2.3 to 4.2.8, and 4.10.1 of these Rules in another way where the relationship with the customer is of medium or lower ML/TF risk.

4.2.13 Part B of an AML/CTF program that requires the reporting entity to do the following will be taken to meet the requirements of paragraphs 4.2.3 to 4.2.8 and 4.10.1 of these Rules in respect of a customer, where a reporting entity determines that the relationship with the customer is of medium or lower risk:

- (1) collect the KYC information described in paragraph 4.2.3 or 4.2.4 (as the case may be) about a customer;
- (2) verify, having regard to the matters set out in subparagraph 4.10.2(1):
 - (a) the customer's name; and
 - (b) either:
 - (i) the customer's residential address; or
 - (ii) the customer's date of birth; or
 - (iii) both (i) and (ii); or
 - (c) that the customer has a transaction history for at least the past 3 years.

4.2.14 For subparagraphs 4.2.13(2)(a) and (b), verification must be undertaken by the reporting entity through the use of reliable and independent electronic data from at least two separate data sources.

Part 4.3 Applicable customer identification procedure with respect to companies

4.3.1 In so far as a reporting entity has any customer who is a domestic or a foreign company, an AML/CTF program must comply with the requirements specified in Part 4.3 of these Rules.

4.3.2 An AML/CTF program must include appropriate risk-based systems and controls that are designed to enable the reporting entity to be reasonably satisfied, where a customer is a company, that:

-
- (1) the company exists; and
 - (2) in respect to beneficial owners, the reporting entity has complied with the requirements specified in Part 4.12 of these Rules.

Existence of the company - collection of minimum information

4.3.3 An AML/CTF program must include a procedure for the reporting entity to collect, at a minimum, the following KYC information about a company:

- (1) in the case of a domestic company:
 - (a) the full name of the company as registered by ASIC;
 - (b) the full address of the company's registered office;
 - (c) the full address of the company's principal place of business, if any;
 - (d) the ACN issued to the company;
 - (e) whether the company is registered by ASIC as a proprietary or public company; and
 - (f) if the company is registered as a proprietary company, the name of each director of the company;
- (2) in the case of a registered foreign company:
 - (a) the full name of the company as registered by ASIC;
 - (b) the full address of the company's registered office in Australia;
 - (c) the full address of the company's principal place of business in Australia (if any) or the full name and address of the company's local agent in Australia, if any;
 - (d) the ARBN issued to the company;
 - (e) the country in which the company was formed, incorporated or registered;
 - (f) whether the company is registered by the relevant foreign registration body and if so whether it is registered as a private or public company or some other type of company; and
 - (g) if the company is registered as a private company by the relevant foreign registration body - the name of each director of the company;

-
- (3) in the case of an unregistered foreign company:
- (a) the full name of the company;
 - (b) the country in which the company was formed, incorporated or registered;
 - (c) whether the company is registered by the relevant foreign registration body and if so:
 - (i) any identification number issued to the company by the relevant foreign registration body upon the company's formation, incorporation or registration;
 - (ii) the full address of the company in its country of formation, incorporation or registration as registered by the relevant foreign registration body; and
 - (iii) whether it is registered as a private or public company or some other type of company by the relevant foreign registration body;
 - (d) if the company is registered as a private company by the relevant foreign registration body - the name of each director of the company; and
 - (e) if the company is not registered by the relevant foreign registration body, the full address of the principal place of business of the company in its country of formation or incorporation.

4.3.4 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine whether, in addition to the KYC information referred to in paragraph 4.3.3, any other KYC information relating to the company's existence will be collected in respect of a company.

Existence of company – verification of information

4.3.5 An AML/CTF program must include a procedure for the reporting entity to verify, at a minimum, the following information about a company:

- (1) in the case of a domestic company:
 - (a) the full name of the company as registered by ASIC;
 - (b) whether the company is registered by ASIC as a proprietary or public company; and
 - (c) the ACN issued to the company;

-
- (2) in the case of a registered foreign company:
 - (a) the full name of the company as registered by ASIC;
 - (b) whether the company is registered by the relevant foreign registration body and if so whether it is registered as a private or public company; and
 - (c) the ARBN issued to the company;
 - (3) in the case of an unregistered foreign company:
 - (a) the full name of the company; and
 - (b) whether the company is registered by the relevant foreign registration body and if so:
 - (i) any identification number issued to the company by the relevant foreign registration body upon the company's formation, incorporation or registration; and
 - (ii) whether the company is registered as a private or public company.

4.3.6 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine whether, in addition to the KYC information referred to in paragraph 4.3.5, any other KYC information referred to in paragraph 4.3.3 or other KYC information relating to the company's existence collected in respect of the company, should be verified.

4.3.7 In determining whether, and what, additional information will be collected and/or verified in respect of a company pursuant to paragraphs 4.3.4 and/or 4.3.6, the reporting entity must have regard to ML/TF risk relevant to the provision of the designated service.

4.3.8 If an AML/CTF program includes the simplified company verification procedure described below with respect to a company that is:

- (1) a domestic listed public company;
- (2) a majority owned subsidiary of a domestic listed public company; or
- (3) licensed and subject to the regulatory oversight of a Commonwealth, State or Territory statutory regulator in relation to its activities as a company;

an AML/CTF program is taken to comply with the requirements of paragraphs 4.3.5, 4.3.6 and 4.3.7 of these Rules in so far as those customers are concerned.

Simplified Company Verification Procedure

The reporting entity must confirm that the company is:

- (1) a domestic listed public company;
- (2) a majority owned subsidiary of a domestic listed public company; or
- (3) licensed and subject to the regulatory oversight of a Commonwealth, State or Territory statutory regulator in relation to its activities as a company;

by obtaining one or a combination of the following:

- (4) a search of the relevant domestic stock exchange;
- (5) a public document issued by the relevant company;
- (6) a search of the relevant ASIC database;
- (7) a search of the licence or other records of the relevant regulator.

- 4.3.9 (1) An AML/CTF program may include appropriate risk-based systems and controls for the reporting entity to determine whether and in what manner to verify the existence of a foreign company by confirming that the foreign company is a foreign listed public company.
- (2) If an AML/CTF program includes systems and controls of that kind, the AML/CTF program must include a requirement that, in determining whether and in what manner to verify the existence of a foreign listed public company in accordance with those systems and controls, the reporting entity must have regard to ML/TF risk relevant to the provision of the designated service, including the location of the foreign stock or equivalent exchange (if any).
- (3) If an AML/CTF program includes systems and controls of that kind, an AML/CTF program is taken to comply with the requirements of paragraphs 4.3.5, 4.3.6 and 4.3.7 of these Rules in so far as those customers are concerned.

Methods of verification

- 4.3.10 Subject to paragraph 4.3.11, an AML/CTF program must require that the verification of information about a company be based as far as possible on:
- (1) reliable and independent documentation;
 - (2) reliable and independent electronic data; or

(3) a combination of (1) and (2) above.

- 4.3.11 For the purposes of subparagraph 4.3.10(1), ‘reliable and independent documentation’ includes a disclosure certificate that verifies information about the beneficial owners of a company if a reporting entity is permitted to obtain a disclosure certificate as described in Chapter 30.
- 4.3.12 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine whether to rely on a disclosure certificate to verify information about a foreign company where such information is not otherwise reasonably available.
- 4.3.13 An AML/CTF program must include a requirement that, in determining whether to rely on a disclosure certificate to verify information in relation to a foreign company in accordance with the requirements of paragraph 4.3.12 above, the reporting entity must have regard to ML/TF risk relevant to the provision of the designated service, including the jurisdiction of incorporation of the foreign company as well as the jurisdiction of the primary operations of the foreign company and the location of the foreign stock or equivalent exchange (if any).

Responding to discrepancies

- 4.3.14 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to respond to any discrepancy that arises in the course of verifying information about a company, so that the reporting entity can determine whether it is reasonably satisfied about the matters referred to in subparagraphs 4.3.2(1) and (2).

Part 4.4 Applicable customer identification procedure with respect to trustees

- 4.4.1 In so far as a reporting entity has any customer who acts in the capacity of a trustee of a trust, an AML/CTF program must comply with the requirements specified in Part 4.4 of these Rules.
- 4.4.2 Subject to paragraph 4.4.18, an AML/CTF program must include appropriate risk-based systems and controls that are designed to enable the reporting entity to be reasonably satisfied, where a person notifies the reporting entity that the person is a customer of the reporting entity in the person’s capacity as the trustee of a trust, that:
- (1) the trust exists; and
 - (2) the name of each trustee and beneficiary, or a description of each class of beneficiary, of the trust has been provided.

Existence of the trust - collection and verification of information

4.4.3 An AML/CTF program must include a procedure for the reporting entity to collect, at a minimum, the following KYC information about a customer:

- (1) the full name (if any) of the trust;
- (2) the full business name (if any) of the trustee in respect of the trust;
- (3) the type of the trust;
- (4) the country in which the trust was established;
- (5) the full name of the settlor of the trust, unless:
 - (a) the material asset contribution to the trust by the settlor at the time the trust is established is less than \$10,000; or
 - (b) the settlor is deceased; or
 - (c) the trust is verified using the simplified trustee verification procedure under paragraph 4.4.8 of these Rules; or
 - (d) the customer is either:
 - (A) a custodian; or
 - (B) a nominee of a custodian.

Note: 'Custodian' and 'nominee of a custodian' are defined in paragraph 4.4.19 of these Rules.

- (6) if any of the trustees is an individual, then in respect of one of those individuals – the information required to be collected about an individual under the applicable customer identification procedure with respect to individuals set out in an AML/CTF program;
- (7) if any of the trustees is a company, then in respect of one of those companies – the information required to be collected about a company under the applicable customer identification procedure with respect to companies set out in an AML/CTF program; and
- (8) if the trustees comprise individuals and companies then in respect of either an individual or a company – the information required to be collected about the individual or company (as the case may be) under the applicable customer identification with respect to the individual or company set out in an AML/CTF program.

-
- 4.4.4 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine whether, in addition to the KYC information referred to in paragraph 4.4.3, any other KYC information relating to the trust's existence will be collected in respect of a trust.
- 4.4.5 An AML/CTF program must include a procedure for the reporting entity to verify, at a minimum:
- (1) the full name (if any) of the trust;
 - (2) if any of the trustees is an individual, then in respect of one of those individuals – information about the individual in accordance with the applicable customer identification procedure with respect to individuals set out in an AML/CTF program;
 - (3) if any of the trustees is a company, then in respect of one of those companies – information about the company in accordance with the applicable customer identification procedure with respect to companies set out in an AML/CTF program;
 - (4) if the trustees comprise individuals and companies then in respect of either an individual or a company – the information about the individual or company (as the case may be) in accordance with the applicable procedures with respect to the individual or company set out in an AML/CTF program; and
 - (5) the full name of the settlor of the trust, unless:
 - (a) the material asset contribution to the trust by the settlor at the time the trust is established is less than \$10,000; or
 - (b) the settlor is deceased; or
 - (c) the trust is verified using the simplified trustee verification procedure under paragraph 4.4.8 of these Rules; or
 - (d) the customer is either:
 - (A) a custodian; or
 - (B) a nominee of a custodian.

Note: 'Custodian' and 'nominee of a custodian' are defined in paragraph 4.4.19 of these Rules..

- 4.4.6 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine whether and to what extent, in addition to the KYC information referred to in paragraph 4.4.5, any other

KYC information relating to the trust's existence collected in respect of the trust should be verified.

- 4.4.7 In determining whether, and what, additional information will be collected and/or verified in respect of a trust pursuant to paragraphs 4.4.4 and/or 4.4.6, the reporting entity must have regard to ML/TF risk relevant to the provision of the designated service.
- 4.4.8 If an AML/CTF program includes the simplified trustee verification procedure described below with respect to a trust that is:
- (1) a managed investment scheme registered by ASIC;
 - (2) a managed investment scheme that is not registered by ASIC and that:
 - (a) only has wholesale clients; and
 - (b) does not make small scale offerings to which section 1012E of the *Corporations Act 2001* applies;
 - (3) registered and subject to the regulatory oversight of a Commonwealth statutory regulator in relation to its activities as a trust; or
 - (4) a government superannuation fund established by legislation;

an AML/CTF program is taken to comply with the requirements of paragraphs 4.4.5, 4.4.6 and 4.4.7 of these Rules in so far as those customers are concerned.

Simplified Trustee Verification Procedure

The reporting entity must verify that the trust is:

- (1) a managed investment scheme registered by ASIC;
- (2) a managed investment scheme that is not registered by ASIC and that:
 - (a) only has wholesale clients; and
 - (b) does not make small scale offerings to which section 1012E of the *Corporations Act 2001* applies;
- (3) registered and subject to the regulatory oversight of a Commonwealth statutory regulator in relation to its activities as a trust; or
- (4) a government superannuation fund established by legislation.

Trustees and beneficiaries— collection and verification of information

- 4.4.9 Subject to paragraph 4.4.18, an AML/CTF program must include a procedure for the reporting entity to collect, at a minimum, the following KYC

information about a customer (other than a trustee in respect of a trust to which paragraph 4.4.13 or 4.4.14 applies):

- (1) the full name and address of each trustee in respect of the trust; and
- (2) either:
 - (a) the full name of each beneficiary in respect of the trust; or
 - (b) if the terms of the trust identify the beneficiaries by reference to membership of a class – details of the class.

4.4.10 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine whether, in addition to the KYC information referred to in paragraph 4.4.9, any other KYC information relating to the trustees, or beneficiaries will be collected in respect of the trust.

4.4.11 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine whether and, if so, in what manner to verify the name of any or each trustee or beneficiary, or details of any or each class of beneficiaries, or any other KYC information collected pursuant to a procedure of the kind described in paragraph 4.4.9, from the sources described in paragraph 4.4.15.

4.4.12 An AML/CTF program must include a requirement that, in determining whether and what KYC information will be collected and/or verified in respect of a trust and the extent to which any KYC information is verified, pursuant to a procedure of the kind described in paragraphs 4.4.10 and/or 4.4.11, the reporting entity must have regard to ML/TF risk relevant to the provision of the designated service.

4.4.13 An AML/CTF program need not include the requirements specified in paragraphs 4.4.9 to 4.4.12 in relation to a trust that is:

- (1) a managed investment scheme registered by ASIC;
- (2) a managed investment scheme that is not registered by ASIC and that:
 - (a) only has wholesale clients; and
 - (b) does not make small scale offerings to which section 1012E of the *Corporations Act 2001* applies; or
- (3) a government superannuation fund established by legislation.

4.4.14 An AML/CTF program need not include the requirements specified in paragraph 4.4.9 in relation to a trust that is registered and subject to the

regulatory oversight of a Commonwealth statutory regulator in relation to its activities as a trust.

Methods of verification

4.4.15 Subject to paragraph 4.4.16, an AML/CTF program must require that the verification of information about a trust be based on:

- (1) a trust deed, certified copy or certified extract of a trust deed;
- (2) reliable and independent documents relating to the trust;
- (3) reliable and independent electronic data; or
- (4) a combination of (1) to (3) above.

4.4.16 For the purposes of subparagraph 4.4.15(2), 'reliable and independent documents relating to the trust' includes a disclosure certificate that verifies information about a trust where:

- (1) the verification is for the purposes of a procedure of the kind described in paragraphs 4.4.6 or 4.4.11 of these Rules; and
- (2) the information to be verified is not otherwise reasonably available from the sources described in paragraph 4.4.15.

Responding to discrepancies

4.4.17 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to respond to any discrepancy that arises in the course of verifying information about a customer so that the reporting entity can determine whether it is reasonably satisfied about the matters referred to in subparagraphs 4.4.2(1) and (2).

Trustees who are either custodians or nominees of a custodian

4.4.18 An AML/CTF program need not include the requirements specified in the following AML/CTF Rules in relation to the provision by the reporting entity of designated services to a customer who is either:

- (A) a custodian or;
- (B) a nominee of a custodian:
 - (1) subparagraph 4.4.2(2); and
 - (2) subparagraph 4.4.9(2); and

-
- (3) in so far as they relate to the collection, verification, updating or review (as applicable) of information on the underlying customers to whom the custodian or nominee of a custodian is providing a custodial or depository service:
- (a) Parts 4.12 and 4.13; and
 - (b) paragraphs 15.2 and 15.3; and
 - (c) subparagraphs 15.9(2), 15.10(1)(b), 15.10(1)(c), 15.10(2) and 15.10(4).

Note 1: The requirements in Parts 4.12 and 4.13 of the AML/CTF Rules continue to apply to reporting entities in relation to the collection and verification of information on the custodian or nominee of a custodian customer.

Note 2: The requirements in paragraphs 15.2 and 15.3 and subparagraphs 15.9(2), 15.10(1)(b), 15.10(1)(c), 15.10(2) and 15.10(4) of the AML/CTF Rules continue to apply to reporting entities in relation to the collection, verification, re-verification, clarification, updating, review and detailed analysis of:

- (a) *KYC information of customers that are either custodians or nominees of custodians; and*
- (b) *beneficial owner information, other than information relating to the underlying customers of either custodians or nominees of custodians.*

Note 1: The requirements in Parts 4.12 and 4.13 of the AML/CTF Rules continue to apply to reporting entities in relation to the collection and verification of information on the custodian customer.

Note 2: The requirements in paragraphs 15.2 and 15.3 and subparagraphs 15.9(2), 15.10(1)(b), 15.10(1)(c), 15.10(2) and 15.10(4) of the AML/CTF Rules continue to apply to reporting entities in relation to the collection, verification, re-verification, clarification, updating, review and detailed analysis of:

- (a) *KYC information of customers that are custodians; and*
- (b) *beneficial owner information, other than information relating to the underlying customers of custodians.*

4.4.19 For the purpose of Part 4.4 of these AML/CTF Rules:

- (1) ‘custodian’ means a company that:

-
- (a) is acting in the capacity of a trustee; and
 - (b) is providing a custodial or depository service of the kind described in item 46 of table 1 in subsection 6(2) of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act); and
 - (c) either:
 - (i) holds an Australian financial services licence authorising it to provide custodial or depository services under the *Corporations Act 2001*; or
 - (ii) is exempt under the *Corporations Act 2001* from the requirement to hold such a licence; and
 - (d) either:
 - (i) satisfies one of the ‘geographical link’ tests in subsection 6(6) of the AML/CTF Act; or
 - (ii) has certified in writing to the relevant reporting entity that its name and enrolment details are entered on the Reporting Entities Roll; and
 - (e) has certified in writing to the relevant reporting entity that it has carried out all applicable customer identification procedures and ongoing customer due diligence requirements in accordance with Chapter 15 of the AML/CTF Rules in relation to its underlying customers prior to, or at the time of, becoming a customer of the reporting entity.
- (2) ‘IDPS’ has the same meaning as in ASIC Class Order [CO 13/763] – *Investor directed portfolio services*, or any legislative instrument that replaces that class order.
 - (3) ‘MDA service’ has the same meaning as in the *ASIC Corporations (Managed Discretionary Account Services) Instrument 2016/968*, or any legislative instrument that replaces that instrument.
 - (4) ‘nominee of a custodian’ means a related body corporate of a custodian provided:
 - (a) the appointing custodian meets the criteria specified in subparagraph 4.4.19(1) of these Rules; and
 - (b) the nominee of the custodian gives the relevant reporting entity certification from the appointing custodian that the former:
-

- (i) satisfies the geographical link or is on the Reporting Entity Roll; and
 - (ii) has carried out all applicable customer identification procedures in relation to their underlying customers.
- (5) 'providing a custodial or depository service' has the same meaning as in section 5 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* and includes providing a custodial or depository service as part of an IDPS or MDA service.
- (6) 'Reporting Entities Roll' has the meaning given by section 51C of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.

Part 4.5 Applicable customer identification procedure with respect to partners

- 4.5.1 In so far as a reporting entity has any customer who acts in the capacity of a partner in a partnership, an AML/CTF program must comply with the requirements specified in Part 4.5 of these Rules.
- 4.5.2 An AML/CTF program must include appropriate risk-based systems and controls that are designed to enable the reporting entity to be reasonably satisfied, where a person notifies the reporting entity that the person is a customer of the reporting entity in the person's capacity as a partner in a partnership, that:
- (1) the partnership exists; and
 - (2) the name of each of the partners in the partnership has been provided in accordance with subparagraph 4.5.3(5).

Collection and verification of information

- 4.5.3 An AML/CTF program must include a procedure for the reporting entity to collect, at a minimum, the following KYC information and documentation about a customer:
- (1) the full name of the partnership;
 - (2) the full business name (if any) of the partnership as registered under any State or Territory business names legislation;
 - (3) the country in which the partnership was established;
 - (4) in respect of one of the partners - the information required to be collected about an individual under the applicable customer

identification procedure with respect to individuals set out in an AML/CTF program; and

- (5) the full name and residential address of each partner in the partnership except where the regulated status of the partnership is confirmed through reference to the current membership directory of the relevant professional association.

4.5.4 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine whether, in addition to the information referred to in paragraph 4.5.3, any other KYC information will be collected in respect of a partnership.

4.5.5 An AML/CTF program must include a procedure for the reporting entity to verify at a minimum:

- (1) the full name of the partnership from the partnership agreement, certified copy or certified extract of the partnership agreement, reliable and independent documents relating to the partnership or reliable and independent electronic data; and
- (2) information about one of the partners in accordance with the applicable customer identification procedure with respect to individuals set out in an AML/CTF program.

4.5.6 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine whether, and to what extent, in addition to the KYC information referred to in paragraph 4.5.5, any other KYC information collected in respect of the partnership should be verified.

Methods of verification

4.5.7 Subject to paragraph 4.5.8, an AML/CTF program must require that the verification of information about a partnership be based on:

- (1) a partnership agreement, certified copy or certified extract of a partnership agreement;
- (2) a certified copy or certified extract of minutes of a partnership meeting;
- (3) reliable and independent documents relating to the partnership;
- (4) reliable and independent electronic data; or
- (5) a combination of (1) to (4) above.

4.5.8 For the purposes of subparagraph 4.5.7(3), ‘reliable and independent documents relating to the partnership’ includes a disclosure certificate that verifies information about a partnership where:

- (1) the verification is for the purposes of a procedure of the kind described in paragraph 4.5.6 of these Rules; and
- (2) the information to be verified is not otherwise reasonably available from the sources described in paragraph 4.5.7.

Responding to discrepancies

4.5.9 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to respond to any discrepancy that arises in the course of verifying information about a customer so that the reporting entity can determine whether it is reasonably satisfied about the matters referred to in subparagraphs 4.5.2(1) and (2).

Part 4.6 Applicable customer identification procedure with respect to associations

4.6.1 In so far as a reporting entity has any customer who is an incorporated or unincorporated association, an AML/CTF program must comply with the requirements specified in Part 4.6 of these Rules.

4.6.2 An AML/CTF program must include appropriate risk-based systems and controls that are designed to enable the reporting entity to be reasonably satisfied, where a customer notifies the reporting entity that it is an incorporated or unincorporated association, that:

- (1) the association exists; and
- (2) the names of any members of the governing committee (howsoever described) of the association have been provided.

Collection and verification of information

4.6.3 An AML/CTF program must include a procedure for the reporting entity to collect, at a minimum, the following KYC information about an incorporated or unincorporated association:

- (1) if the customer notifies the reporting entity that it is an incorporated association:
 - (a) the full name of the association;
 - (b) the full address of the association’s principal place of administration or registered office (if any) or the residential

address of the association's public officer or (if there is no such person) the association's president, secretary or treasurer;

- (c) any unique identifying number issued to the association upon its incorporation by the State, Territory or overseas body responsible for the incorporation of the association; and
 - (d) the full name of the chairman, secretary and treasurer or equivalent officer in each case of the association; and
- (2) if the person notifies the reporting entity that he or she is a customer in his or her capacity as a member of an unincorporated association:
- (a) the full name of the association;
 - (b) the full address of the association's principal place of administration (if any);
 - (c) the full name of the chairman, secretary and treasurer or equivalent officer in each case of the association; and
 - (d) in respect of the member – the information required to be collected about an individual under the applicable customer identification procedure with respect to individuals set out in an AML/CTF program.

4.6.4 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine whether, in addition to the KYC information referred to in paragraph 4.6.3, any other KYC information will be collected in respect of an association.

4.6.5 An AML/CTF program must include a procedure for the reporting entity to at a minimum:

- (1) if the customer is an incorporated association - verify from information provided by ASIC or by the State, Territory or overseas body responsible for the incorporation of the association or from the rules or constitution of the association or from a certified copy or certified extract of the rules or constitution of the association or from reliable and independent documents relating to the association or from reliable and independent electronic data:
 - (a) the full name of the incorporated association; and
 - (b) any unique identifying number issued to the incorporated association upon its incorporation; and

-
- (2) if the customer notifies the reporting entity that he or she is a customer in his or her capacity as a member of an unincorporated association:
 - (a) verify the full name (if any) of the association from the rules or constitution of the association or from a certified copy or certified extract of the rules or constitution of the association or from reliable and independent documents relating to the association or from reliable and independent electronic data; and
 - (b) verify information about the member in accordance with the applicable customer identification procedure with respect to individuals set out in an AML/CTF program.

4.6.6 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine whether and to what extent, in addition to the KYC information referred to in paragraph 4.6.5, any other KYC information collected in respect of the association should be verified.

Methods of verification

- 4.6.7 Subject to paragraph 4.6.8, an AML/CTF program must require that the verification of information about an association be based on:
- (1) the constitution or rules of the association or a certified copy or certified extract of the constitution or rules of the association;
 - (2) the minutes of meeting of the association or a certified copy or certified extract of minutes of meeting of the association;
 - (3) in the case of an incorporated association, information provided by ASIC or by the State, Territory or overseas body responsible for the incorporation of the association;
 - (4) reliable and independent documents relating to the association;
 - (5) reliable and independent electronic data; or
 - (6) a combination of (1)–(5) above.
- 4.6.8 For the purposes of subparagraph 4.6.7(4), ‘reliable and independent documents relating to the association’ includes a disclosure certificate that verifies information about an association where:
- (1) the verification is for the purposes of a procedure of the kind described in paragraph 4.6.6 of these Rules; and
 - (2) the information to be verified is not otherwise reasonably available from the sources described in paragraph 4.6.7.

Responding to discrepancies

- 4.6.9 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to respond to any discrepancy that arises in the course of verifying information about an association so that the reporting entity can determine whether it is reasonably satisfied about the matters referred to in subparagraphs 4.6.2(1) and (2).

Part 4.7 Applicable customer identification procedure with respect to registered co-operatives

- 4.7.1 In so far as a reporting entity has any customer who is a registered co-operative, an AML/CTF program must comply with the requirements specified in Part 4.7 of these Rules.
- 4.7.2 An AML/CTF program must include appropriate risk-based systems and controls that are designed to enable the reporting entity to be reasonably satisfied, where a customer notifies the reporting entity that it is a registered co-operative, that:
- (1) the co-operative exists; and
 - (2) the names of the chairman, secretary or equivalent officer in each case of the co-operative have been provided.

Collection and verification of information

- 4.7.3 An AML/CTF program must include a procedure for the reporting entity to collect, at a minimum, the following KYC information about a registered co-operative:
- (1) the full name of the co-operative;
 - (2) the full address of the co-operative's registered office or principal place of operations (if any) or the residential address of the co-operative's secretary or (if there is no such person) the co-operative's president or treasurer;
 - (3) any unique identifying number issued to the co-operative upon its registration by the State, Territory or overseas body responsible for the registration of the co-operative; and
 - (4) the full name of the chairman, secretary and treasurer or equivalent officer in each case of the co-operative.
- 4.7.4 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine whether, in addition to the

information referred to in paragraph 4.7.3, any other KYC information will be collected in respect of a registered co-operative.

4.7.5 An AML/CTF program must include a procedure for the reporting entity to, at a minimum, verify from information provided by ASIC or by the State, Territory or overseas body responsible for the registration of the co-operative or from any register maintained by the co-operative or a certified copy or certified extract of any register maintained by the co-operative or from reliable and independent documents relating to the co-operative or from reliable and independent electronic data:

- (1) the full name of the co-operative; and
- (2) any unique identifying number issued to the co-operative upon its registration.

4.7.6 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine whether and to what extent, in addition to the KYC information referred to in paragraph 4.7.5, any other KYC information relating to the registered co-operative should be verified.

Methods of verification

4.7.7 Subject to paragraph 4.7.8, an AML/CTF program must require that the verification of information about a registered co-operative be based on:

- (1) any register maintained by the co-operative or a certified copy or certified extract of any register maintained by the co-operative;
- (2) any minutes of meeting of the co-operative or a certified copy or certified extract of any minutes of meeting of the co-operative;
- (3) information provided by the State, Territory or overseas body responsible for the registration of the co-operative;
- (4) reliable and independent documents relating to the co-operative;
- (5) reliable and independent electronic data; or
- (6) a combination of (1)–(5) above.

4.7.8 For the purposes of subparagraph 4.7.7(4), ‘reliable and independent documents relating to the co-operative’ includes a disclosure certificate that verifies information about a registered co-operative where:

- (1) the verification is for the purposes of a procedure of the kind described in paragraph 4.7.7 of these Rules; and

- (2) the information to be verified is not otherwise reasonably available from the sources described in paragraph 4.7.7.

Responding to discrepancies

- 4.7.9 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to respond to any discrepancy that arises in the course of verifying information about a registered co-operative so that the reporting entity can determine whether it is reasonably satisfied about the matters referred to in subparagraphs 4.7.2(1) and (2).

Part 4.8 Applicable customer identification procedure with respect to government bodies

- 4.8.1 In so far as a reporting entity has any customer who is a government body an AML/CTF program must comply with the requirements specified in Part 4.8 and (in so far as they are applicable) Parts 4.9 and 4.10.
- 4.8.2 An AML/CTF program must include appropriate risk-based systems and controls that are designed to enable the reporting entity to be reasonably satisfied, where a customer notifies the reporting entity that it is a government body, that:
- (1) the government body exists; and
 - (2) in the case of certain kinds of government bodies – information about the beneficial owners of the government body has been provided, where sought by the reporting entity.

Collection and verification of information

- 4.8.3 An AML/CTF program must include a procedure for the reporting entity to collect, at a minimum, the following KYC information about a government body:
- (1) the full name of the government body;
 - (2) the full address of the government body's principal place of operations;
 - (3) whether the government body is an entity or emanation, or is established under legislation, of the Commonwealth; and
 - (4) whether the government body is an entity or emanation, or is established under legislation, of a State, Territory, or a foreign country and the name of that State, Territory or country.
- 4.8.4 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine whether, in addition to the KYC

information referred to in paragraph 4.8.3 above, any other KYC information will be collected in respect of a government body.

- 4.8.5 An AML/CTF program must include a procedure for the reporting entity to verify the information collected under paragraph 4.8.3 from reliable and independent documentation, reliable and independent electronic data or a combination of both.
- 4.8.6 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine whether, in addition to carrying out the procedure described in paragraph 4.8.5, any KYC information collected under paragraph 4.8.4 should be verified.

Beneficial ownership in respect of foreign government entities

- 4.8.7 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine whether to collect any KYC information about the ownership or control of a government body that is an entity or emanation, or is established under legislation, of a foreign country.
- 4.8.8 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine whether to verify any KYC information collected pursuant to a procedure of the kind described in paragraph 4.8.7 from reliable and independent documentation, reliable and independent electronic data or a combination of both.

Responding to discrepancies

- 4.8.9 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to respond to any discrepancy that arises in the course of verifying information about a government body so that the reporting entity can determine whether it is reasonably satisfied about the matters referred to in subparagraphs 4.8.2(1) and (2).

Part 4.9 Verification from documentation

Verification with respect to individuals

- 4.9.1 In so far as an AML/CTF program provides for the verification of KYC information about an individual by means of reliable and independent documentation, an AML/CTF program must comply with the requirements specified in paragraphs 4.9.2 and 4.9.3.
- 4.9.2 An AML/CTF program must require that the reporting entity be satisfied that any document from which the reporting entity verifies KYC information about an individual has not expired (other than in the case of a passport issued by the Commonwealth that expired within the preceding two years).

- 4.9.3 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine:
- (1) what reliable and independent documentation the reporting entity will require for the purpose of verifying the individual's name and date of birth and/or residential address (as the case may be);
 - (2) if any other KYC information about an individual is to be verified – what reliable and independent documentation may be used to verify that information;
 - (3) whether, and in what circumstances, the reporting entity is prepared to rely upon a copy of a reliable and independent document;
 - (4) in what circumstances a reporting entity will take steps to determine whether a document produced about an individual may have been forged, tampered with, cancelled or stolen and, if so, what steps the reporting entity will take to establish whether or not the document has been forged, tampered with, cancelled or stolen;
 - (5) whether the reporting entity will use any authentication service that may be available in respect of a document; and
 - (6) whether, and how, to confirm KYC information about an individual by independently initiating contact with the person that the individual claims to be.

Verification with respect to persons other than individuals

- 4.9.4 In so far as an AML/CTF program provides for the verification of KYC information about a customer who is not an individual by means of reliable and independent documentation, an AML/CTF program must comply with the requirements specified in paragraph 4.9.5.
- 4.9.5 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine:
- (1) what and how many reliable and independent documents the reporting entity will use for the purpose of verification;
 - (2) whether a document is sufficiently contemporaneous for use in verification;
 - (3) whether, and in what circumstances, the reporting entity is prepared to rely upon a copy of a reliable and independent document;
 - (4) in what circumstances the reporting entity will take steps to determine whether a document produced about a customer may have been

cancelled, forged, tampered with or stolen and, if so, what steps the reporting entity will take to establish whether or not the document has been cancelled, forged, tampered with or stolen;

- (5) whether the reporting entity will use any authentication service that may be available in respect of a document; and
- (6) whether, and how, to confirm information about a customer by independently initiating contact with the customer.

Part 4.10 Verification from reliable and independent electronic data

4.10.1 In so far as an AML/CTF program provides for the verification of KYC information collected about a customer by means of reliable and independent electronic data, an AML/CTF program must comply with the requirements specified in paragraph 4.10.2.

4.10.2 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine:

- (1) whether the electronic data is reliable and independent, taking into account the following factors:
 - (a) the accuracy of the data;
 - (b) how secure the data is;
 - (c) how the data is kept up-to-date;
 - (d) how comprehensive the data is (for example, by reference to the range of persons included in the data and the period over which the data has been collected);
 - (e) whether the data has been verified from a reliable and independent source;
 - (f) whether the data is maintained by a government body or pursuant to legislation; and
 - (g) whether the electronic data can be additionally authenticated; and
- (2) what reliable and independent electronic data the reporting entity will use for the purpose of verification;
- (3) the reporting entity's pre-defined tolerance levels for matches and errors; and

- (4) whether, and how, to confirm KYC information collected about a customer by independently initiating contact with the person that the customer claims to be.

Part 4.11 Agents of customers

Agents of customers who are individuals

- 4.11.1 For the purposes of paragraph 89(1)(b) and 89(2)(b) of the AML/CTF Act, paragraphs 4.11.2 to 4.11.4 of these Rules apply in relation to an agent of a customer who is an individual where that agent is authorised to act for or on behalf of the customer in relation to a designated service.
- 4.11.2 An AML/CTF program must include a procedure for the reporting entity to collect, at a minimum, the following information and documentation (if any) about the customer:
 - (1) the full name of each individual who purports to act for or on behalf of the customer with respect to the provision of a designated service by the reporting entity; and
 - (2) evidence (if any) of the customer's authorisation of any individual referred to in subparagraph 4.11.2(1).
- 4.11.3 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine whether, and to what extent, it should verify the identity of any of the individuals referred to in subparagraph 4.11.2(1).
- 4.11.4 An AML/CTF program must require the reporting entity to have regard to the ML/TF risk relevant to the provision of the designated service for the purposes of determining whether, and to what extent, it should verify the identity of any of the individuals referred to in paragraph 4.11.2(1).
- 4.11.5 For the purposes of paragraph 89(1)(b) and 89(2)(b) of the AML/CTF Act, paragraphs 4.11.6 to 4.11.8 of these Rules apply in relation to an agent of a customer who is not acting in his or her capacity as an individual where that agent is authorised to act for or on behalf of the customer in relation to a designated service.
- 4.11.6 An AML/CTF program must include a procedure for the reporting entity to collect, at a minimum, the following information and documentation about the customer:
 - (1) the full name of each individual who purports to act for or on behalf of the customer with respect to the provision of a designated service by the reporting entity; and

- (2) evidence of the customer's authorisation of any individual referred to in subparagraph 4.11.6(1).

4.11.7 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine whether, and to what extent, it should verify the identity of any of the individuals referred to in subparagraph 4.11.6(1).

4.11.8 An AML/CTF program must require the reporting entity to have regard to the ML/TF risk relevant to the provision of the designated service for the purposes of determining whether, and to what extent, it should verify the identity of any of the individuals referred to in subparagraph 4.11.6(1).

Verifying officers and agents of non-natural customers

4.11.9 An AML/CTF program may provide for an agent of a customer who is a non-natural person to be identified by the customer's verifying officer, provided the requirements in paragraphs 4.11.12 to 4.11.13 are met.

4.11.10 In so far as:

- (1) an AML/CTF program provides for an agent of a non-natural customer to be identified by a verifying officer; and
- (2) the requirements in paragraphs 4.11.12 to 4.11.13 of these Rules are met;

an AML/CTF program need not apply the requirements in 4.11.6 to 4.11.8 of these Rules in relation to that agent.

Appointment of a verifying officer

4.11.11 A verifying officer is a person appointed by a customer to act as a verifying officer for the purposes of these Rules. A person may be appointed as a verifying officer if he or she is an employee, agent or contractor of the customer.

Identification by a verifying officer

4.11.12 Where an AML/CTF program provides for an agent to be identified by a verifying officer, an AML/CTF program must include a requirement for:

- (1) the agent to be identified by the customer's verifying officer in accordance with paragraph 4.11.13 of these Rules;
- (2) the verifying officer to be identified and verified by the reporting entity in accordance with the requirements specified in Chapter 4 of these Rules;

- (3) the reporting entity to be provided with evidence of the customer's authorisation of the verifying officer to act as a verifying officer;
- (4) the verifying officer to make and for the customer to retain, a record of all matters collected pursuant to paragraph 4.11.13; and
- (5) the verifying officer to provide the following to the reporting entity:
 - (a) the full name of the agent; and
 - (b) a copy of the signature of the agent.

4.11.13 A verifying officer will be taken to have identified an agent if he or she has collected the following:

- (1) the full name of the agent;
- (2) the title of the position or role held by the agent with the customer;
- (3) a copy of the signature of the agent; and
- (4) evidence of the agent's authorisation to act on behalf of the customer.

Part 4.12 Collection and Verification of Beneficial Owner information

4.12.1 An AML/CTF program must include appropriate systems and controls for the reporting entity to determine the beneficial owner of each customer and carry out the following, either before the provision of a designated service to the customer or as soon as practicable after the designated service has been provided:

- (1) collect, (including from the customer, where applicable) and take reasonable measures to verify:
 - (a) each beneficial owner's full name, and
 - (b) the beneficial owner's date of birth; or
 - (c) the beneficial owner's full residential address.

4.12.2 The requirements of paragraph 4.12.1 may be modified:

- (1) for a customer who is an individual, the reporting entity may assume that the customer and the beneficial owner are one and the same, unless the reporting entity has reasonable grounds to consider otherwise;
- (2) for a customer who is:

- (a) a company which is verified under the simplified company verification procedure under paragraph 4.3.8 of these Rules;
- (b) a trust which is verified under the simplified trustee verification procedure under paragraph 4.4.8 of these Rules;
- (c) an Australian Government Entity; or
- (d) a foreign listed public company, or a majority-owned subsidiary of such a company, subject to disclosure requirements (whether by stock exchange rules or through law or enforceable means) that ensure transparency of beneficial ownership;

then,

- (e) paragraph 4.12.1 need not be applied.

Note: The terms 'foreign company', 'listed public company' and 'foreign listed public company' are defined in Chapter 1 of the AML/CTF Rules.

4.12.3 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to determine whether, in addition to the information referred to in paragraph 4.12.1 above, any other information will be collected and verified about any beneficial owner.

Note: Reporting entities should consider the requirements in the Privacy Act 1988 relating to the collection and handling of information about beneficial owners.

Verification

4.12.4 An AML/CTF program must require that the verification of information collected about each beneficial owner of a customer be based on:

- (1) reliable and independent documentation;
- (2) reliable and independent electronic data; or
- (3) a combination of (1) and (2) above.

Safe harbour procedure where ML/TF risk of the beneficial owner is medium or lower

4.12.5 Paragraph 4.12.7 sets out one procedure for documentation-based verification (subparagraphs 4.12.7(2) and (3)) and electronic verification (subparagraph 4.12.7(4)) which a reporting entity may include in its AML/CTF program to comply with its obligations under paragraph 4.12.1 of these Rules where the customer and the beneficial owner of the customer is of medium or lower ML/TF risk. Paragraph 4.12.7 does not preclude a

reporting entity from meeting the verification requirements of paragraph 4.12.1 of these Rules in another way where the beneficial owners of the customer are of medium or lower ML/TF risk.

- 4.12.6 Paragraph 4.12.7 is not applicable if any beneficial owner is a foreign politically exposed person.
- 4.12.7 An AML/CTF program that requires the reporting entity to do the following will be taken to meet the requirements of paragraph 4.12.1 of these Rules in respect of the beneficial owners of a customer, where a reporting entity determines that the relationship with that customer and the beneficial owner is of medium or lower risk:
- (1) collect the information described in paragraph 4.12.1 in regard to each beneficial owner;

Documentation-based safe harbour procedure

- (2) verify each beneficial owner's full name and either the beneficial owner's full residential address or date of birth, or both, from:
 - (a) an original or certified copy of a primary photographic identification document; or
 - (b) both:
 - (i) an original or certified copy of a primary non-photographic identification document; and
 - (ii) an original or certified copy of a secondary identification document; and
- (3) verify the document produced by the customer in regard to each beneficial owner has not expired (other than in the case of a passport issued by the Commonwealth that expired within the preceding two years);

Electronic-based safe harbour procedure

- (4) verify each beneficial owner's full name and either the beneficial owner's full residential address or date of birth, or both, using reliable and independent electronic data from at least two separate data sources.

Responding to discrepancies

- 4.12.8 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to respond to any discrepancy that arises in the course of verifying information collected about each beneficial owner so that the reporting entity can determine that it is reasonably satisfied that each beneficial owner is the person that the customer claims they are.

Procedure to follow where unable to determine the identity of the beneficial owner

- 4.12.9 If the reporting entity is unable to ascertain a beneficial owner, the reporting entity must identify and take reasonable measures to verify:
- (1) for a company (other than a company which is verified under the simplified company verification procedure under paragraph 4.3.8 of these Rules) or a partnership, any individual who:
 - (a) is entitled (either directly or indirectly) to exercise 25% or more of the voting rights, including a power of veto, or
 - (b) holds the position of senior managing official (or equivalent);
 - (2) for a trust (other than a trust which is verified under the simplified trustee verification procedure under paragraph 4.4.8 of these Rules), any individual who holds the power to appoint or remove the trustees of the trust;
 - (3) for an association or a registered co-operative, any individual who:
 - (a) is entitled (either directly or indirectly) to exercise 25% or more of the voting rights including a power of veto, or
 - (b) would be entitled on dissolution to 25% or more of the property of the association or registered co-operative, or
 - (c) holds the position of senior managing official (or equivalent).

Note: In addition to the verification procedures set out in Part 4.12, a reporting entity may be able to use a disclosure certificate. Details regarding disclosure certificates are set out in Chapter 30 of the AML/CTF Rules.

Part 4.13 Collection and Verification of Politically Exposed Person information

- 4.13.1 An AML/CTF program must include appropriate risk-management systems to determine whether a customer or beneficial owner is a politically exposed person. The determination must occur either before the provision of a designated service to the customer or as soon as practicable after the

designated service has been provided. If it is determined that the customer or beneficial owner is a politically exposed person, the reporting entity must carry out the applicable steps in this Part.

4.13.2 An AML/CTF program must include appropriate risk-management systems for the reporting entity to undertake each of the following steps for domestic politically exposed persons and international organisation politically exposed persons:

- (1) in the case of a beneficial owner, comply with the identification requirements specified in paragraphs 4.2.3 to 4.2.9 of these Rules as if the politically exposed person was the customer; and
- (2) determine whether the person is of high ML/TF risk; and
- (3) if the person is determined to be of high ML/TF risk, then, in addition to the action specified in subparagraph 4.13.2(1), carry out the actions specified in subparagraphs 4.13.3(2), (3) and (4).

4.13.3 An AML/CTF program must include appropriate risk-management systems for the reporting entity to undertake each of the following steps for foreign politically exposed persons and for high ML/TF risk domestic or international organisation politically exposed persons:

- (1) in the case of a beneficial owner, comply with the identification requirements specified in paragraphs 4.2.3 to 4.2.9 of these Rules as if the politically exposed person was the customer; and
- (2) obtain senior management approval before establishing or continuing a business relationship with the individual and before the provision, or continued provision, of a designated service to the customer;
- (3) take reasonable measures to establish the politically exposed person's source of wealth and source of funds; and
- (4) comply with the obligations in Chapter 15 of these Rules.

4.13.4 An AML/CTF program must include appropriate risk-based systems and controls for the reporting entity to respond to any discrepancy that arises in the course of verifying information collected about a politically exposed person, so that the reporting entity can be reasonably satisfied that the politically exposed person is the person that he or she claims to be.

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

Part 4.14 Exemptions relating to the identification of beneficial owners and politically exposed persons

4.14.1 The requirements in Parts 4.12 and 4.13 of these Rules do not apply to a reporting entity which:

- (1) provides a designated service of the type specified in Column 1; and
- (2) is exempt from Division 4 of Part 2 of the AML/CTF Act in accordance with the circumstances and conditions of the AML/CTF Act or AML/CTF Rules specified in Column 2;

of the following table:

Column 1 – Relevant designated service in subsection 6(2), 6(3) or 6(4) of the AML/CTF Act	Column 2 – AML/CTF Act and AML/CTF Rules references relevant to the exemptions
Multiple tables – Financial Services, Bullion and Gambling services	
Any of the designated services in tables 1, 2 or 3	Chapter 28 – Applicable customer identification procedures in certain circumstances – assignment, conveyance, sale or transfer of businesses
Any of the designated services in tables 1, 2, or 3	Chapter 50 – Exemption from applicable customer identification procedure in certain circumstances
Item 50 of table 1 or item 14 of table 3	Paragraph 14.4 in Chapter 14 – Thresholds for certain designated services
Table 1 – Financial Services	

Any of the designated services	Chapter 66 – Applicable customer identification procedures in certain circumstances – compulsory partial or total transfer of business made under the <i>Financial Sector (Business Transfer and Group Restructure) Act 1999</i>
Items 40, 42 or 44	Subsection 39(6)
Items 2 or 3	Chapter 35 – Exemption from applicable customer identification procedures for correspondent banking relationships
Items 6 or 7	Chapter 39 – Exemption from applicable customer identification procedures – premium funding loans for a general insurance policy
Items 6, 7, 8, 31 and 32	Chapter 45 – Debt collection
Item 17	Paragraph 14.2 in Chapter 14 – Thresholds for certain designated services
Items 25 or 26	Paragraph 14.3 in Chapter 14 – Thresholds for certain designated services
Item 33	Chapter 38 – Exemption from applicable customer identification procedures for the sale of shares for charitable purposes
Item 33	Chapter 49 – International Uniform Give-Up Agreements
Items 35 or 46	Chapter 67 – Warrants

Item 43(a)	Part 41.2 in Chapter 41 – Exemption from applicable customer identification procedures – cashing out of low value superannuation funds and for the Departing Australia Superannuation Payment
Items 43 or 45	Part 41.3 in Chapter 41 – Exemption from applicable customer identification procedures – cashing out of low value superannuation funds and for the Departing Australia Superannuation Payment
Table 2 – Bullion	
Items 1 or 2	Chapter 33 – Applicable customer identification procedure for purchases and sales of bullion valued at less than \$5000
Table 3 – Gambling services	
Items 5, 6, 9 and 10	Chapter 52 – Persons who are licensed to operate no more than 15 gaming machines

Part 4.15

Procedure to follow where a customer cannot provide satisfactory evidence of identity

Reporting entities may rely on Part 4.15 in limited and exceptional cases where a person does not possess, and is unable to obtain, the necessary information or evidence of identity. This may include: individuals whose birth was not registered, people who are homeless, those who are experiencing or have experienced family and domestic violence, undocumented arrivals in Australia, people living in remote areas, people who are transgender or intersex, people affected by natural disasters, people with limited access to identity documents (for example because they were raised in institutional or foster care), people with limited participation in society, and young people or those over 18 who have not established a ‘social footprint’ in the community.

Reporting entities may also rely on Part 4.15 where a person possesses, but is unable to produce or provide, the necessary information or evidence of identity due to

measures implemented or recommended by government, or reasonable measures that a person or reporting entity has adopted, to prevent the spread of COVID-19. This may include customers who are in self-isolation, businesses that have temporarily shut down, and reporting entities that have closed offices/branches and restricted customer visits to limit face-to-face interaction with customers.

- 4.15.1 If a reporting entity is unable to establish the identity of a customer using the applicable customer identification requirements specified in Chapter 4 of the AML/CTF Rules because the customer does not possess, and is unable to obtain, the necessary information or evidence of identity, then it may use alternative identity proofing processes, in accordance with its risk-based systems and controls, to do so.

Alternative identity proofing processes during the COVID-19 Pandemic

- 4.15.1A If a reporting entity is unable to establish the identity of a customer using the applicable customer identification requirements specified in Chapter 4 of the AML/CTF Rules because the customer possesses, but is unable to produce or provide, the necessary information or evidence of identity due to COVID-19 Pandemic measures, then it may use alternative identity proofing processes, in accordance with its risk-based systems and controls, to do so.

Note: Alternative identity proofing processes could include, but are not limited to, acceptance of multiple types of secondary identification documents where normally a primary identification document would be required.

- 4.15.2 If a reporting entity is unable to establish the identity of a customer in accordance with paragraph 4.15.1 or 4.15.1A, then it may accept a self-attestation from the customer certifying that the information provided in relation to their identity is true and correct.
- 4.15.3 A reporting entity must apply appropriate levels of ongoing customer due diligence in order to identify, mitigate and manage any ML/TF risk associated with customer identities established using self-attestation.
- 4.15.4 A reporting entity must not rely on a self-attestation if it knows or has reason to believe that it is incorrect or misleading.

Note: Customers and reporting entities seeking to rely on self-attestation to establish identity should be aware that criminal or civil penalties may apply under Part 12 of the AML/CTF Act for providing false or misleading information, producing false or misleading documents, and for providing or receiving a designated service using a false customer name.

Alternative verification processes during the COVID-19 Pandemic

4.15.5 If a reporting entity is required, in accordance with its applicable customer identification procedure, to verify information based on the original, or a certified copy or certified extract, of a document but cannot do so because of COVID-19 Pandemic measures, then it may rely on a copy of the document in accordance with its risk-based systems and controls.

4.15.6 In this Part, ‘COVID-19 Pandemic measures’ means any:

- (1) measures implemented or recommended by an Australian government body;
- (2) reasonable measures adopted by a reporting entity; or
- (3) reasonable measures adopted by a person;

to prevent the spread of COVID-19.

Note: ‘Reasonable measures’ include those adopted in a foreign country where the person, or a permanent establishment of a reporting entity or subsidiary, is located.

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