Australian Government

AUSTRAC

Explanatory note for consultation – draft of Anti-Money Laundering and Counter-Terrorism Financing Rules to implement the reforms under the Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Act 2020

On 10 December 2020, the Parliament passed the *Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Act 2020* (**the Amendment Act**) to implement the next phase of reforms arising from the recommendations of the *Report on the Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and Associated Rules and Regulations.*

The Amendment Act amends the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (**AML/CTF Act**), and contains a range of measures to strengthen Australia's capabilities to address money laundering and terrorism financing risks and generate regulatory efficiencies.

These draft Anti-Money Laundering and Counter-Terrorism Financing Rules (**AML/CTF Rules**) implement the Amendment Act by amending chapters 3, 6, 7 and 10 of the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1).*

CHAPTER 3: CORRESPONDENT BANKING

The amendments to the AML/CTF Act strengthen protections on correspondent banking by prohibiting financial institutions from entering into a correspondent banking relationship with another financial institution that permits its accounts to be used by a shell bank. The amendments require banks to conduct due diligence assessments before entering into, and for the duration of, any correspondent banking relationship. These changes are consistent with international banking practice.

More specifically, the Amendment Act imposes the following obligations on a reporting entity that enters into a correspondent banking relationship.

- A reporting entity that is a financial institution is prohibited from entering into a correspondent banking relationship involving a vostro account unless it has carried out a due diligence assessment in accordance with the Rules. A senior officer of the reporting entity must approve entering into that correspondent banking relationship.

- Within 20 business days after the day of entering into a correspondent banking relationship that involves a vostro account, the reporting entity must prepare a written record of the arrangement. The record must set out the responsibilities of each party to the correspondent banking relationship.

- A reporting entity must carry out ongoing due diligence assessments on the correspondent banking relationship:

    - in accordance with the Rules; and
    - at times specified in the Rules; and
    - prepare a written record of the assessment within 10 business days after the day the assessment is completed.

- The reporting entity must also ensure that the written record of the assessment is reviewed by a senior officer of the reporting entity, within 20 business days after the written record is prepared to assess whether it should remain in the correspondent banking relationship.

Proposed changes to Chapter 3

The draft AML/CTF Rules propose amendments to Chapter 3 to set out factors that must be considered when conducting initial or ongoing due diligence assessment. They include:

- ownership, control and management structures of the other financial institution and any parent company;
- nature, size and complexity including products, services, delivery channels and customer types;
- countries or jurisdictions in which the other financial institution operates including quality of AML/CTF regulation and supervision;
- the adequacy and effectiveness of AML/CTF controls;
- publicly available information on the other financial institution;
- the comprehensiveness of the other financial institution's customer due diligence (CDD) records and the reporting entity's level of access to those records.

The draft AML/CTF Rules also specify that a senior officer of the reporting entity must consider the assessment of these factors in the written record before providing their approval.

With respect to the timing of ongoing due diligence assessments, the draft AML/CTF Rules state that assessments should be undertaken periodically (at least every 2 years). The assessment must consider the degree of risk that the correspondent banking relationship may involve or facilitate money laundering or terrorism financing (**ML/TF**) or other serious crimes, and any material changes to the factors noted above.

CHAPTER 6: CUSTOMER DUE DILIGENCE – DOUBTS ABOUT THE VERACITY OR ADEQUACY OF THE CUSTOMER'S IDENTITY

The amendments to the AML/CTF Act clarify the requirement to complete the applicable customer identification procedure (**ACIP**) before providing a designated service.

Proposed changes to Chapter 6

The draft AML/CTF Rules amend Chapter 6 to specify the requirements for a reporting entity when it has doubts about the veracity or adequacy of previously obtained know your customer information.

The proposed amendments to Chapter 6 require consequential amendments to Chapter 10 to update the references made in that Chapter to Chapter 6.

CHAPTER 7: RELIANCE

The amendments to the AML/CTF Act expand the circumstances in which a reporting entity may rely on an ACIP or other identification procedure undertaken by another person. This includes permitting reporting entities to enter into an agreement or arrangement for reliance on another person.

Reliance agreements or arrangements

Section 37A introduces the following requirements as an additional reliance mechanism.

A reporting entity can use the new reliance measures where:

- it enters into a written agreement or arrangement with another person that provides for the reporting entity to rely on the ACIP or other identification procedures carried out by that other person; and
- it had reasonable grounds to believe that each of the requirements prescribed by the AML/CTF Rules were met at the time the reporting entity entered into the agreement or arrangement.

A reporting entity is taken to have carried out the ACIP when:

- an agreement or arrangement is in place; and
- the reporting entity:
    - has complied with section 37B of the AML/CTF Act (regular assessments of the agreement/arrangement); and
    - is providing, or proposes to provide, a designated service to a customer; and
    - has obtained identity information of the customer from the other person; and
- the requirements in the AML/CTF Rules are met.

However, if the reporting entity, after completing an assessment under section 37B, no longer has reasonable grounds to believe that each of the relevant requirements prescribed by the AML/CTF Rules are being met, the reporting entity can no longer rely on the ACIP or other identification procedure carried out by the other person.

Proposed changes to Chapter 7

The proposed Part 7.1 under the draft AML/CTF Rules prescribes procedures other than ACIP that can be relied on under a reliance agreement or arrangement. These are customer due diligence procedures that have been carried out by another person in accordance with one or more laws of a foreign country, which deal with the identification and verification of customers, beneficial owners and agents.

The proposed Part 7.2 sets out the requirements relating to reliance agreements or arrangements. The written agreement or arrangement must:

- document the responsibilities of each party; and
- allow for the reporting entity to obtain all relevant KYC information; and
- be approved by the board or a senior management official of the reporting entity.

The proposed Part 7.2 requires the reporting entity, when determining if it is appropriate to rely upon another person's ACIP or other identification procedures, to consider:

- the type and level of ML/TF risk that the relying entity may reasonably be expected to face in its provision of designated services; and
- the nature, size, and complexity of the other party's business, including its products, services, delivery channels, and customer types; and
- the level of ML/TF risk in the country or jurisdiction in which the other party operates.

The proposed Part 7.2 also requires that the other party must be subject to, and supervised or monitored for compliance with, AML/CTF obligations relating to customer due diligence and record-keeping and have appropriate measures in place to comply with those obligations.

The proposed Part 7.3 sets out the requirements that must be met by a reporting entity that, on a case-by-case basis, may rely on the ACIP or other identification procedures carried out by another person.

In addition to the same requirements set out in Part 7.2 for determining the appropriateness of relying upon another person's ACIP or other identification procedures, the relying entity must reasonably believe that the data and documents relevant to the verification of KYC information will be:

- immediately accessible to the relying entity under an agreement; or
- made available within 5 days of a written request being made.

The proposed Part 7.3 also sets the requirements relating to reliance within a corporate or designated business group, including where a member of the corporate group may be located offshore.

A reporting entity can rely on the ACIP or other identification procedure where:

- the reporting entity is a member of a corporate or designated business group; and
- the reporting entity is relying on an ACIP or other identification procedure undertaken by another member of the same corporate or designated business group; and
- both entities apply a joint anti-money laundering program or other group-wide measures relating to customer due diligence and record keeping and have implemented group-wide AML/CTF programs consistent with the requirements of the relevant FATF Recommendations; and
- any higher ML/TF risk in the country or jurisdiction in which the second entity operates is adequately mitigated by the group's AML/CTF programs; and
- the implementation of the measures and programs outlined above are supervised or monitored at a group level by a competent authority.

Draft Notes to Chapter 7 explains that when a reporting entity relies on an ACIP or other identification procedures undertaken by another reporting entity, a person in another country, or a person within their corporate or designated business group under Part 7.3, the relying reporting entity retains ultimate responsibility for ensuring that all relevant obligations relating to customer identification, verification, and ongoing due diligence under the AML/CTF Act and AML/CTF Rules are met.

Regular assessments of reliance agreements or arrangements

Section 37B provides that a reporting entity that enters into an agreement or arrangement under new section 37A is required to carry out regular assessments of the agreement or arrangement in accordance with requirements in the AML/CTF Rules. This includes the conduct and timing of the assessments, and associated record-keeping.

Proposed changes to Chapter 7

The draft AML/CTF Rules amend Chapter 7 to specify that the purpose of the regular assessments is to:

- enable the reporting entity to determine the level of ML/TF risk involved in continuing to rely on an ACIP or other identification procedures undertaken by the other person; and
- identify any deficiencies in the effectiveness of the agreement or arrangement.

The draft AML/CTF Rules require these assessments to be carried out at appropriate and regular intervals having regard to:

- the type and level of ML/TF risk faced by the reporting entity; and
- any material change in respect of the matters specified in subparagraph 7.2.2(2)–(5) of the AML/CTF Rules.

However, the assessments must be done, in any event, at least every 2 years. The draft AML/CTF Rules also specify that a reporting entity must ensure that any changes to the agreement or arrangement considered necessary to correct any deficiencies identified as part of the assessment are implemented as soon as practicable.

CHAPTER 10: GAMBLING SERVICES

The proposed amendments to Chapter 6 require consequential amendments to subparagraphs 10.1.7 and 10.2.7. These subparagraphs have been renumbered as subparagraphs 10.1.6 and 10.2.6 in the draft AML/CTF Rules. The consequential amendments update the references to Chapter 6 in Chapter 10, and do not change the requirements set out in those subparagraphs.

AUSTRAC has made some minor drafting changes to improve the readability of Chapter 10. The obligations of reporting entities under this Chapter are in no way affected by these changes.

Human Rights (Parliamentary Scrutiny) Act 2011 requirements

The *Human Rights (Parliamentary Scrutiny) Act 2011* requires that Statements of Compatibility be made by the rule-maker with regard to disallowable legislative instruments, and must contain an assessment of whether the legislative instrument is compatible with the rights and freedoms recognised in the seven core international human rights treaties that Australia has ratified.

The proposed amendments set out the requirements of the expanded circumstances in which reporting entities may rely on identification procedures undertaken by a third party, and strengthen protections around correspondent banking.

Human rights implications

The proposed amendments to Chapter 7 of the AML/CTF Rules engage the right to privacy in Article 17 of the International Covenant on Civil and Political Rights (**ICCPR**) by expanding the circumstances in which reporting entities may rely on identification procedures undertaken by a third party. Article 17 of the ICCPR provides that no one shall be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence. The use of the term 'arbitrary' means that any interference with privacy must be in accordance with the provisions, aims and objectives of the ICCPR and should be reasonable in the particular circumstances. The United Nations Human Rights Committee has interpreted 'reasonableness' to imply that any limitation must be proportionate and necessary in the circumstances. The right to privacy can be limited by necessity in a democratic society in the interests of national security or public order.

The amendments to Chapter 7 of the AML/CTF Rules will expand the circumstances in which reporting entities may rely on identification procedures undertaken by a third party. This will include the exchange of personal information such as transactional information.

The amendments relating to reliance will facilitate more efficient information sharing between reporting entities and other entities to ensure the proper identification of customers. This outcome supports cooperation and collaboration to detect, deter and disrupt money laundering, terrorism financing, and other serious crimes.

The limitation on the right to privacy is proportionate and not arbitrary as there are appropriate safeguards and controls. For instance, because of section 6E of the *Privacy Act 1988* (the Privacy Act), all reporting entities are subject to the Privacy Act and must abide by the Australian Privacy Principles (**APP**). This ensures that when reporting entities are engaging with foreign entities for the purposes of a reliance agreement or arrangement, they are subject to APP 8.1 that provides that the reporting entity must take such steps as are reasonable in the circumstances to ensure that an overseas entity does not breach the APPs (excluding APP 1) before it discloses personal information to that overseas entity.

Conclusion

The proposed amendments to the AML/CTF Rules are compatible with human rights because, to the extent that they may limit human rights, those limitations are reasonable, necessary and proportionate.

CHAPTER 3 Correspondent Banking

Part 3.1—Entry into a correspondent banking relationship

3.1.1 This Part is made for subsection 96(1) of the Act.

Carrying out an initial assessment

3.1.2 The first institution (the ***correspondent***) must assess in a due diligence assessment the money laundering, financing of terrorism or other serious crime risks associated with entry into a correspondent banking relationship with another financial institution (the ***respondent***).

3.1.3 The correspondent must consider the following factors when assessing money laundering, financing of terrorism or other serious crime risks:

(1) the ownership, control and management structures of the respondent and any parent company of the respondent;

(2) the nature, size, and complexity of the respondent's business, including:

(a) its products, services, delivery channels and customer types; and

(b) the types of transactions carried out as part of the correspondent banking relationship;

(3) the country or countries in which:

(a) the respondent operates or resides; and

(b) if the parent company of the respondent has group-wide anti-money laundering and counter-terrorism financing systems and controls, and the respondent operates within the requirements of those controls—the parent company operates or resides;

Note 1: ***Country*** has the meaning given by section 5 of the Act.

Note 2: A foreign country may include a region or regions. These regions may have a different risk profile to each other or the rest of the foreign country.

(4) the existence and quality of any anti-money laundering and counter-terrorism financing regulation and supervision in the country or countries identified under subparagraph (3) and the respondent's compliance practices in relation to those regulations;

(5) the adequacy and effectiveness of the respondent's anti-money laundering and counter-terrorism financing systems and controls;

(6) publicly-available information relating to the reputation of the respondent and any related bodies corporate, including whether the respondent has been the subject of:

(a) an investigation; or

(b) adverse regulatory action; or

(c) criminal or civil proceedings relating to money laundering, financing of terrorism or other serious crimes;

(7) if the correspondent maintains vostro accounts that can be accessed directly by the customers of the respondent (***payable-through accounts***)—the respondent:

(a) conducts customer due diligence and ongoing customer due diligence in relation to those customers; and

(b) is able to provide to the correspondent, on request, the documents, data or other information obtained when conducting customer due diligence and ongoing customer due diligence in relation to those customers.

Requirement for senior officer approval

3.1.4 The senior officer of the correspondent (***senior officer*)** must have regard to:

(1) the money laundering, financing of terrorism or other serious crime risks assessed in the written record of the due diligence assessment; and

(2) the adequacy and effectiveness of the correspondent's anti-money laundering and counter-terrorism financing program to manage those risks;

before approving entry into a correspondent banking relationship.

3.1.5 If the correspondent maintains payable-through accounts, the senior officer must be satisfied that the respondent:

(1) has verified the identify of, and conducts ongoing customer due diligence in relation to, the customers that have access to those accounts; and

(2) is able to provide the correspondent, on request, the documents, data, or other information obtained when conducing customer due diligence and ongoing customer due diligence in relation to the customers that have access to those accounts.

Part 3.2—Ongoing assessments of a correspondent banking relationship

3.2.1 This Part is made for subsection 96(3) of the Act.

Carrying out ongoing assessments

3.2.2 The first institution (the ***correspondent***) must assess in a due diligence assessment the money laundering, financing of terrorism or other serious crime risks of a correspondent banking relationship with another financial institution (the ***respondent***).

3.2.3 The correspondent must consider the factors set out in subparagraphs 3.1.3(1)–(7) when assessing money laundering, financing of terrorism or other serious crime risks.

Timing of ongoing assessments

3.2.4 The correspondent must conduct assessments at times determined appropriate by the correspondent, based on consideration of:

(1) the level of money laundering, financing of terrorism or other serious crime risks of the correspondent banking relationship; and

(2) any material change in respect of those risks;

but in any event, at least every two years.

CHAPTER 6 Verification of identity

Part 6.1—Re-verification of KYC information

6.1.1 This Part is made for subparagraph 35(1)(b) and subsection 35(2) of the Act.

6.1.2 A reporting entity must take the action set out in paragraph 6.1.3 if:

(1) the reporting entity suspects on reasonable grounds that the customer is not the person that customer claims to be; or

(2) the reporting entity has doubts about the veracity or adequacy of documents or information previously obtained for the purpose of identifying or verifying:

(a) the customer; or

(b) the beneficial owner of the customer; or

(c) a person purporting to act on behalf of the customer.

6.1.3 The reporting entity must, as soon as practicable, take reasonable measures to:

(1) obtain and verify additional KYC information; or

(2) update and verify existing KYC information;

so that the reporting entity is reasonably satisfied that the customer is the person that the customer claims to be.

Part 6.2—Verification of identity of pre-commencement customers

6.2.1 This Part is made for subsection 29(2) of the Act.

6.2.2 If a suspicious matter reporting obligation arises for a pre-commencement customer, the reporting entity must take one or more of the following actions as appropriate:

(1) carry out the applicable customer identification procedure unless the reporting entity has previously carried out, or been deemed to have carried out, that procedure or a comparable procedure;

(2) collect additional KYC information about the customer;

(3) verify the KYC information obtained under subparagraph (2) from reliable and independent sources;

so that the reporting entity is reasonably satisfied that the customer is the person that the customer claims to be.

6.2.3 The reporting entity must take the required action or actions within 14 days starting after the day on which the suspicious matter reporting obligation arose.

Note: A reporting entity is not required to take any measures that would contravene the tipping off offence in section 123 of the Act.

Part 6.3—Verification of identity of low-risk service customers

6.3.1 This Part is made for subsection 31(2) of the Act.

6.3.2 If a suspicious matter obligation arises for a low-risk service customer, the reporting entity must take one or more of the following actions as appropriate:

(1) carry out the applicable customer identification procedure unless the reporting entity has previously carried out, or been deemed to have carried out, that procedure or a comparable procedure;

(2) collect additional KYC information about the customer;

(3) verify the KYC information obtained under subparagraph (2) from reliable and independent sources;

so that the reporting entity is reasonably satisfied that the customer is the person that the customer claims to be.

6.3.3 The reporting entity must take the required action or actions within 14 days starting after the day on which the suspicious matter reporting obligation arose.

Note: A reporting entity is not required to take any measures that would contravene the tipping off offence in section 123 of the Act.

CHAPTER 7 Reliance on third parties

Part 7.1—Reliance

7.1.1 This Part is made for paragraphs 37A(1)(a) and 38(b) of the Act.

Other procedures that may be relied on for customer identification

7.1.2 The procedures in paragraph 7.1.3 are prescribed.

7.1.3 Customer due diligence procedures (however described) that comply with one or more laws of a foreign country and require the other person to:

(1) identify the customer and verify the customer's identity using reliable and independent sources, so that the other person is satisfied that it knows who the customer is; and

(2) identify the beneficial owner of the customer and take reasonable measures to verify the identity of the beneficial owner, so that the other person is satisfied that it knows who the beneficial owner is; and

(3) identify a person acting on behalf of the customer and take reasonable steps to verify the person's identity and authority to act on behalf of the customer, so that the other person is satisfied that it knows who the person is and that the person has authority to act on behalf of the customer.

Note 1: ***Country*** has meaning given by section 5 of the Act.

Note 2: A foreign country may include a region or regions. These regions may have a different risk profile to each other or the rest of the foreign country.

Part 7.2—Ongoing reliance under an agreement or arrangement

7.2.1 This Part is made for paragraph 37A(1)(b) and subsection 38B(1) of the Act.

Requirements relating to agreements or arrangements for reliance

7.2.2 The following requirements are prescribed:

(1) the written agreement or arrangement must:

(a) document the responsibilities of the first entity and the other person; and

(b) enable the first entity to obtain all required KYC information relating to the identity of:

(i) the customer; or

(ii) the beneficial owner of the customer; or

(iii) a person acting on behalf of the customer;

from the other person on request without delay; and

(c) be approved by the governing board or a senior managing official of the first entity;

(2) the first entity must determine:

(a) the type and level of money laundering, financing of terrorism or other serious crime risks that the first entity may reasonably be expected to face in its provision of designated services; and

(b) the nature, size, and complexity of the other person's business, including its products, services, delivery channels, and customer types; and

(c) the level of money laundering, financing of terrorism or other serious crime risks in the country or countries in which the other person operates or resides;

(3) the other person must be:

(a) a reporting entity; or

(b) a foreign entity 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 (***equivalent obligations***);

(4) if the other person is a reporting entity, the other person must have measures in place to comply with their obligations under parts 2 and 10 of the Act;

(5) if the other person is a foreign entity, the other person must have measures in place to comply with the equivalent obligations.

Regular assessments of agreements or arrangements for reliance

7.2.3 The first entity must carry out regular assessments of the requirements prescribed in paragraph 7.2.2 to ensure that the other person is continuing to meet those requirements.

7.2.4 The assessments must be carried out by the first entity at regular intervals, having regard to:

(1) the type and level of money laundering, financing of terrorism or other serious crime risks faced by the first entity; and

(2) any material change in respect of a matter prescribed in subparagraphs 7.2.2(2)–(5);

but in any event, at least every two years.

Note: If the assessment conducted under subparagraph 7.2.3 identifies that the requirements are not being met, the first entity cannot rely on procedures carried out by the other person until the first entity believes on reasonable grounds that the requirements of subparagraph 7.2.2 are being met.

Part 7.3—Case-by-case reliance

7.3.1 This Part is made for paragraph 38(e) of the Act.

7.3.2 The first entity may rely on applicable customer identification procedures or other procedures (as prescribed in paragraph 7.2.2) carried out by the other person if the first entity has reasonable grounds to believe that:

(1) the other person satisfies the requirements in subparagraph 7.2.2(3)–(5); and

(2) all relevant documents, data and information obtained by the other person in the course of carrying out applicable customer identification procedures or the other

procedures (as specified in paragraph 7.2.2) relating to the identity of the customer, the beneficial owner of the customer or a person acting on behalf of the customer will be:

(a) immediately available to the first entity under an agreement in place for the management of relevant documents and electronic data relating to identification and verification; or

(b) otherwise made available to the first entity as soon as practicable following receipt by the other person of a written request from the first entity, but in any event within 5 days of the request being received.

7.3.3 A belief formed under paragraph 7.3.2 will only be reasonable if the first entity has considered the following factors:

(1) the type and level of money laundering, financing of terrorism or other serious crime risks that the first entity may reasonably be expected to face in its provision of the designated services to the customer;

(2) the level of money laundering, financing of terrorism or other serious crime risks in the country or countries in which the other person operates or resides;

(3) the nature, size, and complexity of the other person's business, including its products, services, delivery channels, and customer types.

7.3.4 The first entity must make a written record that sets out how the first entity met the requirements in paragraphs 7.3.2 and 7.3.3.

Deemed compliance—reliance within a corporate or designed business group

7.3.5 The first entity is taken to comply with the requirements of paragraphs 7.3.2 and 7.3.3 if the following conditions are met:

(1) the first entity relies on the applicable customer identification procedures or other procedures (as specified in paragraph 7.2.2) carried out by another person who is a member of the same corporate group or designated business group;

(2) the first entity and the other person:

(a) apply a joint anti-money laundering and counter terrorism-financing program (***AML/CTF program***) or other group-wide measures relating to customer due diligence and record keeping; and

(b) have implemented a joint AML/CTF program or other group-wide anti-money laundering and counter terrorism-financing risk-based systems and controls consistent with the requirements of the relevant FATF Recommendations;

(3) any higher money laundering, financing of terrorism or serious crime risks in the country or countries in which the other person operates or resides are adequately identified, mitigated and managed by the AML/CTF program and risk-based systems and controls of the corporate group or designated business group;

(4) the implementation of the risk-based system and controls mentioned in subparagraphs (2) and (3) are supervised or monitored at a group-level by a competent authority.

Note 1: If the first entity relies on applicable customer identification procedures or other procedures (as specified in paragraph 7.2.2) undertaken by another person under Part 7.3, the first entity retains ultimate responsibility for ensuring that all relevant obligations relating to customer identification, verification, and ongoing due diligence under the Act and Rules are met.

Note 2: Reporting entities that collect information about a customer, beneficial owner of a customer, or person acting on behalf of a customer, from a third party will need to consider their obligation under Australian Privacy Principle (APP) 3. An APP entity must only collect personal information which is reasonably necessary for one or more of the entity's functions or activities (APP 3.8).

CHAPTER 10

Part 10.1—Casinos

10.1.1 This Part is made for subsections 39(4), 118(2) and 118(4) of the Act.

10.1.2 This Part applies to designated services provided by a casino other than online gambling services.

Customer identification

10.1.3 Division 4 of Part 2 of the Act, subject to paragraph 10.1.5, does not apply to a designated service that:

(1) is of a kind described in items 1, 2, 4, 6, 7, 8 or 9 of table 3 in subsection 6(4) of the Act; and

(2) involves an amount less than $10,000.

10.1.4 Division 4 of Part 2 of the Act, subject to paragraph 10.1.5, does not apply to a designated service that is of a kind described in items 1, 2, 4, 6 or 9 of table 3 in subsection 6(4) of the Act where the service:

(1) involves an amount of $10,000 or more; and

(2) involves the customer giving or receiving only gaming chips or tokens.

10.1.5 The exemption does not apply if the reporting entity determines that it must obtain and verify any KYC information about a customer in accordance with its enhanced customer due diligence program and customer identification program.

Verification of identity

10.1.6 Chapter 6 is modified as follows:

(1) the specified action in paragraph 6.1.3 must be taken:

(a) within 14 days starting after the day on which the circumstance specified in paragraph 6.1.2 comes into existence; or

(b) before the reporting entity commences to provide another designated service to the customer to which Part 2 of the Act applies;

(2) the specified action in paragraph 6.2.2 must be taken:

(a) within 14 days starting after the day on which the suspicious matter reporting obligation arose; or

(b) before the reporting entity commences to provide another designated service to the customer to which Part 2 of the Act applies;

(3) the specified action in paragraph 6.3.2 must be taken:

(a) within 14 days starting after the day on which the suspicious matter reporting obligation arose; or

(b) before the reporting entity commences to provide another designated service to the customer to which Part 2 of the Act applies;

(4) paragraphs 6.2.3 and 6.3.3 do not apply.

Record-keeping

10.1.7 Sections 106 and 107 of the Act do not apply to a designated service of a kind described in:

(1) items 1, 2, or 6 of table 3 in subsection 6(4) of the Act; or

(2) item 4 of table 3 in subsection 6(4) to the extent that the customer is only given gaming chips or tokens when the service is provided.

Part 10.2—On-course bookmakers and totalisator agency boards

10.2.1 This Part is made for subsections 39(4), 118(2) and 118(4) of the Act.

10.2.2 This Part applies to designated services provided by a reporting entity that is an on-course bookmaker or a totalisator agency board.

Customer identification

10.2.3 Division 4 of Part 2 of the Act, subject to paragraph 10.2.5, does not apply to a designated service of a kind described in items 1 or 2 of table 3 in subsection 6(4) of the Act.

10.2.4 Division 4 of Part 2 of the Act, subject to paragraph 10.2.5, does not apply to a designated service that:

(1) is of a kind described in items 4, 7 or 8 of table 3 in subsection 6(4); and

(2) involves an amount less than $10,000.

10.2.5 The exemption does not apply if the reporting entity determines that it must obtain and verify any KYC information about a customer in accordance with its enhanced customer due diligence program and customer identification program.

Verification of identity

10.2.6 Chapter 6 is modified as follows:

(1) the specified action in paragraph 6.1.3 must be taken:

(c) within 14 days starting after the day on which the circumstance specified in paragraph 6.1.2 comes into existence; or

(d) before the reporting entity commences to provide another designated service to the customer to which Part 2 of the Act applies;

(2) the specified action in paragraph 6.2.2 must be taken:

(c) within 14 days starting after the day on which the suspicious matter reporting obligation arose; or

(d) before the reporting entity commences to provide another designated service to the customer to which Part 2 of the Act applies;

(3) the specified action in paragraph 6.3.2 must be taken:

(c) within 14 days starting after the day on which the suspicious matter reporting obligation arose; or

(d) before the reporting entity commences to provide another designated service to the customer to which Part 2 of the Act applies;

(4) paragraphs 6.2.3 and 6.3.3 do not apply.

Record-keeping

10.2.7 Sections 106 and 107 of the Act do not apply to a designated service of a kind described in:

(1) items 1, 2, or 6 of table 3 in subsection 6(4) of the Act; or

(2) items 7 or 8 of table 3 in subsection 6(4) of the Act where that service involves an amount less than $10,000.

Part 10.3—Gaming machines

10.3.1 This Part is made for subsection 39(4) of the Act.

10.3.2 This Part applies to designated services provided by a reporting entity by way of a gaming machine other than designated services provided at a casino.

Customer identification

10.3.3 Division 4 of Part 2 of the Act, subject to paragraph 10.3.5, does not apply to a designated service of a kind described in items 5 or 6 of table 3 in subsection 6(4) of the Act.

10.3.4 Division 4 of Part 2 of the Act, subject to paragraph 10.3.5, does not apply in respect of a designated service that:

(1) is of a kind described in items 9 or 10 of table 3 in subsection 6(4); and

(2) involves an amount less than $10,000.

10.3.5 The exemption does not apply if the reporting entity determines that it must obtain and verify any KYC information about a customer in accordance with its enhanced customer due diligence program and customer identification program.

Part 10.4—Accounts for online gambling services

10.4.1 This Part is made for paragraphs 33(a) and (b) and subparagraph 34(1)(d)(i) of the Act.

Special circumstances that justify carrying out the applicable identification procedure after commencement of the provision of a designated service

10.4.2 Online gambling services, subject to the conditions specified in paragraph 10.4.3, are specified for the purposes of paragraph 33(a) of the Act.

10.4.3 The special circumstances are only available to the reporting entity if:

(1) the customer is required to open an account in order to obtain the service; and

(2) the reporting entity does not permit the customer to withdraw any funds from the account prior to carrying out the applicable customer identification procedure.

The period ascertained in accordance with subparagraph 34(1)(d)(i) of the Act

10.4.4 The period is 14 days starting on the day that the reporting entity opens the account in the name of the customer.