TOBIQUE GAMING COMMISSION

REGULATIONS CONCERNING ANTI-MONEY LAUNDERING AND COUNTER TERRORISM FINANCING

Version 2.0

These Regulations were enacted by the Tobique Gaming Commission on April 5, 2024 pursuant to Section 22 of the *TOBIQUE GAMING ACT 2023*.

Contents

PART 1: APPLICATION AND PURPOSE

1. Purpose

The purpose of these Anti- Money Laundering ("**AML**") Regulations is to implement and apply the Recommendations of the Financial Action Task Force ("**FATF**") entitled "International Standards on Combatting Money Laundering and the Financing of Terrorism and Proliferation" in so far as they apply to interactive gaming conducted in and from the Territory.

2. Application

(1) These AML Regulations apply to all forms of gambling based in and offered from within the Territory, including interactive gaming involving players situated both within and outside the Territory.

(2) On the enactment of these AML Regulations:

(a) Each holder of a permit, license or authorization issued under the Tobique Gaming Act in relation to the provision of gambling services to end user customers under direct agreements with them (part of the class known as B2C Operators), including authorized Direct Licensees, is deemed to be a "reporting entity" for the purpose of these AML Regulations.

(b) Compliance with these AML Regulations is deemed to be a condition of the relevant permit, license, or authorization.

(c) These AML Regulations will be further elaborated on and implemented in accordance with AML/Counter Terrorist Financing ("**CTF**") Codes of Practice which should be read in conjunction with these AML Regulations. In any event in case of any conflict or overlapping provisions between these AML Regulations and the AML/CTF Codes of Practice, the former shall be overriding and binding.

(d) For the purposes of clarity, holders of a permit, license or authorization issued under the Tobique Gaming Act in relation to services provided to any B2C Operators (B2B Suppliers) will be subject to a varying degree of AML/CTF compliance depending on their service offering as set out in the AML/CTF Codes of Practice.

(3) The Commission may, in the administration of these AML Regulations, exercise such investigative and disciplinary powers as it enjoys under the Gaming Act and Regulations.

3. Effect

These AML Regulations may serve as a basis for co-operation and mutual assistance between the Commission and other regulatory and law enforcement agencies within or outside or the Territory. However, these AML Regulations are not dependent on the ratification or approval of any other jurisdiction or agency.

4. Definitions

(1) For the purposes of these AML Regulations:

"AML Regulations" means these regulations Concerning Anti-Money Laundering and Counter Terrorism Financing.

"Commission" means the Tobique Gaming Commission.

"Financing of terrorism" includes an activity where:

(a) A person provides or collects funds, and intends or is negligent or reckless as to whether the funds will be used to facilitate or engage in a terrorist act; or

(b) A person to become involved in an arrangement which makes money or other property available to another if he or she knows, or has reasonable cause to suspect, it may be used for terrorist purposes.

"Financing of terrorism offence" is an offence whether committed in the Territory or under the laws of another jurisdiction, which criminalizes the financing of terrorism, and includes circumstances where financing was provided even if the terrorist act does not occur.

"Gaming Act" means the Tobique Gaming Act 2023.

"Money Laundering" is the activity whereby:

(a) A person uses, transfers the possession of, sends or delivers to any person or place, or otherwise deals with, in any manner and by any means, any property or any proceeds of any property with intent to conceal or convert that property or those proceeds, knowing or believing that, or being reckless as to whether, all or a part of that property or of those proceeds was obtained or derived directly or indirectly as a result of criminal activity; or,

(b) A person enters into, or becomes concerned in, an arrangement which he or she knows, or has reasonable cause to suspect, facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person.

"Money laundering offence" is an offence whether committed in the Territory or under the laws of another jurisdiction, which criminalizes money laundering or disposal of the proceeds of crime.

"Person" includes an individual, corporation, partnership, limited liability company and any other business entity recognized under the laws applicable within the Territory.

"Transaction" includes a single transaction or a series of transactions which appear to be linked.

5. Functions and Powers of Commission

In addition to such functions, roles and powers set out in the Gaming Act and these AML Regulations, the Commission shall:

(1) Coordinate actions relating to the assessment of money-laundering and financing of terrorism risks in and from the Territory, and to apply resources, aimed at ensuring the risks are mitigated effectively; and,
(2) Based on that assessment, apply a risk-based approach to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified within its area of control.

6. Inter-Agency Cooperation

(1) The Commission may cooperate with and, when appropriate, provide information concerning actual or potential money-laundering activities of which it becomes aware, to domestic law enforcement agencies and/or such other domestic or international agency or agencies that are appropriate.
(2) The Commission may enter into memoranda of understanding with regulatory authorities from other jurisdictions for the purpose of assisting the Commission in the regulation and supervision of the Territory's anti-money laundering and counter- terrorism financing functions and any related matter.
(3) No memorandum of understanding may call for assistance beyond that which is provided for by these AML Regulations or relieve the Commission of any of its functions or duties under these AML Regulations.
(4) Subject to mutual and appropriate obligations of confidentiality, the Commission may provide such information to other regulatory authorities as may be agreed between the Commission and those agencies.

7. Obligation of Confidentiality

(1) All information received from or about reporting entities under these AML Regulations is to be treated as confidential.
(2) No person working for the Commission or acting on its behalf (or who has worked or acted for the Commission) may, except in accordance with these AML Regulations, disclose any information received in the course of their duties under these AML Regulations to any person outside of the Commission.
(3) Information referred to in paragraph (1) may be disclosed in summary or aggregate form, provided that no reporting entity is identifiable from the information disclosed.
(4) The Commission may only disclose information received pursuant to these AML Regulations:
    (a) In the discharge of its disciplinary duties under these AML Regulations or under other legislation relating to:
        (i) Money laundering or financing of terrorism; or,
        (ii) Gaming regulation.
    (b) In a judicial review of a decision of the Commission; or
    (c) In court proceedings initiated by the Commission in the exercise of the duties referred to in sub-paragraph (a), or otherwise relating to the Commission's discharge of those duties.
(5) This Regulation does not prevent the exchange of information between the Commission

and law enforcement or regulatory agencies within the Territory or from other jurisdictions provided that, except for its disclosure in legal proceedings, the agency to which the information is provided agrees to hold it subject to an appropriate obligation of confidentiality.

PART 2: ASSESSMENT OF MONEY LAUNDERING AND FINANCING OF TERRORISM RISKS BY REPORTING ENTITIES

8. Preparation of the AML/CTF Program

(1) A reporting entity shall prepare an Anti-Money Laundering and Counter Terrorism Financing Program ("AML/CTF Program") consisting of:

(a) Its risk assessment; and,
(b) Its policies, controls and procedures designed to control and mitigate the identified risks.

9. Risk Assessment by Reporting Entity

(1) A reporting entity must undertake a risk assessment to identify and assess the risks of money laundering and financing of terrorism to which its business may be subject.
(2) In conducting the risk assessment, the reporting entity must take into account all relevant money laundering and financing of terrorism risk factors including factors relating to:

(a) Its customers;
(b) The countries or geographic areas in which it operates;
(c) Its products or services;
(d) Its payments and transactions;
(e) Its operational set up and delivery channels; and,
(f) Any third parties that provide services to the business.

(3) In deciding what steps are appropriate under paragraph (1), the reporting entity must take into account the size and nature of its business.
(4) A reporting entity must regularly review its risk assessment.
(5) A reporting entity must keep an up-to-date record in writing of all the steps it has taken under paragraphs (1) to (4).
(6) A reporting entity must provide:

(a) The risk assessment it has prepared under paragraph (1);
(b) Any reviews conducted under paragraph (4);
(c) The information on which that risk assessment or any changes was based; or
(d) Any record required to be kept under paragraph (5), to the Commission on request.

(7) The Commission may issue a direction as to the form or content of any risk assessment, or

any aspect of an assessment.

10. Policies, Controls and Procedures

(1) A reporting entity must:

(a) Establish and maintain policies, controls, and procedures as part of its obligation to mitigate and effectively manage the risks of money laundering and financing of terrorism identified in any risk assessment undertaken by the reporting entity;
(b) Regularly review:

(i) Its risk assessment; and,
(ii) Its policies, controls, and procedures.

(c) Maintain a record in writing of the policies, controls and procedures, any changes to those policies, controls and procedures made as a result of any review, and the steps taken to communicate those policies, controls and procedures, or any changes to them, within the reporting entity's business.

(2) The policies, controls and procedures adopted by a reporting entity under paragraph (1) must be:

(a) Proportionate to the size and nature of the reporting entity's business;
(b) Approved by its board or governing body; and,
(c) Subject to the ongoing oversight of the board and senior management.

(3) The policies, controls and procedures referred to in paragraph (1) must include:

(a) Risk management practices;
(b) Internal controls;
(c) Customer due diligence;
(d) Record keeping; and,
(e) The monitoring and management of compliance with, and the internal communication of, such policies, controls, and procedures.

(4) The policies, controls and procedures referred to in paragraph (1) must include policies, controls, and procedures:

(a) Which provide for the identification and scrutiny of any case where:

(i) A transaction is:
a. Complex;
b. Unusual including unusually large or there is an unusual pattern of transactions;
c. Where the transaction or transactions have no apparent economic or legal purpose; and,

(ii) Any other activity or situation which the reporting entity regards as particularly likely by its nature to be related to money laundering or financing of terrorism.

(b) Which specify the taking of additional measures, where appropriate, to prevent the use of the entity's products or services for money laundering or financing of terrorism.

(c) Which ensure that when new products, new business practices (including new delivery mechanisms) or new technology are adopted by the reporting entity, appropriate measures are taken in preparation for, and during, the adoption of such products, practices or technology to assess and if necessary mitigate any money laundering or financing of terrorism risks this new product, practice or technology may cause.

(d) Under which anyone in the reporting entity's organization who knows or suspects (or has reasonable grounds for knowing or suspecting) that a person is engaged in money laundering or financing of terrorism as a result of information received in the course of the business or otherwise through the carrying on of that business is required to comply with internal reporting obligations.

11. Reliance on Agents or Third Parties

(1) Where a reporting entity relies on agents or third parties to perform elements of the customer due diligence, the ultimate responsibility for compliance with customer due diligence requirements remains with the reporting entity.

(2) Where a reporting entity uses agents or third parties, it must:

(a) Ensure that appropriate measures are taken to assess whether an agent or third party is suitable to undertake the task and has in place adequate controls to ensure compliance with any relevant money laundering or financing of terrorism legislation including these AML Regulations;

(b) Take adequate steps to satisfy itself that copies or records of identification data and other relevant documentation will be made available upon request without delay; and,

(c) The obligations and responsibilities of the reporting entity and the third party are clearly defined.

12. Subsidiaries and Groups

(1) When a reporting entity relies on a third party that is a related company or part of the same group of companies, and that company or group applies a program combatting the risks of money laundering and financing of terrorism, and is supervised by the competent authority of another jurisdiction to a standard equivalent to these AML Regulations, the Commission may consider the reporting entity is adequately controlled by the group AML/CFT program.

(2) If the group program does not impose requirements to counter money laundering and financing of terrorism equivalent to these AML Regulations, the subsidiary must apply measures equivalent to those required by these AML Regulations, as far as permitted under the law of the third country.

(3) Where the law of a third country does not permit the application of such equivalent measures by the subsidiary undertaking or branch established in that country, the relevant parent undertaking must:

(a) Inform the Commission; and,
(b) Take additional measures to effectively mitigate the risk of money laundering or financing of terrorism.

13. Compliance Governance

(1) A reporting entity must appoint a member of senior management to have oversight and overall responsibility for AML/ CTF mitigation. This includes the appointment of a suitably senior and qualified manger to monitor and manage compliance with, and the internal communication of, the policies, controls and procedures adopted by the reporting entity, and in particular to:

(a) Identify any situations at higher risk of money laundering or financing of terrorism;
(b) Maintain a record of its risk assessment, changes to any assessment and its risk management policies, controls and procedures, and relevant changes;
(c) Maintain a record of its compliance with its policies, controls, and procedures, including its compliance with reporting obligations to the Commission; and,
(d) Provide information to senior management about the operation and effectiveness of its policies, controls, and procedures whenever appropriate.

(2) The manager may have other duties.

14. Training

(1) A reporting entity must take appropriate measures to:

(a) Ensure that its employees are made aware of the law relating to money laundering and financing of terrorism, and to the requirements of these AML Regulations; and,
(b) Regularly given training in how to recognize and deal with transactions and other activities or situations which may be related to money laundering or financing of terrorism, as appropriate to their roles.

(2) A reporting entity must maintain a record in writing of the training given to its employees.

15. Employee Due Diligence

(1) A reporting entity must put in place appropriate risk-based systems and controls to determine whether to, and in what manner to, screen any prospective employee who, if employed, may be in a position to facilitate the commission of any money laundering or financing of terrorism offence.

(2) The systems should also describe whether to, and in what manner to, re-screen an employee where the employee is transferred or promoted and may be in a position to facilitate the commission of any money laundering or financing of terrorism offence.

(3) The reporting entity must establish and maintain a system for the reporting entity to manage any employee who fails, without reasonable excuse, to comply with any system, control, or procedure.

16. Independent Review

(1) In addition to any audit the Commission may require, the reporting entity's AML/CTF program must be subject to regular, independent and, where appropriate, external review.

(2) The frequency of the review should consider the nature, size and complexity of a reporting entity's business, and the type and level of money laundering or financing of terrorism risk it might face, but in any case, shall be undertaken at least once every two years.

(3) The purpose of the review is to:

(a) Assess the effectiveness of the program having regard to the money laundering or financing of terrorism risk of the reporting entity;
(b) Assess whether the program has been effectively implemented; and,
(c) Assess whether the reporting entity has complied with its program.

(4) The results of the review, including any report prepared, must be provided to senior management and, where applicable, the governing body of the reporting entity.

(5) The results of the review, including any report prepared, must be provided to the Commission.

17. Directions by the Commission

(1) The Commission may issue a direction to a reporting entity to adopt additional measures to handle its risks of money laundering and terrorist financing more effectively.

(2) Without limiting the scope of its power of direction, the Commission may, in the public interest, direct a reporting entity:

(a) Not to enter into a business relationship with a specified person or class of persons;
(b) Not to undertake transactions of a specified description with a specified person or class of persons;
(c) To terminate an existing business relationship with a specified person or class of persons; or,

(d) To cease any operations in a particular jurisdiction.

PART 3: CUSTOMER DUE DILIGENCE AND RECORD-KEEPING

18. When to Apply Customer Due Diligence

(1) A reporting entity must:

(a) Undertake Customer Due Diligence ("CDD") identification measures when a customer opens an account, which, for the purposes of this Regulation, is when a customer registers with a reporting entity and accepts the Terms and Conditions ("T&Cs") of the site; and,
(b) Must complete the verification of identity and undertake such other CDD measures as are appropriate, as soon as reasonably practicable following the deposit of funds into the account.

19. Customer Due Diligence Measures

(1) The CDD measures to be taken are as follows:

(a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data, or information;
(b) Where the customer is a corporation, partnership, limited liability company, trust or other business entity, the reporting entity must take reasonable measures to verify the identity of the individual or individuals who are the beneficial owners of the customer, such that the reporting entity is satisfied that it knows who the beneficial owner is. This may require reporting entities to understand the ownership and control structure of the customer;
(c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; and,
(d) Conducting ongoing due diligence and monitoring transactions undertaken throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the reporting entity's knowledge of the customer, including, where necessary, the customer's source of funds.

(2) A reporting entity shall determine the application of such CDD measures according to its assessment of the risk of money laundering or financing of terrorism that the customer poses, having regard to such factors as the size of the transactions or location of the customer, and in accordance with the reporting entity's AML/CTF program.

(3) Where the reporting entity is unable to satisfy itself that it has verified the identity of the customer, it:

(a) Should terminate the business relationship; and,
(b) Must make a suspicious matter report in relation to the customer.

(4) A reporting entity shall conduct customer due diligence for existing customers on the basis of materiality and risk and shall conduct due diligence on such existing relationships at appropriate times.

20. Enhanced Due Diligence

(1) A reporting entity's AML/CTF program must describe the systems and controls to be used to determine in what circumstances enhanced customer due diligence should be applied, including when further information should be collected or verified in respect of customers.

(2) A reporting entity must apply enhanced customer due diligence measures where there is:

(a) A change in the risk assessment for that customer;
(b) Where there is any indication that the identity of the customer is not correct or has changed;
(c) Where there are any transactions which are not reasonably consistent with the reporting entity's knowledge of the customer;
(d) There is a suspicion of money laundering or terrorist financing; or,
(e) The reporting entity has doubts about the veracity or adequacy of previously obtained customer identification data.

(3) The Enhanced Due Diligence ("EDD") measures shall include:

(a) Obtaining additional information to verify the customer's identity;
(b) Obtaining additional information as to the customer's source of funds;
(c) Obtaining the approval of senior management for establishing or continuing the business relationship; and,
(d) Conducting enhanced monitoring of the business relationship.

21. Politically Exposed Persons

(1) In addition to performing normal CDD measures, reporting entities must have appropriate risk-management systems to determine whether the customer or the beneficial owner is a Politically Exposed Person, ("PEP") or an immediate family member or close associate of the PEP.

(2) In this Section:

A *"Politically Exposed Person"* means an individual who holds a prominent public position or function in a government body or an international organization, including:

(a) Head of State or head of a country or government;
(b) Government minister or equivalent senior politician;
(c) Senior government official;
(d) Senior judge in a foreign country or international organization;

(e) Governor of a central bank;
(f) Senior foreign representative, ambassador, or high commissioner;
(g) High-ranking member of the armed forces; or,
(h) Board chair, chief executive, or chief financial officer of, or any other position that has comparable influence in, any State enterprise or international organization.

An *"immediate family member"* includes a:

(a) Spouse;
(b) De facto partner;
(c) Child and a child's spouse or de facto partner; or,
(d) Parent.

A "close associate" means any individual who is known (having regard to information that is public or readily available) to have:

(a) Joint beneficial ownership of a legal entity or legal arrangement with a politically exposed person referred to in paragraph (1); or,
(b) Sole beneficial ownership of a legal entity or legal arrangement that is known to exist for the benefit of a politically exposed person described in paragraph (1).

(3) A reporting entity must:

(a) Obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;
(b) Take reasonable measures to establish the source of funds; and,
(c) Conduct enhanced ongoing monitoring of the business relationship.

(4) Should a reporting entity:

(a) Receive any adverse information about a person, immediate family member or close associate that may affect the integrity of the business relationship, or,
(b) If it is unable to reasonably satisfy itself as the source of any funds, it must act reasonably and appropriately with regard to the further conduct of the business relationship which shall include consideration of the termination of the relationship.

(5) A reporting entity shall fully document the reasons for any decision regarding the further conduct of the business relationship.

22. Persons Connected to Sporting Events

(1) In addition to performing normal CDD measures, reporting entities must:

(a) Have appropriate risk-management systems to determine whether a customer is a

person, or a family member or close associate of such a person, who has a close connection to:

(i) A sporting event, team, sporting association or organization; and,
(ii) The reporting entity accepts bets on that team, sport, or sporting event.

(2) In this Section:

A *"person having a close connection to a sport or sporting event"* includes an individual who (having regard to information that is public or readily available) owns, plays with, coaches, trains or manages a sporting team, or who has a senior role with the governing body of a sport;

An *"immediate family member"* includes:

(a) Spouse;
(b) De facto partner;
(c) Child and a child's spouse or de facto partner; or,
(d) Parent.

A *"close associate"* means any individual who is known (having regard to information that is public or readily available) to have:

(a) Joint beneficial ownership of a legal entity or legal arrangement with a politically exposed person referred to in paragraph (1); or,
(b) Sole beneficial ownership of a legal entity or legal arrangement that is known to exist for the benefit of a politically exposed person described in paragraph (1).

(3) A reporting entity must:

(a) Obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;
(b) Take reasonable measures to establish the source of wealth and source of funds; and,
(c) Conduct enhanced ongoing monitoring of the business relationship.

(4) Should a reporting entity:

(a) Receive any adverse information about a person, immediate family member or close associate that may affect the integrity of the business relationship, or,
(b) If it is unable to reasonably satisfy itself as the source of any funds, it must act reasonably and appropriately with regard to the further conduct of the business relationship which shall include consideration of the termination of the relationship.

(5) A reporting entity shall fully document the reasons for any decision regarding the further

conduct of the business relationship.

23. Obligations to comply with Financial Sanctions

(1) A reporting entity must ensure compliance with United Nations ("UN") Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing and in particular must freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either (i) designated by, or under the authority of, the UN Security Council under Chapter VII of the Charter of the UN, including in accordance with resolution 1267 (1999) and its successor resolutions; or (ii) designated by that country pursuant to resolution 1373 (2001).

(2) A reporting entity must ensure compliance with UN Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing and, in particular, must freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the UN Security Council under Chapter VII of the Charter of the UN.

PART 4: RECORDS AND REPORTS

24. Record-keeping

(1) Reporting entities must maintain, for at least five years, all necessary records on transactions, both domestic and international.

(2) Reporting entities shall maintain records of the originator/payer information, and required beneficiary/payee information, on wire transfers, electronic fund transfers and other electronic payments.

(3) Reporting entities shall keep all records obtained through CDD including copies or records of official identification documents, account files and business correspondence, for at least five years after the business relationship is ended, or after the date of the occasional transaction.

(4) A reporting entity must provide the Commission with a copy of all records as specified by the Commission, whenever a reporting entity relocates the business or ceases business.

25. Reports of Suspicious Matters

(1) A reporting entity must lodge a suspicious matter report if, at a particular time:

(a) The reporting entity suspects on reasonable grounds that a customer is not the person the customer claims to be;
(b) The reporting entity suspects on reasonable grounds that the provision, or prospective provision, of its services is related to a financing of terrorism offence, or a money laundering offence, or other criminal offence; and/or,
(c) A transaction, for whatever reason, does not appear to have a lawful economic purpose.

(2) A suspicious matter report concerning a possible money laundering offence or other criminal offence must be lodged with the Commission within 5 business days after the day on which the reporting entity forms the relevant suspicion.

(3) A suspicious matter report concerning or in relation to possible financing of terrorism, must be lodged with the Commission within 24 hours after the time when the reporting entity forms the relevant suspicion.

(4) A suspicious matter report must contain a statement of the grounds on which the reporting entity holds the relevant suspicion.

(5) A reporting entity shall fully document the reasons for any decision regarding the submission or non-submission of a suspicious matter report.

26. Offence of Tipping Off

(1) If a reporting entity forms:

(a) A reasonable suspicion under Section 25 (1);
(b) Lodges a suspicious matter report with the Commission, or,
(c) provides documents or other information to the Commission,

neither the reporting entity nor any person employed or associated with the entity may disclose to someone other than the Commission that the suspicion has been formed, report lodged, or information has been communicated to the Commission, as applicable.

27. Report and Information Not Admissible

(1) In any court, tribunal, or disciplinary proceedings neither of the following is admissible in evidence:

(a) A suspicious matter report or any document purporting to set out information (including the formation or existence of a suspicion) contained in such a report; or,
(b) Whether any document or information was produced to the Commission in relation to such a report.

28. Power to Require Information

(1) The Commission may, by notice in writing, require any reporting entity to:

(a) Provide specified information, or information of a specified description;
(b) Produce specified documents, or documents of a specified description; or,
(c) Attend before an officer of the Commission at a time and place specified in the notice and answer questions.

(2) The information or documents must be provided or produced:

(a) Before the end of such reasonable period as may be specified; and,
(b) At such place as may be specified.

(3) The Commission may require:

(a) Information contained in a computer or other storage device, or recorded in any other way otherwise than in legible form to be produced to it in legible form or in a form from which the information can readily be produced in visible and legible form; and,
(b) Any information provided under this regulation to be provided in such form as it may require.

(4) The production of a document does not affect any lien which a person has on the document.

29. Power to Appoint External Auditor

(1) Where the Commission has reasonable cause for concern as to a reporting entity's compliance with these AML Regulations, the Commission may appoint a suitably qualified person to audit the entity's compliance and may do so at the reporting entity's expense.

PART 5: GENERAL

30. Amendment

(1) These AML Regulations may be amended at any time by resolution of the Commission.