BETTING GAMING & LOTTERIES COMMISSION

78CEF Hagley Park Road,
Kingston 10, Jamaica, W.I.
Tel: (876) 758-5601; 630-1353
Fax: (876) 758-7594; 758-4904
Email: info@bglc.gov.jm
Web: www.bglc.gov.jm

June 6, 2023

CIRCULAR LETTER TO:

ALL GAMING MACHINE OPERATORS - GAMING LOUNGES

- Chief Executive Officers
- Chief Operating Officers
- Nominated Employees
- Compliance Officers
- Other Principal Senior Officers
- Other Relevant Personnel

REF: CIR-005-06-2023

Policy for Anti-Money Laundering Compliance Programme

---

1. Introduction

Purpose of the Policy

The purpose of this policy is to provide guidance to the gaming sector in developing an effective compliance framework for Anti-Money Laundering, Counter Financing of Terrorism and Counter Financing of Proliferation (AML/CFT/CFP) measures. It covers essential areas such as policy and procedure, risk assessment, customer due diligence, enhanced due diligence, suspicious transaction reporting, record keeping, staff training and independent reviews.

Legal and Regulatory Requirements

The Betting, Gaming and Lotteries Commission (BGLC) is designated as the Competent Authority for the operations of entities operating twenty (20) or more gaming machines pursuant to a license granted by the Betting, Gaming and Lotteries Act (BGLA). The following Acts form the basis for developing an effective compliance program:

- Proceeds of Crime Act
- Proceeds of Crime (Money Laundering Prevention) Regulations
- Terrorism Prevention Act
- Terrorism Prevention (Reporting Entities) Regulations

- United Nations Security Council Resolutions Implementation Act
- The United Nations Security Council Resolutions Implementation (Asset Freeze-Democratic People's Republic of Korea) Regulations, 2013

Under Section 91 of the Proceeds of Crime Act, Section 18 of the Terrorism Prevention Act and Section 9 of the United Nations Security Council Resolutions Implementation Act the BGLC has the authority to issue guidelines to businesses in the regulated sector to prevent money laundering, terrorist financing and proliferation financing (ML/TF/PF).

Scope of the Policy

This policy applies to all entities operating twenty (20) or more gaming machines, pursuant to a license under the BGLA. It aims to ensure compliance with all applicable laws and regulations related to AML/CFT/CFP, including provisions of the Financial Action Task Force (FATF) recommendations. The policy is subject to periodic review and modification based on changes in the sector's operations, regulatory requirements, and risk assessment findings.

2. Policy and Procedure

An effective AML/CFT/CFP compliance programme requires the implementation of comprehensive policies, procedures, and controls to prevent and detect money laundering. These measures should ensure compliance with applicable laws and Regulations.

The policies and procedures must be documented, and include, but not limited to, the following:[1]

- Provisions for identifying high-risk operations and establishing a programme to manage those risks effectively.
- Provisions for the submission of reports to the Board (at least quarterly).
- Assignment of responsibilities to establish clear accountability for staff and ensure proper separation of duties as a control measure.
- Measures to ensure business continuity despite changes in management or employees.
- Definition of requirements for periodic reviews as well as timely updates to implement changes regarding the Regulations.
- Provisions for self-audits and independent reviews of the compliance program.
- The requirement for adherence to mandatory legislation.

[1] See Appendix that outlines the Minimum Standard for AML/CFT/CFP Policy and Procedural Manual

- Measure to ensure that the policies and procedures are updated annually and/or as dictated by legislative changes and industry practices. These updates should be approved by the Board or Senior Management.

3. Risk Assessment

A comprehensive risk assessment[2] is a fundamental component of an effective AML/CFT/CFP compliance programme. The risk assessment should identify and evaluate the inherent risks associated with the gaming operator, considering factors such as the types of games offered, customers served, geographic locations, transaction volumes, the sources of funds used to place bets and delivery channels. The risk assessment should be documented and regularly reviewed to ensure its accuracy and relevance.

4. Compliance Team

A compliance team plays a crucial role in ensuring the effectiveness of the AML/CFT/CFP compliance programme within the gaming lounge(s). Comprised of knowledgeable and dedicated professionals, the compliance team ensures the programme's implementation and adherence to regulatory requirements. They oversee policy implementation, conduct risk assessments, and act as a central point of contact for AML/CFT/CFP matters. The team also collaborates with other departments, reports suspicious activities, and maintains communication with regulatory authorities.

5. Customer Due Diligence

Customer due diligence (CDD)[3] measures are essential to a gaming operator's compliance program to understand the identity and risk profile of its customers. The CDD measures should be risk-based and commensurate with the level of risk posed by the customer. CDD should include the verification of customer identities through reliable sources, assessing the source of funds used to place bets and conducting ongoing monitoring of customer transactions and activities. Enhanced due diligence measures should be applied to high-risk customers and politically exposed persons (PEPs).

6. Monitoring Program

Ongoing monitoring is a critical component of the AML/CFT/CFP compliance program within the gaming lounge(s). It involves the continuous surveillance of customer transactions and activities to detect any suspicious or unusual patterns that may indicate potential illicit financial activities. This can be achieved through transaction monitoring systems that analyze customer transactions

---

[2] Refer to the Commission's circulars CIR-001-03-2023 and CIR-002-03-2023 dated March 17, 2023, which provide elaborative guidance on business and customer risk assessment.

[3] Refer to the Commission's circular CIR-003-05-2023, dated May 17, 2023, which provides guidance for CDD.

in real-time or near-real-time and based on predetermined thresholds. Factors such as transaction amount, frequency, counterparties, geographic locations, and customer profiles should be considered. By leveraging technology, the entity can enhance its ability to detect and prevent financial crimes.

7. Suspicious Transaction Reporting

The compliance program should establish mechanisms to identify, report, and investigate suspicious activity. Staff should be trained to recognize red flags of money laundering, such as unusual or larger transactions and to report them to the designated AML officer or a dedicated compliance team and the appropriate authorities. Timely and accurate reporting of suspicious transactions to the appropriate authorities is crucial for combating money laundering, terrorist financing and proliferation.

8. Record Keeping

Proper record keeping is essential for AML/CFT/CFP compliance. The compliance program should include policies and procedures for the retention of records related to customer transactions, CDD measures, suspicious transaction reports, and internal reviews for at least seven (7) years[4]. These records, whether in physical or electronic form, must be securely stored and readily accessible for regulatory examinations or law enforcement investigations.

9. Training

Training and awareness programs on a regular basis are vital to ensure that staff members understand their AML/CFT/CFP obligations and are equipped with the necessary knowledge and skills to fulfill them. The compliance program should include comprehensive training initiatives that cover topics such as

- understanding the legal and regulatory obligations related to AML/CFT/CFP
- the company's AML/CFT/CFP policies, procedures, and risk assessment methodology as well as any updates done;
- recognizing the warning signs and red flags of ML/FT/FP activities;
- emerging trends and typologies related to AML/CFT/CFP; and
- implementing effective control measures

[4] Regulation 14(5)(a) of the Proceeds of Crime (Money Laundering Prevention) Regulation

Employees should also be made aware of the ramifications of willful blindness[5] and tipping off[6] in executing their functions.

10. Independent Review

Regular independent reviews of the compliance program should be conducted to assess its effectiveness and identify any weaknesses or areas for improvement. These reviews may be conducted by internal audit teams, external consultants, or regulatory authorities. The findings and recommendations from these reviews should be documented and promptly addressed to enhance the overall compliance framework.

Commission's Expectations

The Commission expects licensees to comply with all relevant statutory and regulatory requirements concerning the AML/CFT/CFP compliance programme.

Where gaming machine operators identify any deficiencies in systems and controls, the Commission expects licensees to remedy them in a timely manner and to consider what assurance activities may provide comfort to the Board and senior management that those deficiencies have been effectively addressed.

The Commission will take enforcement action if the gaming operator is found to be in breach of this guidance.

Please be guided accordingly.

Yours sincerely,

BETTING, GAMING & LOTTERIES COMMISSION

.....

Laurie Wiggan (Mrs.)
Director of Compliance & Regulatory

---

[5] Deliberately choosing to ignore certain facts or information that would have otherwise alerted to suspicious transaction activity.

6 Disclosing information to a person who is likely to prejudice an investigation of money laundering or terrorist financing.

APPENDIX

Minimum Standard for AML/CFT/CFP Policy and Procedural Manual

- LEGISLATIVE OVERVIEW
    a) Betting, Gaming and Lotteries Commission (BGLC) Anti-Money Laundering Guidance Notes;
    b) Proceeds of Crime Act (POCA) Guidance Notes;
    c) The Proceeds of Crime Act, Proceeds of Crime (Amendment) Act, 2007, 2013, 2019;
    d) The Proceeds of Crime (Money Laundering Prevention) Regulations, 2007 and 2013, 2019 Amendments;
    e) The Terrorism Prevention Act (TPA), 2005 and 2011, 2012 and 2013 Amendments; and
    f) The Financial Investigations Division Act, 2010 and 2013 Amendment.

- ROLES AND RESPONSIBILITIES
    a) Designated Authority
    b) Competent Authority
    c) Board of Directors
    d) Senior Management
    e) Designated/Nominated Employee
    f) Employees

- ANTI-MONEY LAUNDERING & COUNTER FINANCING OF TERRORISM
    - Definition of money laundering: stages
    - Definition of Terrorist Financing
    - Proliferation of Financing
    - Similarities and Differences of ML and TF

- RISK BASED APPROACH (RBA)
    a) Risk-Based approach
    b) Risk assessment Requirements: Categorization of Risks, Risk Identification: Low Risk Clients, Medium Risk Clients and High-Risk Clients

- CUSTOMER DUE DILIGENCE AND ENHANCED DUE DILIGENCE
    a) Identification and Verification
    b) Acceptable Forms of Identification
    c) Verification Procedures
    d) How are customer details verified?
    e) Enhanced Customer Due Diligence
    f) On-going monitoring

- COMPLIANCE MONITORING AND TESTING
  - Monitoring of Transaction and Account Activity: Threshold Transaction
  - Nominated Employee monitoring, review and testing: policies and procedures
  - Independent Audit of Compliance Programme

- REPORTING TO THE DESIGNATED AUTHORITY (FID)
  - Suspicious Transaction
    - What is a suspicious transaction?
    - Examples of suspicious transaction in the gaming sector
    - Suspicious and Unusual Activities Indicative of Potential Terrorist Financing
    - Internal reporting of suspicious transaction
    - Reporting Suspicious Transaction to FID
    - Terminating Relationship due to continued suspicious activity
    - Treatment of suspicious transaction detected
  - Unusual Transaction
  - Prescribed Reports
    a) Suspicious Transaction Report (STR)
    b) Proscribe Entity Reports
    c) Listed Entities Report (LER)
    d) Authorized Disclosures (& Request for Consent)
    e) Procedure for Seeking Consent
    f) Reporting Procedure
    g) Penalties for Non-Reporting

- RECORD KEEPING
  - Transaction records
  - KYC documentation
  - Unusual and Suspicious Transaction reported to FID

- KNOW YOUR EMPLOYEE (KYE)
  a) Background due diligence
  b) Employee Training
  c) Wilful Blindness by employee
  d) Ongoing Monitoring
  e) Disciplinary Actions for non-compliance
  - Tipping off