

May 17, 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-003-05-2023

CUSTOMER DUE DILIGENCE (CDD)

1.1 Purpose

This Customer Due Diligence (CDD) Policy is intended to assist all gaming operators in meeting their CDD responsibilities as prescribed in the relevant legislation outlined in Section 1.3 below. Furthermore, the policy aims to provide regulated businesses with a clearer understanding of their customer identification, verification and monitoring obligations and is to be read and interpreted within the context of Jamaica's anti-money laundering, counter-terrorism financing and counter proliferation financing (AML/CFT/CFP) legal regime.

1.2 Scope

This policy outlines the approach to CDD procedures that regulated businesses should employ when establishing a business relationship or undertaking an occasional transaction¹ with a client, the procedures to be followed when verifying an individual's identity and the various situations in which CDD should be applied. These procedures aim to ensure that gaming operators can reasonably satisfy themselves that their customers are who they claim to be and embody a risk-based approach for determining the appropriate level of CDD measures to apply in any situation.

¹ Occasional transactions include- (a) the wagering of a stake, including— (i) the purchase from, or exchange with, the gaming operator of credits for use in gambling at the gaming lounge; and (ii) payment for use of gaming machines; (b) the collection of winnings, etc.

1.3 Legislative References

All gaming operators are reminded of their responsibility to implement customer due diligence measures as required of regulated businesses under the:

- Proceeds of Crime Act (POCA);
- Proceeds of Crime (Money Laundering Prevention) Regulations;
- Terrorism Prevention Act (TPA);
- Terrorism Prevention (Reporting Entities) Regulations;
- United Nations Security Council Resolutions Implementation Act (UNSCRIA);
- FATF Recommendations (1, 10, 11, 12, 17, 19 and 22); and
- Betting, Gaming & Lotteries Gazetted Guidance Notes.

2 Customer Due Diligence

2.1 What is Customer Due Diligence?

Customer due diligence (CDD) is the process in which a regulated business collects information on a prospective customer to ensure that at all stages of the business relationship they have a clear understanding of who the customer is and the intended nature of their business, as well as to assess any risk they may bring to the business.

Customer due diligence requirements should include:

- Identification of the customer;
- Verification of the customer's identity;
- Identification of beneficial owners and verification of their identity;
- Establishing the customer's risk profile;
- Establishing the purpose and intended nature of the business relationship;
- Taking reasonable measures to establish source of funds; and
- Monitoring customer activity on an ongoing basis to ensure that the transactions being conducted are consistent with the entity's knowledge of the customer, their business and risk profile, including, where necessary, their source of funds.

2.1.1 Levels of Due Diligence

Following the completion of a risk assessment to establish customer risk, one of three levels of due diligence may be performed proportionally to the increasing level of risk identified:

- **Simplified Due Diligence** – relaxed procedures used for low risk customers;

- **Customer Due Diligence (Standard Customer Due Diligence)** – standard procedures used for medium/average risk customers; or
- **Enhanced Due Diligence** – strengthened procedures used for high-risk customers.

2.1.2 When to Conduct Customer Due Diligence

Customer due diligence must be completed:

- before establishing a business relationship;
- before carrying out an occasional transaction;
- on an ongoing basis;
- when there is knowledge or suspicion of money laundering, terrorism financing or proliferation financing, irrespective of any threshold;
- at appropriate times and on a risk-sensitive basis, including at times when the operator becomes aware that the relevant circumstances have changed; and
- when doubts arise about the veracity or adequacy of previously obtained customer identification information.

2.2 Identification and Verification Measures

In performing CDD, operators must ensure that the customer produces satisfactory evidence of their identity as soon as reasonably possible after contact is first made, which must then be validated.

2.2.1 Customer Identification

A sound CDD program should have reliable customer identification and account opening procedures that allow the operator to establish the identity of the player. All prospective customers must undergo the process of identification upon registration, which involves the gathering of necessary personal data, including:

- Full true name and any aliases used;
- Current permanent address (including postal address, if different from the permanent address);
- Date of Birth;
- Place of Birth;
- Nationality;

- Taxpayer Registration Number (TRN) or other national reference number;
- Occupation/Business activity;
- Source of Funds (SOF); and
- Contact numbers (work, home, mobile/cell).

Operators must ensure that each customer is only permitted to register one (1) account and should implement procedures to conduct checks for customers holding duplicate accounts. Customers should also be prohibited from opening anonymous accounts, accounts under fictitious names, or numbered accounts².

2.2.2 Verification of Customer Information

To ensure compliance, gaming operators must verify customers' identities using reliable, current, independent source documents, databases, or information. Operators should establish to their reasonable satisfaction that the customer's provided identification information truthfully supports their claim of identity.

The verification of personal data provided should be done in a robust way to ensure reliability and ought to be considered an ongoing process. Additionally, operators should request and obtain the best possible documentation of identification from the customer to facilitate ease of verification.

2.2.3 Acceptable Identification and Verification Documents

Identification Documents

Identification documents, issued by reputable sources, must be obtained to establish a business relationship, and may include the following:

- Valid driver's licence, issued by the authorities in the country in which the person is a resident;
- Valid passport issued by the authorities in the country in which the person is a resident; or
- Valid voter's identification card.
- Any other national identification issued by the authorities in the country.

² A numbered account refers to an account that is identifiable solely by reference to the number or numbers assigned to that account.

If an identification document shows visible indications of fraud, the gaming lounge must consider those factors when deciding whether it can form a reasonable belief that it knows the customer's true identity.

Address Verification Documents

To verify a customer's address, an operator may use one of the following methods:

- Voter Identification Card;
- Driver's License;
- Residence Permit;
- Credit Card Statement or Bank Statement³; or
- Utility Bill⁴.
- National identification card issued by the Government

2.3 Risk Assessment of Customers⁵

Gaming operators are required to apply each of the CDD measures outlined in Section 2.1 above. However, the extent of such measures should be determined using a risk-based approach (RBA). The evaluation of the operator's customers, using a customer risk assessment to identify the risks arising from each customer connection, is at the heart of a risk-based strategy. This will enable operators to effectively manage such risks by using various procedures. Furthermore, a client's risk evaluation necessitates the operator categorizing each consumer as low, medium, or high risk.

A customer risk assessment must be undertaken:

- before establishing a business relationship with a customer or carrying out an occasional transaction;
- on a periodic basis; and
- whenever it is otherwise appropriate for existing customers, including where the operator becomes aware of any change to the risk factors associated with the customer that might contribute to the potential for money laundering, terrorism financing and proliferation financing (ML/TF/PF) risk to increase materially.

³ Issued by a reputable financial institution and may be retrieved electronically (e.g. via cellphone)

⁴ May be retrieved electronically (e.g. via cellphone)

⁵ Refer to Circular (CIR-002-03-2023) issued by the BGLC in May 2023, which provides detailed guidance on how to conduct a comprehensive Customer Risk Assessment

When conducting a customer risk assessment consideration must be given to all relevant risk factors including:

- the business risk assessment conducted;
- the nature, scale, complexity and location of the customer's activities;
- how products and services are provided to the customer;
- the frequency with which a customer uses a particular product or service; and
- the involvement of any third parties in elements of the customer due diligence process.

Once the level of risk has been determined, risk-specific procedures must be employed when dealing with the customer and adequate CDD measures applied.

2.4 Enhanced Due Diligence (EDD)

To adequately manage and mitigate high risks, each client designated as high risk must be subjected to enhanced customer due diligence in addition to standard customer due diligence.

2.4.1 Enhanced Due Diligence Procedures

EDD involves a more in-depth process of investigation and identification, which requires operators to obtain more detailed information from customers to enable them to:

- conduct additional verification and validation of customer identity;
- carry out more frequent updates of customer information;
- reasonably confirm a customer's location and occupation;
- take reasonable measures to establish and verify a customer's source of funds and/or wealth;
- satisfy themselves that transactions are consistent with the purpose and intended nature of the business relationship;
- obtain approval from senior management to commence or continue the business relationship;
- determine whether limits (e.g. threshold limits, disallowance of certain transactions, etc.) should be imposed on the business relationship or transaction;
- determine what additional ongoing monitoring should be carried out.

Establishment of Source of Funds/Wealth

It is crucial for gaming operators to obtain reliable information about their customers' SOF and SOW to comply with Anti-Money Laundering and Counter Financing of Terrorism and proliferation regulations. By verifying the legitimacy of their customers' wealth and the origins of

their funds, gaming operators can mitigate potential risks and protect their businesses and the financial system.

Source of funds (SOF) refers to the origins of money that a customer uses to fund transactions undertaken during the business relationship.

Source of wealth (SOW) refers to the customer's overall wealth or assets, regardless of whether they have a business relationship with the operator. The information gathered from a prospective client should reveal the amount of wealth that the prospective customer is reasonably anticipated to have and how it was attained.

Examples of sources of funds/wealth include:

- Employment income;
- Personal savings;
- Business ownership interests;
- Pension payments; and
- Inheritances.

Verification of Source of Funds/Wealth

Regulated businesses must validate the SOF/SOW for all applicants for business and one-off transactions that pose a high risk to the operator. Similarly to the need for customer identification verification, a regulated business must verify the SOF of a potential customer throughout the onboarding process and ensure that the SOW is validated where the circumstances described in Section 2.4.2 support this verification.

SOF/SOW can be verified using credible and independent sources, along with external confirmations and information provided by the applicant for business.

2.4.2 Trigger Events/Transactions for the Application of EDD Measures

Gaming operators should conduct enhanced customer due diligence:

- where a customer poses a higher risk of ML/TF/PF as assessed by the customer risk assessment;
- where the operator is unsure of the veracity of the customer's information or otherwise has reasonable grounds to suspect that a customer has provided false information or fraudulent identification documentation;

- in any business relationship or transaction with a customer that has affiliation to a country or jurisdiction identified as high risk by the FATF or any other relevant international body;
- whenever there is suspicion that a customer is subject to sanctions or freezing of assets as identified by the UN Sanctions List;
- in instances where the operator has determined that a customer, potential customer or beneficial owner is a PEP, or relative⁶ or known close associate⁷ of a PEP;
- in any case where a transaction is complex or unusually large, or there is an unusual pattern of transactions, and the transaction(s) have no apparent economic or legitimate purpose which, by its nature, can present a higher risk of ML/TF/PF; and
- where you know or suspect money laundering, terrorism financing or proliferation financing.

2.4.3 High Risk Customers

Examples of high-risk customers include, but are not limited to:

- A person who is not ordinarily resident in Jamaica;
- Politically Exposed Persons (PEPs);
- A person acting as a trustee for another in relation to the business relationship or one-off transaction concerned;
- A business relationship or transaction with a customer that resides or is domiciled in a specified territory⁸ or a country that has been identified as high-risk; or
- A member of such other class or category of persons as the Supervisory Authority may specify by notice published in the Gazette.

New or existing business relationships may not initially meet the criteria of high risk; however, this may change over time. Therefore, operators must ensure adequate screening measures are implemented to enable them to determine any changes in such status.

Politically Exposed Persons (PEPs)

Operators are required to take reasonable measures to determine whether a customer or beneficial owner is a domestic or international PEP. A politically exposed person is an individual who is or has been entrusted with prominent public functions and includes the following persons and their relatives and known close associates:

⁶ Relatives mean spouse, child (including stepchild or adopted child), the spouse of his child, his parents, or his brothers or sisters.

⁷ Close associate means an individual who is a business partner, or associated in any other form, in a common commercial enterprise with the person concerned.

⁸ See section 94A of the Proceeds of Crime (Amendment) Act, 2019

- A Head of State or Government;
- A member of any House of Parliament;
- A Minister of Government;
- A member of the judiciary;
- A military official above the rank of Captain;
- A member of the police force of or above the rank of Assistant Commissioner;
- A Permanent Secretary, Chief Technical Director, or Chief Officer in charge of the operations of a Ministry, department of government, Executive Agency or Statutory Body;
- A Director or Chief Executive of any company in which the government owns a controlling interest;
- An official of any political party; or
- An individual who holds, or has held, a senior management position in an international organization.

2.5 Simplified Due Diligence (SDD)

Simplified due diligence is a streamlined CDD process used when a regulated business has determined that a business relationship or one-off transaction presents a minimal risk of ML/TF/PF based on preliminary screening. Prior to seeking written approval from the Competent Authority and implementing SDD procedures, gaming operators must satisfy the conditions outlined in paragraph 2.5.1 below.

Despite the utilization of SDD procedures, regulated businesses are still expected to identify the applicant for business and take reasonable measures to verify the identity of the applicant.

2.5.1 Conditions for the Application of Simplified Due Diligence

Gaming machine operators intending to apply SDD must meet the requirements set out below:

- Identify, document and evaluate the risks of ML/TF/PF to justify the adoption of the SDD procedures;
- Implement appropriate controls and systems to reduce or mitigate those risks, which should be documented and readily available to the Designated Authority, Competent Authority and/or external auditors;
- Implement appropriate controls and systems to ensure sufficient monitoring of any business relationships or transactions which are subject to SDD measures to detect any unusual or suspicious transactions;
- Demonstrate a satisfactory level of compliance with all relevant laws concerning ML/TF/PF;

- Determine, having regard to guidance given by the BGLC, that the matter is one for the application of simplified due diligence procedures after considering the product features of the relevant business, such as –
 - i. the existence of features that permit or facilitate anonymous use of the product;
 - ii. whether non-face-to-face transactions are permissible;
 - iii. threshold limits for the value of transactions;
 - iv. whether cross-border transactions are permitted; and
 - v. and any other factors that the Competent Authority and the Designated Authority consider relevant.

Where there is any change in circumstances that renders the business relationship or occasional transaction high-risk, or the operator suspects or has knowledge of money laundering, terrorism financing, or proliferation financing, the operator must discontinue SDD measures and immediately apply customer due diligence and enhanced due diligence procedures where applicable.

2.5.2 Simplified Due Diligence Procedures

Once approval is granted by the Competent Authority, SDD may include the following:

- Requiring only one form of identification, preferably government-issued, from the prospective customer. However, regulated businesses may accept any form of identification as recommended by the Competent Authority;
- Collecting only basic identification information such as names, addresses, dates and places of birth, nationalities, TRNs or any other reference numbers⁹, contact numbers and sources of funds or, in the case of bodies corporate, dates and places of incorporation;
- Accepting identification verification from third parties who are under similar obligations concerning customer identification and transaction verification procedures;
- Reliance on publicly available documents or such other documents as the BGLC may specify;
- Reducing the frequency of customer identification updates;
- Reducing the degree of ongoing monitoring and scrutinizing of transactions; and/or
- Such other procedures as the BGLC may specify.

2.6 Actions to be Taken when CDD cannot be Conducted

Where the regulated business is unable to obtain satisfactory evidence of the identity of the customer and cannot conduct or complete the requisite CDD, the operator should:

⁹ Other reference number means any other uniquely assigned number, for example, tax identification number (TIN), or passport number.

- a) not commence a business relationship (new business);
- b) not carry out a transaction with or for the customer;
- c) terminate or suspend any existing business relationship with the customer;
- d) consider and determine whether the inability to conduct or complete CDD requires the submission of a suspicious transaction/activity report.

Gaming operators are not obliged to comply with (a) to (d) above if doing so would result in “tipping off”¹⁰ the customer or if they are otherwise directed by the Designated or Competent Authority. If necessary, the operator may carry on with the transaction and immediately inform the relevant authority through the required disclosure.

2.7 Reliance on a Third Party

Regulated businesses may use third parties to gather information for due diligence purposes such as third-party records or information services, or by making reasonable inferences about a customer’s identity using their databases of information. However, it is important to note that the operator retains ultimate responsibility for the outcome of this process. It is not enough for operators to simply rely on third parties to have already completed CDD on their behalf.

Where reliance is placed on a third party, operators must satisfy themselves that the third party is:

- of reputable integrity and reliability;
- not established in a high-risk jurisdiction;
- regulated, supervised or monitored for, and has measures in place for compliance with, CDD and record keeping requirements in line with relevant legislation;
- willing and able to provide copies of identification data and other relevant documentation relating to the CDD requirement upon request without delay;
- subject to a contractual agreement confirming that they accept being relied upon.

2.7.1 Name (Sanction) Screening Systems

Software solutions provide highly effective methods for quickly screening customer information such as names, dates of birth and national identification/reference numbers against collected customer data to detect politically exposed persons (PEPs), sanctioned/listed individuals, or

¹⁰ Disclosing information with the knowledge or belief that a protected or authorized disclosure has been made or is to be made under Section 100 of the POCA, where such disclosure is likely to prejudice any investigation that might be conducted following the disclosure.

individuals who are the subject of negative public domain information (e.g. charged with criminal activity).

Gaming operators should carefully consider which providers they contract with, how the systems are configured, have a good understanding of the system and its parameters, and not be completely dependent on the system provider.

When selecting a third-party IT solution, consideration should be given to:

- Whether the system provides functionality for a manual check (i.e. you type in a name to search) or automated (i.e. you upload a list of names or it runs against your database);
- Whether the system provides a one-off check, periodic or real-time monitoring;
- Where the system pulls information from (e.g. public databases, internet searches, manual research);
- What PEP definition is used in the system;
- Which countries are covered (e.g. does it include the US OFAC sanctions list?);
- How your data is used (e.g. does it go to their servers, are there data protection issues?);
- Whether the system provides audit trail functionality (i.e. recording the outcome of investigations, discounting of false positives, etc.);
- Whether there is functionality to screen against names and other data (i.e. date of birth) to reduce false positives;
- Whether the screening includes negative press screening (e.g. public domain information about criminals, etc.);
- Whether there is the ability to customize settings (e.g. types of negative press you care about, how close a name match must be to alert, etc.); and
- Whether there is a need for the functionality to check foreign language characters on registration details (e.g. Chinese, Japanese, etc.).

3 Ongoing Due Diligence and Monitoring

Gaming operators are required to conduct ongoing monitoring of all customer relationships since the customer identification process does not end once a business relationship has been established. It is not always adequate to rule out the possibility of ML/TF/PF risk even after a new customer has been first satisfactorily identified.

3.1 Monitoring of Transactions and Activities

Regulated businesses are required to conduct ongoing due diligence, including scrutiny of transactions to ensure consistency with their knowledge of the customer. The degree of the ongoing due diligence to be undertaken will depend on the customer risk assessment conducted.

When undertaking ongoing monitoring, operators must:

- a) review information and documents held for the purpose of customer due diligence to ensure that they are up-to-date, accurate and appropriate, in particular where that transaction or relationship poses a higher risk of ML/FT/PF;
- b) scrutinize transactions and other activities undertaken during the course of the customer relationship to ensure that it is consistent with the operator's knowledge of the customer, their business, risk rating, and their source of funds/wealth;
- c) pay particular attention to any complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or legitimate purpose;
- d) enquire into the background and purpose of the transactions in (c);
- e) monitor whether the customer or any known beneficial owner is listed on the Sanctions List; and
- f) periodically review each customer to ensure that the risk rating assigned remains appropriate for the customer considering the ML/TF/PF risks.

The extent and frequency of any monitoring must be determined:

- in accordance with the risk assessment completed;
- based on materiality and risk of ML/TF/PF; and
- having regard to whether a customer poses a higher risk of ML/TF/PF.

Through monitoring customer transactions and activities, operators should be better able to:

- Identify behaviours/transactions, which diverge from the usual pattern, or do not fit with the customer's profile, or are otherwise not in line with what is normally expected from the customer;
- Identify suspicious activities/transactions for which a suspicious activity/ transaction report (SAR/STR) needs to be filed with the Designated Authority; and
- Determine whether the initial risk assessment requires updating, and whether, given the updated risk assessment or other considerations, the operator desires to continue the business relationship.

4 Suspicious Transaction/Activity Reporting (STR/SAR)

4.1 Identifying Suspicious Transactions/Activities

Effective customer due diligence measures and record keeping form the basis for recognizing unusual and suspicious transactions/activities. Where there is a customer relationship, suspicious activity will often be inconsistent with a customer's known legitimate activity or with the normal business activities for that type of account or customer. Therefore, the key to recognizing "suspicious activity" is knowing enough about the customer and the customer's normal expected activities to recognize when their actual activity is abnormal.

Circumstances that might give rise to suspicion or reasonable grounds for suspicion of ML/TF/PF include, but are not limited to:

- a) transactions which have no apparent purpose, which make no obvious economic sense;
- b) transactions or activities which are inconsistent with a customer's normal known activity;
- c) where the size or pattern of transactions, without reasonable explanation, is out of line with any pattern that has previously emerged or may have been deliberately structured or designed to avoid detection;
- d) customer's refusal to provide the information requested without reasonable explanation;
- e) frequent cash-out transactions without corresponding buy-in transactions;
- f) use of the gaming account as a savings account.

Operators must also ensure sufficient guidance is given to their employees to enable them to form a suspicion or to recognize when they have reasonable grounds to suspect that ML/TF/PF is taking place. This should involve training that will enable relevant employees to request and assess the information that is required for them to judge whether a person is involved in suspicious activity related to ML/TF/PF. If the employee reasonably believes that performing CDD measures will tip off a customer or potential customer, they may choose not to pursue that process and should file a SAR.

Where an operator identifies any unusual activity during an ongoing customer relationship or occasional transaction, the operator must, within fifteen (15) days:

- perform appropriate scrutiny of the activity;
- conduct enhanced customer due diligence; and
- consider whether to make a disclosure.

4.2 Internal Disclosures

Where a staff member reasonably believes or has grounds for suspicion that a customer or prospective customer is engaged in ML/TF/PF a disclosure must be made to the Nominated Employee (NE). All disclosure reports must be submitted directly to the NE without any unnecessary delay and, in any event, within fifteen (15) days of the information's receipt.

All suspicions reported to the Nominated Employee must be documented and should contain the customer's identity details, relevant transactions, and an explanation for suspicion.

4.3 External Disclosures

Following the receipt of an internal disclosure, the NE should consider whether a report should be submitted to the Designated Authority. Once it is determined that the information substantiates a suspicion of ML/TF/PF, the NE must make a disclosure within fifteen (15) days of receiving the information. Additionally, if the NE concludes that there is uncertainty as to whether the information submitted constitutes a suspicion, a report should still be made with the Designated Authority.

If the NE decides that the information does not substantiate a suspicion, the reasons for not submitting the report to the Designated Authority must be documented.

Where the gaming operator is convinced that it must proceed with the transaction, relationship, or arrangement, before making the relevant disclosure and securing the appropriate consent¹¹ the institution must:

- have a reasonable excuse for failing to make the disclosure before proceeding with the transaction;
- make the relevant disclosure on its own initiative; and
- make the said disclosure as soon as is reasonably practical.

¹¹ Appropriate consent occurs- i. when the Designated Authority gives consent to undertake the prohibited act within seven (7) business days of the request for consent; ii. after a request is made and there is no response from the Designated Authority and seven (7) business days have passed; or iii. after consent has been denied but ten days have passed since the denial of consent notice was received.

5 Record Keeping and Retention

5.1 Record Keeping Requirements

Operators must implement policies, procedures and systems that allow them to meet their obligation to retain, for the required period of seven (7) years, records of the measures that were applied to establish the identity of customers and all necessary records of gaming transactions completed. Such records must be sufficient to recreate individual transactions and, if required, provide adequate evidence for criminal prosecution.

Records should be kept of:

- the identity of all current and prior registered customers;
- all information used to register a customer;
- supporting records captured to verify a customer's identity;
- any due diligence report created;
- any changes made to a customer's account;
- any customer risk assessments and risk ratings conducted;
- any action taken as a result of the customer assessment (including monitoring, reporting, or restrictions placed on the customer's account and/or gaming activity);
- the customer's activity and transactions (all deposits and withdrawals);
- specific procedures performed to analyze a customer's gaming patterns and transactions, and all corresponding results of that analysis;
- any internal and external reports, whether or not they have been submitted;
- employee training records;
- contact between the operator and any relevant authority.

5.2 Updating of Customer Information

Customer information should be kept under review and should be updated:

- at least once in every seven (7) years during the course of the business relationship;
- at more frequent intervals as warranted by the risk profile;
- when there is doubt about the veracity or adequacy of previously obtained information;
- when the customer's transactions are inconsistent with their financial profile;
- where transactions which are carried out in a single activity or in several activities appear to be linked;
- where any cash transaction involves or exceeds the prescribed amount;
- where the transaction being conducted is a wire transfer;
- when there is a material change in the business relationship with the customer;

- when there is a material change in the manner in which the account is operated;
- when there are doubts regarding the identity of the customer or the beneficial owner of the account;
- when the gaming establishment changes its CDD documentation requirements; or
- where the regulated business is required to file a STR.

6 Commission's Expectations

The Commission expects licensees to comply with all relevant statutory and regulatory requirements concerning customer due diligence (CDD) measures.

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 effectively been addressed.

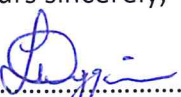
The goal of this **REF: CIR-003-05-2023** is:

- to ensure the gaming operator understands their obligations as it relates to evaluating overall risk and developing and implementing adequate customer due diligence measures to mitigate those identified risks;
- to improve staff knowledge to enhance the application of the measures;
- to ensure the gaming operator is in the best position to prevent the gaming lounge from being used to facilitate money laundering, terrorism financing, or the proliferation of weapons of mass destruction; and
- to ensure compliance with the Proceeds of Crime (Money Laundering Prevention) (Amendment) Regulations, 2019 and other relevant legislations.

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

Please be guided accordingly.

Yours sincerely,



.....
Laurie Wiggan (Mrs.)

Director, Compliance & Regulatory

BETTING, GAMING & LOTTERIES COMMISSION