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

**March 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-002-03-2023**

***CUSTOMER RISK ASSESSMENT (CRA)***

---

The Betting Gaming and Lotteries Commission (BGLC) reminds all gaming operators of their responsibility to conduct customer risk assessments as required of regulated businesses under the Proceeds of Crime Act (POCA), the Proceeds of Crime (Money Laundering Prevention) Regulations, the Terrorism Prevention Act (TPA), FATF Recommendations (1, 10, 12, 19 and 22) and the BGLC's Gazette Guidance Notes.

A comprehensive customer risk assessment should be:

- conducted to ensure there is clear identification, determination and understanding of money laundering or terrorist financing risk
- conducted on an accurate and comprehensive understanding of presented and potential threats and vulnerabilities
- periodically undertaken on an ongoing basis to account for emerging and changing risks and circumstances
- documented as a methodology, approved by the Board of Directors and kept up to date
- available upon request to internal and external auditors as well as the Competent and Designated Authorities.

**Risk is a function of three factors:**

i. Threats

This encompasses individuals, groups and/or particular activities which have the potential to introduce criminal elements into the gambling sector. This can manifest itself in various respects including criminal groups or individuals seeking ownership or control of gambling operators for illegal purposes; the intentional laundering of funds through gambling operators or simple criminal spend; and operators not being fully aware of or negligent in respect of their responsibilities.

ii. Vulnerabilities

This refers to the inherent aspects of gambling operators' services which are open to potential exploitation for the purposes of supporting or facilitating money laundering and/or terrorist financing. These can generally be sub-divided into the following categories:

a) Internal Control Vulnerabilities;
b) Licensing and Integrity Vulnerabilities;
c) Customer Related Vulnerabilities;
d) Product Related Vulnerabilities;
e) Payment Method Vulnerabilities

iii. Consequences

This refers to the impact or harm that money laundering or terrorist financing may cause, including the effect of the underlying criminal and terrorist activity on financial systems and institutions, the economy and society more generally.

The key to any risk assessment is that it adopts an approach that attempts to distinguish the extent of different risks to assist with prioritizing mitigation efforts, rather than being a generic box-ticking exercise.

**The risk assessment process should consist of the following standard stages:**

**i. Identification**

This stage seeks to develop an initial list of potential risks or risk factors when combating money laundering and terrorist financing.

**ii. Analysis**

This stage involves consideration of the nature, sources, likelihood, impact and consequences of the identified risks or risk factors. The aim of this stage is to gain a

comprehensive understanding of each of the risks. Risk analysis can be undertaken with varying degrees of detail, depending on the type of risk, the purpose of the risk assessment, and the information, data and resources available.

**iii. Evaluation**

This stage involves assessing the risks analyzed during the previous stage to determine priorities for addressing them, taking into account the purpose established at the beginning of the assessment process. These priorities can then contribute to development of a strategy for the mitigation of the risks.

## 1. WHY?

A customer risk assessment is necessary to enable each entity to:

- identify the composition of the customer base and the risks posed by each customer;
- fully understand the risks identified;
- determine the overall risk rating of each customer, since not all customers will pose similar risks and, as such will require different treatment.

Being cognizant of the foregoing, the operator is enabled to develop and implement sufficient and appropriate mitigation measures.

## 2. WHEN?

The customer risk assessment must be completed:

a) prior to establishing a business relationship with a customer or carrying out an occasional transaction[1];
b) on a periodic basis; and
c) 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 a significant increase in the risk of money laundering or terrorist financing.

## 3. HOW?

Gaming licensees are required to:

a) take appropriate steps to identify and assess ML/TF/PF risks to which its business is exposed, taking into consideration the nature, size and complexity of its activities;

[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

b) when identifying and assessing the risks in (a), take into account, to the extent relevant, any vulnerabilities relating to:
   i. its type of customers and their activities;
   ii. the countries or geographic areas in which it does business;
   iii. its products, services and activity profiles;
   iv. the complexity and volume of its transactions;
   v. the development of new products and business practices including new delivery mechanisms, channels and partners;
   vi. the use of new or developing technologies for both new and pre-existing products and services;
   vii. its employees
   viii. unusual transactions
   ix. transactions outside of the customer's normal activity
   x. transactions arising from higher risk counties as outlined in the FATF recommendations

c) monitor information held relative to:
   i) Customer's Financial Habits
   (ii) Customer's Gambling Habits

d) give due consideration to the ML/TF/PF risks posed by their business-to-business relationships including any third parties they contract with. The assessment of these risks is based, among other things, on the risks posed to the operator by transactions and arrangements with business associates and third-party suppliers such as gaming product suppliers or payment providers and processors, including their beneficial ownership and source of funds. Effective management of third-party relationships should assure gaming establishments that the relationship is a legitimate one, and that they can evidence why their confidence is justified.

Key assessment factors to be analyzed for the customer should include[2]:

1. Customer's identification
2. Customer's address, nationality, and country of residence (Specified territories, High-Risk Jurisdictions, etc.)
3. The authenticity of provided identification verification documents
4. Type of customer (Domestic, Foreign, PEPs, high roller, high-cash business, etc.)
5. Types of customer payments and payment methods
6. Customer's occupation
7. Customer's source of funds/wealth
8. Expected/anticipated customer activity

[2] The listing is not exhaustive and should be curated to include any other factor that may present a customer risk specific to your gaming lounge.

9. Customer spending pattern and behaviour (inconsistencies with client profile, unusual transactions, etc.)
10. The reputation of the customer (Adverse news)

The combination of these factors will indicate the level of money laundering or terrorist financing risk.

## 4. RISK MATRIX

A customer's risk assessment requires the operator to assign the customer an appropriate risk rating. Risk ratings should be descriptive, such as "low", "medium", or "high", or a sliding, ordinal numeric scale, such as 1 for the lowest risk to 3 for the highest, with at least three distinct risk ratings. All the aforementioned factors should be evaluated to assess and assign the appropriate risk rating to the customer. This may be done with the use of a risk matrix, which is a visual representation of the risk analysis that categorizes risk depending on its level of likelihood and impact.

Additionally, the weight given to each risk factor highlighted in section 3 used by the operator in assessing the overall risk of money laundering or terrorist financing, both individually or in combination, may vary from one operator or premises to another, depending on their respective circumstances. As a result, operators must make their own decisions on how much weight to assign to each risk factor.

**NB.** The risk matrix should be designed to meet the demands of each respective gaming operator. It should not be static and should be updated as risk factors change.

### 4.1. Guidance on High-risk Customers

1. Deciding that a customer presents a higher risk of money laundering or terrorist financing does not automatically mean that the person is a criminal, money launderer or terrorist financer. Similarly, identifying a customer as presenting a low risk of money laundering or terrorist financing does not mean that the customer is definitely not laundering money or engaging in criminal spend. Employees therefore need to remain vigilant and use their experience and common sense in applying the operator's risk-based criteria and rules, seeking guidance from their nominated officer as appropriate.

2. When assessing the risk factors, the operators must bear in mind that the existence of one or more risk factors does not always imply a high risk of money laundering or terrorist financing in a given context. An example of a business relationship conducted in unusual circumstances would include but is not limited to, a business relationship or proposed business relationship

that involves, or would involve, significant unexplained geographic distance between the location of the operator and the customer or proposed customer.

3. The highest risk products or services in respect of money laundering or terrorist financing are those where unlimited third-party funds can be freely received from or paid to third parties, without evidence of the identity of the third parties being obtained and the identity being verified.

4. Generally, the lowest risk products in respect of money laundering or terrorist financing are those where funds can only be received from a named customer by way of payment from an account held in the customer's name, and similarly where the funds can only be remitted to a named customer.

## 5. OUTCOME OF THE RISK ASSESSMENT

The AML/CFT/CFP risks associated with each customer differ and require an adequate risk management response that is proportionate to the level of risk presented.

Based on the outcomes of the operator's assessment of its customers' money laundering risk, the operator should decide what degree of customer due diligence (CDD)[3] is required. In the case of a customer who poses a high risk of money laundering or terrorist financing, the operator is obligated to conduct Enhanced Due Diligence (EDD)[4] in addition to the standard CDD. For a low-risk customer, the operator may be able to conduct Simplified Due Diligence (SDD)[5]. For any other customer, the operator must undertake CDD.

Additional information should include an understanding of where the customer's funds and wealth have come from. While the Commission recognizes that some relationships with customers will be transient or temporary in nature, operators still need to give consideration to this issue.

[3] Customer due diligence (CDD) is an umbrella term used to describe the various measures required to be carried out, including, for standard risk customers, identification, verification of identity, source of funds and ongoing monitoring.
[4] Enhanced due diligence (EDD) is the term used to describe measures that are required to be carried out for higher-risk customers in addition to the CDD requirements required for standard-risk customers.
[5] Simplified Due Diligence is the lower level of customer due diligence that is conducted on an individual that poses a low risk of money laundering or an act of terrorist financing. In Simplified Due Diligence, the individual poses a lower risk than Standard Due Diligence and far lesser risk than customers in the Enhanced Due Diligence category.

## 6. ONGOING MONITORING

Operators should ensure that the arrangements that they have in place to monitor customers and the accounts they hold across locations, products and platforms are sufficient to manage the risks to which the operator is exposed. This should include the monitoring of account deposits (cash-ins) and withdrawals (cash-outs). Those operators that rely heavily on gaming machines should also have practical systems in place to effectively monitor and reconcile customer spend on gaming machines. Any suspicious activity should be reported by means of a STR to the Designated Authority.

Once knowledge or suspicion of criminal spend is linked to a customer, operators should monitor the customer's activity. Additionally, an operator must apply an enhanced ongoing monitoring programme for higher-risk transactions and customers. Moreover, the degree of the ongoing monitoring to be undertaken will depend on the customer risk assessment carried out.

### 6.1. WHEN?

An operator should undertake a review particularly when:

a) the operator changes its CDD documentation requirements;
b) an unusual transaction with the customer takes place;
c) there is a material change in the business relationship with the customer.

One of the most important aspects of effective CDD is the operator's transaction monitoring policies, procedures, systems, and controls, which may be implemented by manual or automated systems, or a combination thereof. Whether an operator should undertake the monitoring through a manual or computerized system (or both) will depend on several factors, including:

a) the size and nature of the operator's business and customer base; and
b) the complexity and volume of customer transactions.

### 6.2. HOW?

When undertaking ongoing CDD, an operator must:

a) monitor transactions undertaken during the course of its customer relationship to ensure that the transactions are consistent with the operator's knowledge of its customer, its business and its risk rating;
b) pay particular attention to any complex or unusually large transactions or unusual patterns of transactions (both financial or gambling) that have no apparent or visible economic or legitimate purpose;
c) enquire into the background and purpose of the transactions in (b);

d) periodically review the adequacy of the CDD information it holds on customers to ensure that the information is kept up to date, particularly for customers with a high-risk rating;
e) review its customers, their businesses, and transactions against Sanctions Lists; and
f) periodically review each customer to ensure that the risk rating assigned to a customer remains appropriate for the customer in light of the money laundering risks.

**NB.** An operator is expected to ensure that the information and the evidence obtained from a customer are valid and have not expired, for example when obtaining copies of identification documentation such as a passport or identification card. Examples of non-static identity documentation include passport number and residential/business address and, for a Legal Person, its share register or list of partners.

Where an operator identifies any unusual activity in the course of an ongoing customer relationship or occasional transaction, the operator must, within a reasonable timeframe:

a) perform appropriate scrutiny of the activity;
b) conduct enhanced customer due diligence; and
c) consider whether to make an internal disclosure and/or disclosure to the relevant authorities.

The extent and frequency of any monitoring must be determined:

a) on the basis of materiality and risk of ML/FT;
b) following the risk assessments carried out; and
c) having regard to whether a customer poses a higher risk of ML/FT.

## 7. TERMINATING A BUSINESS RELATIONSHIP

Operators are required to have and operate procedures to examine the background and purpose of the relationship and ensure that, satisfactory verification of identity is held from the outset of the relationship and periodically thereafter.

All operators need to consider ending the business relationship with a customer in the following circumstances:

a) If an operator is unable to obtain satisfactory information and verification within a reasonable timeframe;
b) where it is known that the customer is attempting to use the operator to launder criminal proceeds or for criminal spending;
c) where the risk of breaches to POCA is considered by the operator to be too high; and
d) where the customer's gambling activity leads to a steadily increasing level of suspicion, or actual knowledge, of money laundering.

## 8. SYSTEMS AND CONTROLS

When devising internal procedures, the operator should consider how its customers and operational systems impact the capacity of its staff to identify suspicious transactions.

Effective risk mitigation strategies are not only useful for compliance purposes but also provide powerful techniques to prevent fraud. After all, the obscuring or falsification of identity is a cornerstone of any successful fraudulent activity.

Requiring accurate identity information from the outset of the relationship and adding layers of identity information to match the risk level is fundamental to the risk-based approach. Also, several factors may have an impact on risk levels, which will also affect the preventative measures needed to tackle the risks proportionally. These variables include:

- The types of gambling products offered
- The types of payment methods used by customers
- The customers' gambling habits
- The amount wagered
- The account history
- The location of the customers
- The credit history of the customers
- The identity profile
- Changes in the identity profile

and many other factors that can help determine the associated risk of a prospect or customer.

Carefully crafting workflows that accurately consider these factors, at the right time, is fundamental to creating a risk-based approach to gaming that works for players, operators and regulators.

Additionally, operators are best placed to identify and mitigate risks involved in their business activity. A crucial element of this is to ensure that systems are in place to identify and link player activity, and for senior management to oversee risk management and determine whether their policies and procedures are effective in design and application. Reliance on third parties to conduct risk assessment does not relieve the operator of its ultimate responsibility to assess and manage its risks.

### MUST DO

- The operator is to ensure that the risk identification and analysis is properly documented to demonstrate that this forms the basis of its AML/CFT/CFP policies and procedures. The Commission will also require sight of the risk assessment and the methodology utilized.

- Operators must ***ensure*** that periodically, frontline personnel and all other relevant staff involved in customer onboarding and conducting of transactions are made aware of all relevant legislation and operational procedures and provided with the requisite training in the recognition and handling of transactions involving money laundering, terrorism financing, or proliferation financing.

- The gaming lounge operators should monitor changes to the regulatory framework and publications in respect of the level of risk identified in national or sector-specific risk assessments conducted in Jamaica. Any matter which impacts the gaming lounge operator's approach to CRA should be considered and implemented into policies and procedures as soon as practicable.

- Any delays or issues in conducting CRAs in line with the relevant person's policies and procedures are reported to the board and senior management.

- Compliance monitoring of systems and controls relevant to CRA is conducted independently and at an appropriate frequency. The results of the testing are considered by the board/senior management and prompt action is taken to address deficiencies.

- Information regarding the risks present within the gaming lounge operator's customer base is provided to the board/senior management for consideration in a report at least quarterly or more frequently as warranted by the risk profile of the institution, and the Business Risk Assessment is updated if necessary.

## 9. COMMISSION'S EXPECTATIONS

The Commission expects licensees to comply with all relevant statutory and regulatory requirements concerning customer risk assessment (CRA).

Where gaming machine operators identify any deficiencies in systems and controls, the Commission expects licensees to provide a written report/response, and:

- prepare and document a remediation plan setting out the timelines and discuss this with the Commission.
- remedy any identified deficiencies in the manner set out in the documented remediation action plan agreed with the Commission; and
- consider what assurance activities may provide comfort to the Board and senior management that deficiencies identified have been addressed effectively.

In future examinations with us, gaming machine operators may be asked to evidence steps taken to address identified deficiencies in their control environment.

The goal of this **REF: CIR-002-03-2023** is:

- to ensure the gaming operator understands their obligations as it relates to evaluating overall risk and developing and implementing adequate policies, procedures, and controls 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
Director, Compliance & Regulatory
**BETTING, GAMING & LOTTERIES COMMISSION**