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

October 6, 2023

ADVISORY 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-007-09-2023

TRANSACTION MONITORING

Purpose

This Transaction Monitoring advisory is designed to guide all gaming operators in fulfilling their transaction responsibilities as mandated by the relevant legislation outlined below. Furthermore, this advisory seeks to provide regulated businesses with a comprehensive understanding of their transaction monitoring obligations, which must be interpreted within the context of Jamaica's anti-money laundering, counter-terrorism financing, and counter-proliferation financing (AML/CFT/CFP) legal framework.

Legislative References

All gaming operators are reminded of their responsibility to undertake transaction monitoring as required of regulated businesses under the following:

- **Proceeds of Crime Act (POCA):** This foundational legislation empowers gaming operators to identify and report suspicious financial activities, preventing criminal funds from infiltrating the gaming industry.

- **Proceeds of Crime (Money Laundering Prevention) Regulations:** These regulations provide the framework for effective money laundering prevention, outlining specific transaction monitoring requirements for gaming operators.
- **Terrorism Prevention Act (TPA):** Gaming operators are crucial stakeholders in national security efforts, as they are expected to monitor transactions that may be linked to terrorist financing.
- **Terrorism Prevention (Reporting Entities) Regulations:** These regulations define the obligations of gaming operators in reporting suspicious transactions linked to terrorism, ensuring the industry does not inadvertently support terrorist activities.
- **United Nations Security Council Resolutions Implementation Act (UNSCRIA):** As part of the global effort to combat terrorism, gaming operators must align their transaction monitoring practices with UN sanctions and restrictions. This includes tracking and reporting transactions involving individuals or entities subject to UN sanctions.
- **FATF Recommendations:** The Financial Action Task Force (FATF) sets international standards for AML/CFT/CFP, and gaming operators must adhere to these guidelines to maintain the integrity of their operations.[1]
- **Betting, Gaming & Lotteries Gazetted Guidance Notes**: These guidance notes provide practical insights into transaction monitoring specific to the gaming industry, helping operators to apply regulatory expectations effectively.

Transaction Monitoring

What is transaction monitoring?

Transaction monitoring is the ongoing, systematic process of meticulously tracking, meticulously analyzing, and critically evaluating financial transactions conducted by customers within gaming establishments. This process is integral to identifying and reporting any activities that raise suspicions of money laundering, terrorist financing, or proliferation of weapons of mass destruction. It is a vital component of your AML/CFT/CFP compliance framework, ensuring the integrity of your operations and safeguarding the broader financial system.

Additionally, transaction monitoring is not a one-size-fits-all endeavor. Instead, it must be tailored to the risk profile of your customers and the specific nature and complexity of their transactions. Recognize that some customers and transactions carry higher inherent risks than others. For instance, a high-roller customer who frequently engages in large transactions poses a higher risk

[1] For instance, FATF Recommendation 17 specifically addresses gaming establishments, highlighting the importance of robust transaction monitoring.

than a casual player. Consequently, your transaction monitoring practices should be more frequent and intensive for higher-risk scenarios.

The extent of transaction monitoring is based on the risk profile of the customer or the nature and complexity of transactions. The depth and frequency of transaction monitoring should correspond directly to the perceived risk. For example, a customer with a history of large cash transactions and international wire transfers may warrant continuous real-time monitoring, whereas a low-risk customer with infrequent, small transactions may require less intensive scrutiny. Tailoring your monitoring measures ensures that resources are allocated efficiently and effectively.

What is the difference and correlation between enhanced due diligence and transaction monitoring?

While enhanced due diligence involves the collection of additional information about high-risk customers, transaction monitoring is concerned with actively detecting and assessing suspicious activities in real time or through retrospective analysis. These two components are interdependent, with enhanced due diligence providing the foundation upon which transaction monitoring operates. Together, they ensure comprehensive AML/CFT/CFP compliance. For example, if a customer's enhanced due diligence reveals a politically exposed person (PEP) status, transaction monitoring should focus on that customer's transactions with heightened scrutiny.

Detection Rules for Transaction Monitoring

1. Risk-based detection rules

Effective transaction monitoring relies on the application of risk-based detection rules. These rules consider various risk components, such as product type, payment method, customer characteristics, and geographic factors. For example, if your gaming establishment offers online betting, transactions from high-risk jurisdictions should trigger enhanced monitoring.

2. Scenario-based detection

To enhance your monitoring capabilities, develop predefined scenarios that encompass known patterns and typologies of suspicious activities. These scenarios serve as a proactive mechanism for flagging potentially illicit transactions. For instance, a scenario could involve identifying customers who consistently deposit large sums in cash and make minimal withdrawals.

3. Threshold-based detection

Establishing specific thresholds for various transaction parameters, such as transaction amounts or frequency, is another key element of transaction monitoring. Transactions that exceed these predefined thresholds trigger monitoring and investigation, helping you identify unusual or potentially illicit financial activity. For example, you may set a threshold that triggers monitoring when a customer makes a single cash deposit exceeding $10,000 within a 24-hour period.

Some possible red flags in transaction monitoring

1. *Deposit amount inconsistent with player financial information*

Vigilantly review customer financial profiles and promptly flag significant disparities between deposit amounts and their stated financial status. For example, if a customer claims to have a modest income but consistently makes large cash deposits, this inconsistency may suggest an attempt to launder funds through gaming activities.

2. *Lack of withdrawals from customer accounts*

Investigate accounts with prolonged periods of inactivity or abnormal withdrawal patterns, as this may indicate efforts to conceal illicit funds within gaming accounts. For instance, if a customer's account shows no withdrawals despite regular gaming activity, this could be a red flag.

3. *High-value transactions from PEPs (Politically Exposed Persons)*

Pay meticulous attention to transactions involving Politically Exposed Persons (PEPs) and their associates. PEPs are individuals who hold prominent public positions, and their financial transactions may pose a higher risk of corruption or misuse. If a PEP frequently engages in high-value transactions within your gaming lounge, this should trigger enhanced scrutiny.

4. *Rapid deposits on customer accounts, even with significant losses*

Keep a close watch on accounts experiencing unusual deposit patterns, particularly when large deposits coincide with substantial losses. Such behavior may suggest attempts to layer illicit funds through gaming activities. For instance, if a customer makes frequent large deposits despite consistently losing money, this could indicate suspicious activity.

5. *Substantial Changes in Transaction values or volumes*

Be alert to significant shifts in transaction values or volumes by individual customers. Sudden and unexplained increases in betting amounts or the frequency of transactions may indicate attempts

to circumvent monitoring. For example, a customer who typically wagers small amounts suddenly starts placing high-stakes bets should be closely examined.

6. *Carrying out transactions in rapid succession*

Monitor for transactions occurring in rapid succession within a short time frame. Frequent and rapid betting, especially when followed by cashouts, could be indicative of structuring or money laundering attempts. For instance, a customer making a series of quick bets and immediately cashing out should raise concerns.

7. *Inconsistencies in the customer's transactional pattern or behaviour*

Regularly review customer transaction histories for any inconsistencies or deviations from their typical behavior. If a customer suddenly alters their betting patterns, switches to different games, or changes their preferred payment methods without a reasonable explanation, it may signal illicit activity.

8. *Spikes in deposits or withdrawals*

Watch for sudden and unexplained spikes in deposits or withdrawals. Such spikes may be an attempt to quickly move large sums of money in or out of the gaming establishment. For example, if a customer who usually deposits $10,000 at a time suddenly deposits $300,000, this should trigger scrutiny.

9. *Structuring of transactions to evade suspicion*

Be cautious of customers who engage in structuring, which involves conducting transactions in amounts just below reporting thresholds to evade detection. Keep an eye out for repeated deposits or withdrawals that are just under the threshold for mandatory reporting, as this may indicate an intent to avoid scrutiny.

10. *Transactions involving individuals or entities subject to sanctions or named in adverse media*

Ensure that your transaction monitoring system is equipped to identify individuals or entities subject to sanctions or those named in adverse media reports. Transactions involving such individuals or entities should be closely monitored and, if necessary, reported to the relevant authorities.

11. *Incomplete, inadequate, or inconsistent supporting information and/or documentation*

Pay attention to transactions where the supporting information or documentation is incomplete, inadequate, or inconsistent. Proper documentation is crucial for verifying the legitimacy of transactions. For instance, if a customer provides incomplete or falsified identification when making a significant withdrawal, this should be flagged.

12. *Generic explanations or statements for transactions that are not in line with the customer's profile*

Exercise caution when customers provide generic or implausible explanations for their transactions that do not align with their known profile or behavior. Such explanations may indicate an attempt to conceal illicit activity. For example, if a customer claims to have won a large sum of money but has a history of consistent losses, this should be investigated further.

Regularly monitoring these red flags and promptly investigating any suspicious activities is essential to maintaining the integrity of your gaming establishment and ensuring compliance with AML/CFT/CFP regulations. Additionally, providing ongoing training to your staff on recognizing and reporting these red flags is crucial in building a robust AML/CFT/CFP compliance framework.

Automated transaction Monitoring

The importance and benefits of having an automated transaction monitoring system

A. Customization

Implementing customizable monitoring rules empowers gaming operators to adapt their surveillance to the specific risks and nuances of their business operations. This flexibility ensures that your monitoring system remains responsive to evolving threats and vulnerabilities. For example, if your gaming establishment introduces a new gaming product, you can customize monitoring rules to address the associated risks.

B. Velocity

Transaction velocity is a critical metric to monitor, as it helps detect sudden spikes or anomalies in transaction activity. An automated system can promptly flag and investigate unusual velocity patterns, providing real-time insights into potentially suspicious activities. If a customer typically makes small bets but suddenly starts placing significantly larger bets within a short timeframe, the automated system can generate an alert.

C. Data-capturing logs

Comprehensive and well-maintained data-capturing logs are indispensable for AML/CFT/CFP compliance. These logs serve as a digital trail of all transactions, facilitating audits, investigations, and regulatory reporting. For example, if regulatory authorities request transaction records for a specific customer, these logs ensure that you can provide the necessary information promptly.

D. Real-time monitoring and alerts

Real-time monitoring and alert functionality are pivotal components of an automated system. They enable immediate responses to potentially suspicious activities, allowing gaming operators to take swift corrective action and report incidents as required by law. If the system detects a transaction that exceeds a predefined threshold for a specific customer, it can generate a real-time alert, prompting immediate review and investigation.

Investigations and Escalation

- Clearly articulate when and how matters should be escalated to the designated Authority. Timely escalation is crucial to ensuring that suspicious activities are addressed promptly and comprehensively. For example, if your investigation reveals evidence of money laundering, you must promptly escalate the matter to the relevant authorities.

- Detail the record-keeping requirements after matters are escalated to the Designated Authority and provide guidance on maintaining thorough records for incidents that are not immediately reported. Proper documentation is essential for transparency and regulatory compliance. If you escalate a suspicious transaction to the authorities, it is crucial to maintain detailed records of the actions taken, communication with authorities, and any follow-up measures.

Commission's Expectations

Compliance: Licensees are expected to diligently comply with all relevant statutory and regulatory requirements concerning transaction monitoring. This includes the development and implementation of robust monitoring systems and controls. For example, if an audit reveals shortcomings in the transaction monitoring system, the Commission expects the licensee to promptly rectify these deficiencies.

Remediation: In cases where gaming machine operators identify deficiencies in their systems and controls, the Commission expects licensees to develop and execute remediation plans swiftly. These plans should rectify the identified shortcomings to strengthen

the effectiveness of transaction monitoring. If a gaming operator discovers weaknesses in its transaction monitoring system during an internal review, it must develop a remediation plan outlining specific steps and timelines for improvement.

The goal of this **REF: CIR-007-09-2023** is to:

- Ensure gaming operators understand their obligations related to assessing overall risk and implementing adequate transaction monitoring measures.
- Enhance staff knowledge and competencies, thereby improving the practical application of these measures.
- Prevent gaming lounges from being used for money laundering, terrorism financing, or proliferation of weapons of mass destruction.
- Promote full compliance with the Proceeds of Crime (Money Laundering Prevention) (Amendment) Regulations, 2019, and other relevant legislations.

The Commission will take enforcement action if a gaming operator is found to be in breach of any AML/CFT legislative provisions.

Please be guided accordingly.

Yours sincerely,

.....

Laurie Wiggan
Director, Compliance & Regulatory
BETTING, GAMING & LOTTERIES COMMISSION