اللجنة الوطنية لمواجهة غسل الأموال
ومكافحة تمويل الإرهاب وتمويل انتشار التسلح
NATIONAL ANTI-MONEY LAUNDERING AND COMBATTING THE FINANCING
OF TERRORISM AND PROLIFERATION FINANCING COMMITTEE
GENERAL SECRETARIAT الأمانة العامة

gcgra
الهيئة العامة لتنظيم الألعاب التجارية
General Commercial Gaming Regulatory Authority

Policy Paper

Commercial Gaming Policy

EXECUTIVE SUMMARY

Purpose: This policy paper outlines strategic recommendations for strengthening anti-money laundering and countering the financing of terrorism (AML/CFT) standards in the UAE's newly established commercial gaming sector. This paper discusses the key risk factors associated with the commercial gaming industry. It highlights the need to develop a tailored risk-based approach to AML/CFT in the context of this regulated sector in the UAE, providing an overview of the core areas that, if addressed successfully, can reinforce and support the strategic objectives of the regulatory body.

Key Issues: The paper identifies several key inherent money laundering and terrorist financing risks associated with gaming activities, including anonymous transactions, exploitation of player accounts, third-party payments, foreign jurisdiction transactions, the use of multiple and opaque payment methods, and potential employee complicity. For each of these risks, the paper outlines targeted mitigation strategies drawn from international best practices. These strategies should be considered for implementation following the completion of a comprehensive sectoral risk assessment to ensure that adopted measures are proportionate, risk-based, and effective for the UAE commercial gaming sector.

Main Recommendations: The paper recommends completing the sectoral ML/TF risk assessment as a foundational step. It also calls for enhanced coordination among regulatory and enforcement bodies, stricter due diligence and monitoring obligations for Gaming Operators, implementation of technology driven supervision tools, and the promotion of strong internal controls and training within gaming entities. These measures are intended to contribute to the sustainable growth of the UAE's gaming sector while safeguarding the integrity of the UAE's financial system.

Contents

1. Introduction

1.1 Purpose

This policy paper proposes a holistic regime by which the UAE can strengthen AML/CFT measures in its newly established commercial gaming industry. To protect the financial integrity of this sector, the General Commercial Gaming Regulatory Authority (GCGRA) was established to regulate commercial gaming in the UAE and implement robust regulatory frameworks that meet international standards.

This paper outlines the unique challenges and opportunities associated with introducing commercial gaming into the UAE with respect to AML/CFT and explores how to develop a comprehensive set of AML/CFT measures in accordance with Financial Action Task Force (FATF) recommendations. Establishing adequate AML/CFT measures from inception will enable the UAE to lay the foundation for its commercial gaming sector on the pillars of integrity and transparency.

1.2 Background

The General Commercial Gaming Regulatory Authority (GCGRA) was established by Federal Law by Decree and announced in 2023 as the sole federal body mandated to regulate, license, and supervise all commercial gaming activities and facilities in the UAE. Headquartered in Abu Dhabi, the GCGRA holds exclusive jurisdiction and any commercial gaming activities not explicitly authorized under its framework are deemed illegal and subject to enforcement action.

The GCGRA is responsible for regulating all forms of commercial gaming, including Land-Based Gaming Facilities, Internet Gaming, Sports Wagering, Lottery (hereafter collectively referred to as “Gaming Operators”), and other commercial gaming related services. Its authority encompasses licensing of Gaming Operators and gaming related vendors, setting technical and operational standards, conducting inspections, and enforcing compliance with applicable UAE laws and international norms.

Aligned with its foundational mission, the GCGRA’s regulatory strategy is built on four strategic pillars:

- World-Class Excellence: Creating a best-in-class regulatory framework through global benchmarking, professional development, and rigorous oversight.
- Safety and Responsibility: Safeguarding players and society through robust consumer protections, AML/CFT controls, and responsible gaming initiatives.

- Innovation: Enabling a responsive regulatory environment that supports technology adoption, market growth, and pioneering gaming models.
- Value for the UAE: Supporting the country's economic diversification goals by unlocking new sectors of growth, job creation, and foreign investment.

The GCGRA is not only a regulator but also a key enabler of national transformation. Its alignment with the UAE Vision 2030 is evident in its mandate to:

- Promote Economic Diversification: By attracting international investment and establishing a new commercial sector that supports local supply chains and SMEs.
- Develop Human Capital: Through education initiatives and a regulatory framework designed to promote innovation, which will facilitate the development of expertise in gaming operations, new technology development, AML/CFT compliance, responsible gaming, and operational integrity.
- Support Social Cohesion: By ensuring consumer protection, deterring illicit activity, and helping vulnerable populations affected by gaming-related harm.

2. Current State and International Best Practices

2.1 Existing Regulations in the Country

2.1.1 Legal Framework

The GCGRA regulatory framework is built on core objectives encompassing integrity, responsible conduct, economic development, and public protection. Its operational mandate includes, but is not limited to:

- Licensing and supervision of Gaming Operators, vendors, and employees;
- Being the supervisory authority of AML/CFT for the commercial gaming sector;
- Development and enforcement of regulatory and technical standards;
- Investigation and sanctioning of non-compliant or illegal activity;
- Coordination with national AML bodies and international regulators;
- Ongoing monitoring of commercial gaming operations, including Lottery, Internet Gaming, Sports Wagering, and Land Based Gaming Facilities;
- Ensuring all advertising is closely monitored and supervised by both the GCGRA and local government authorities; and
- Creating and implementing a Responsible Gaming Framework to empower and protect consumers against harmful behaviour.

Since its public launch in September 2023, the GCGRA has achieved critical milestones. Within a single year, the GCGRA transitioned from a start-up to a fully operational regulatory authority:

- Established a licensing system, including occupational licenses, gaming-related vendors, and various operator categories, while adhering to legal restrictions which limit operator licenses;
- Issued the UAE's first three c Gaming Operator's licenses, including the Land-Based Gaming Facilities License issued to Island 3 AMI FZ-LLC (i.e., Wynn Al Marjan in Ras Al Khaimah).
- Launched the UAE Lottery with real-time oversight and full regulatory supervision;
- The two long-standing airport lotteries have been allowed to continue their existing operations without further expansion and under the supervision of the GCGRA;
- Approved the first gaming-related vendor licenses, catalyzing the emergence of a gaming technology ecosystem;
- Blocked over 6,500 illegal gaming sites and disrupted 71% of identified illicit activity through a coordinated enforcement strategy;
- Established a robust governance structure and policies, Board-level oversight

committees, and robust financial controls aligned with federal standards; and

- Promulgated Executive Regulations governing every aspect of commercial gaming operations, and related consumer protection measures.

2.1.2 AML/CFT Provisions for Commercial Gaming

In line with the provisions of UAE's AML-CFT Law (Federal Decree Law No. (20) of 2018), a Ministerial Resolution issued by the Ministry of Finance of the UAE in 2024 added the following commercial Gaming Operators to the definition of Designated Non-Financial Businesses and Professions (DNFBPs):

- Internet Gaming Operators
- Land-Based Gaming Facilities Operators
- Sports Wagering Operators
- Lottery Operators

The Resolution also established GCGRA's powers in relation to AML-CFT Supervision.

In line with the above Resolution, GCGRA's Executive Regulations (ERs) mandate its licensed Gaming Operators to adhere to all UAE Federal Laws and Regulations applicable to AML/CFT, including but not limited to:

- Federal Law No. (7) of 2014 on Combatting Terrorism Offences.
- Federal Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organizations, as amended.
- Cabinet Decision No. (10) of 2019 Issuing the Implementing Regulation of Decree Law No. (20) of 2018, as amended.
- Cabinet Decision No. (74) of 2020 on the Lists of Terrorist Organizations and Entities and the Implementation of UN Security Council Resolutions.

In addition, and consistent with the National AML-CFT Regulatory Framework, the GCGRA may issue specific policies and guidance for its Licensees concerning the management of AML/CFT risks. The following table outlines the key elements of GCGRA's AML/CFT regulatory framework for Gaming Operators:

AML/CFT Requirements for Licensed Gaming Operator

Requirement Area	Requirement details
Governance & Oversight	An operator's Board must oversee AML compliance, policies, and internal controls.
Institutional Risk Assessment	Operators must assess ML/TF risks of their entity based on customers, products, geography, channels, and tech used.

Player Risk Assessment	Risk ratings must be assigned at onboarding, reviewed periodically, and when risk factors change.
Player Due Diligence (PDD)	Verify identity, assess relationships, monitor player's behaviour, apply thresholds (≥ AED 11,000 must go through PDD).
Enhanced Due Diligence (EDD)	Additional due diligence checks, including but not limited to verification of source of funds/wealth, senior management's approval for high-risk accounts, and enhanced monitoring of Politically Exposed Persons (PEPs) and high-risk players.
Record Keeping	Maintain records of customer due diligence, transactions, suspicious activity reporting (amongst other things), for 5 years after the last transaction or the customer relationship ends.
Money Laundering Reporting Officer (MLRO) Appointment	Operators must appoint an MLRO with suitable seniority, experience and independence.
Suspicious Activity Reporting (SAR)	Have in place adequate processes to report unusual or suspicious activity internally to the MLRO and externally to the FIU.
Sanctions Compliance	Establish and maintain systems and processes to comply with targeted financial sanctions obligations.
Technical Compliance	Operators should maintain an Information Security Management System (aligned with ISO27001) and undergo periodic Vulnerability Assessment and Penetration Testing (VAPT).

- Governance and Oversight: The board of directors of Gaming Operators are responsible for overseeing the compliance framework, including policies, procedures and activities, implemented to reduce money laundering risks. They are responsible for overseeing the Gaming Operator's AML/CFT risk management framework and ensure that AML policies, procedures, systems, and controls adequately satisfy regulatory requirements.
- Risk Assessment Requirements: Gaming Operators are required to conduct periodic risk assessments and implement adequate mitigant measures at institutional and player levels.
    - Institutional Risk Assessment: Gaming Operators need to identify/assess the risks of money laundering to which their business is exposed to, taking into consideration the types of customers it has (risk exposure), geographic areas of operation, the products and services offered, the distribution channels they

use, the transaction volumes, and the new technologies they are dealing with.

- Risk Assessment of Players: Gaming Operators must conduct risk assessments of each player and assign risk ratings according to the money laundering risks. Such assessments must be done at the time of account creation, periodically thereafter, and when there is a change in risk factors. There are multiple methods which operators may adopt to assess player risk, given their nature, size and complexity, including utilizing data driven dynamic risk rating models to enable close to real time risk assessments factoring in transactional behavior and other attributes.

- Player Due Diligence: The regulations lay out specific requirements for what is considered Player Due Diligence (PDD):
  - Independently and reliably verifying the identity of players
  - Establishing/assessing the relationship with players
  - Assessing player risk profiles
  - Real-time monitoring to ensure gaming activity is aligned with the operator's knowledge of the player.
  - Any individual or linked financial transactions (deposits and/or withdrawals of cash or cash equivalents) conducted by a player in connection with Commercial
  - Gaming that cumulatively exceeds 11,000 AED must be processed through a Player Account of which the due diligence requirements apply.
- Supplemental/Enhanced Due Diligence (required for politically exposed persons (PEPs) and high-risk players):
  - Collect additional identification information, including on the intended nature of the relationship
  - More frequent updates to the due diligence data
  - Source of funds and wealth designation
  - Tighter scrutiny of accounts and transactions
  - Prior approval of senior management in case of opening an account or transaction for high-risk player
  - Systems to identify and monitor PEPs
  - Relationships requiring senior management approval
  - Increased vigilance and monitoring around accounting and transaction activity.
- Record Keeping: Gaming Operators are required to maintain records for five years after the date of the last transaction, or the end of the player relationship, containing:

- Due diligence documentation
- Transaction records
- Suspicious activity reports internal and external
- Correspondence with the Financial Intelligence Unit
- Risk assessment documentation

- Money Laundering Reporting Officer (MLRO): Gaming Operators are required to appoint an MLRO with suitable seniority, experience and independence who must:
  - Regularly reside in the UAE
  - Have enough authority and access to information
  - Be responsible for the day-to-day management of AML compliance activities
  - Function as a point of contact for suspicious activity reports
  - Meet with regulatory authorities
  - Create and sustain training programs
  - Report on key risks, issues and trends to senior management on a semi-annual basis
- Report Suspicious Activity: Gaming Operators need to have systems in place to monitor and detect suspicious activity. There should be defined protocols for:
  - Reporting to the MLRO internally
  - Protection for people making notifications
  - Investigating the Reported Activities
  - Reporting externally to the UAE Financial Intelligence Unit
  - Record of decisions not to submit reports
- Sanctions Compliance: Gaming Operators must establish and maintain systems to ensure compliance with the obligations outlined in Cabinet Decision No. 74 of 2020. This includes:
  - Regular screening of players, transactions, and business relationships against relevant Sanctions and Terrorist Lists.
  - Upon identifying a confirmed match, immediate implementation of Targeted Financial Sanctions, which encompasses:
    - Freezing of assets without delay and without prior notice.
    - Suspension of related accounts.
    - Reporting such actions to the appropriate authorities within five working days.
  - Ensuring that all Key Persons and relevant employees receive appropriate

training at least once each calendar year, tailored to the operator's specific activities, with records maintained for a minimum of five years.

- Technical Compliance: As part of the overall GCGRA' supervisory framework, the technical compliance framework establishes a robust set of regulatory requirements designed to ensure that all licensed Gaming Operators in the UAE meet international technical standards, maintain the highest levels of data security, and operate with integrity. Consistent with the GCGRA's risk-based, outcomes-focused regulatory model, these standards are tailored to the specific operational realities and inherent risks that may occur in commercial gaming.

  The GCGRA's Technical Compliance team undertakes ongoing supervisory activities to evaluate and verify that licensees are fulfilling their technical, operational, and security obligations. These include, but are not limited to:

  - Information Security Oversight: Assessing the operator's implementation of an Information Security Management System (ISMS) to ensure alignment with international best practices (typically ISO/IEC 27001). Reviews focus on the protection of sensitive information, effective risk mitigation, and the preservation of data confidentiality, integrity, and availability.
  - Product Certification and Approval: Reviewing and approving gaming systems, platforms, and products in accordance with GCGRA's technical standards and executive regulations. All systems must be tested and certified by independent testing laboratories for the GCGRA to ensure fairness, integrity, and functional reliability.
  - Change Management and Security Reviews: Conducting regular assessments of each Gaming Operator's Change Management processes, ISMS audits, and technical safeguards. These reviews include Vulnerability Assessments and Penetration Testing (VAPT) conducted independently to proactively identify and address system weaknesses.
  - Ongoing Monitoring and Compliance Assurance: Monitoring compliance through structured reporting, incident reviews, and risk-based audits to ensure operators maintain a resilient technical environment capable of supporting AML/CFT controls and other regulatory obligations.

This integrated compliance model supports a secure, transparent, and accountable gaming ecosystem. By embedding technical standards within a broader risk-based regulatory and supervisory framework, the GCGRA ensures that licensees are not only compliant with international norms but are also equipped to address evolving cybersecurity threats and uphold the integrity of the UAE's commercial gaming sector.

2.2 International Standards and Best Practices

2.2.1 FATF Recommendations

Recommendation 22, Customer Due Diligence for Designated Non-Financial Businesses and Professions (DNFBPs): casinos/gaming Operators are required to apply customer due diligence (CDD) when conducting transactions equal to or exceeding USD/EUR 3,000; maintaining records; applying enhanced due diligence for politically exposed persons where they are considered to pose a higher risk; managing risks related to new technologies; and ensuring proper controls when relying on third parties for CDD. These measures must be applied proportionately to the risks associated with casino operations. Transaction refusal should be required when CDD cannot be completed. GCGRA ERs contain provisions aligned with this recommendation. Furthermore, all online gaming activities must be conducted via a player account, which is subject to CDD requirements.

Recommendation 23 introduces additional measures for DNFBPs, including the imposition of suspicious transaction reporting (STR) requirements on casinos/Gaming Operators, enforcement of internal controls, policies, and procedures, the appointment of a compliance officer, and the establishment of a separate audit function. It also recognizes the high employee learning curve associated with these requirements and mandates enhanced due diligence for business relationships involving nationals of high-risk countries. Furthermore, it prohibits tipping-off in relation to suspicious transaction reports. As mentioned in section 2.1.2 of this paper, the GCGRA's ERs include provisions in relation to transaction monitoring and reporting of suspicious activities and transactions.

Recommendation 28, regulation and supervision of DNFBPs: DNFBPs, including casinos/Gaming Operators, are subject to the same level of regulation and supervision as other reporting entities. A comprehensive regulatory and supervisory framework must be in place, with adequate powers to ensure the effective implementation of AML/CFT measures. At a minimum, this includes a licensing requirement for casinos. Competent authorities are required to take appropriate legal or regulatory actions to prevent criminals or their associates from becoming beneficial owners with significant or controlling interests, holding management positions, or operating casinos. Additionally, casinos must be subject to ongoing monitoring to ensure compliance with AML/CFT obligations. As stated below in section 2.2.2 of this paper, these requirements have been implemented in the UAE.

2.2.2 Regulatory Models: International Approaches

The GCGRA's regulatory framework is based on extensive benchmarking reviews including both gaming regulators in other more mature jurisdictions and other regulators in the UAE, to ensure that it is aligned to best practices and standards, whilst being fit for the local needs and context, and fostering technology innovation and sustainable growth. Many jurisdictions with mature commercial gaming sectors have built detailed and well-structured regulatory frameworks for AML/CFT, which can serve as good reference points for the UAE. Examples include:

- The Singapore's Gambling Regulatory Authority (GRA), responsible to regulate and supervise gambling entities within Singapore.,. Key features include, but are not limited to:
  - Dynamic licensing requirements with comprehensive fit and proper assessments
  - Casino operators have mandatory internal control standards
  - Broad transaction reporting obligations
  - Compliance audits/inspections periodically
  - There are severe penalties for non-compliance
- The Nevada Gaming Control Board (USA) has developed a risk-based regulatory model with a focus on:
  - Detailed and comprehensive pre-licensing investigations
  - Mandatory compliance programs for casinos
  - Routine field audits and inspections
  - Coordination with FinCEN (Financial Crimes Enforcement Network, an agency of the United States Department of the Treasury)
  - Outreach and education
- The UK Gambling Commission has mainly a principle-based approach to AML/CFT regulation, which includes, but is not limited to:
  - Operator-level and national-level risk assessments
  - Regulatory requirements must also be outcome-focused
  - Increased focus on the accountability of senior management
  - Periodic thematic reviews of industry compliance
  - Financial penalties for systemic failures.

2.2.3 GCGRA Risk Based Regulatory Oversight Across the Licensing Lifecyle

Consistent with international best practices and the GCGRA's foundational regulatory philosophy, the GCGRA has implemented a comprehensive risk-based approach to regulating the UAE's commercial gaming sector. This model allocates regulatory attention and resources proportionately, focusing greatest scrutiny on the highest-risk activities, licensees, and transactions. It integrates licensing, supervision, enforcement, and analytics into a coherent lifecycle framework designed to promote integrity, transparency, and public trust. The GCGRA's approach to each element of the lifecycle is as follows:

- Licensing and Suitability Determinations: GCGRA has established rigorous licensing requirements for all Gaming Operators, Gaming Related Vendors, Key Persons, and Gaming Employees to ensure that (amongst other things) licensees remain free from criminal infiltration. The GCGRA views licensing as more than a one-time gateway but rather as the entry point to a continuous process of oversight. Each applicant undergoes thorough due diligence, including comprehensive suitability investigations, financial assessments, and background checks, with a focus on verifying fitness and alignment with GCGRA standards for good conduct. Importantly, suitability is subject to ongoing review, and the GCGRA reserves the right to take action whenever a licensee's risk profile changes.
- Supervision and Ongoing Monitoring: Before any licensee may commence operations, GCGRA conducts a comprehensive review of its Internal Controls, including AML/CF policies, cybersecurity protocols, and compliance frameworks, to assess operational readiness. Post-launch, Gaming Operators are subject to risk-calibrated supervisory activities that may include periodic inspections, data reviews, thematic audits, and third- party independent assessments mandated by the GCGRA.

  Regulatory engagement is not simply a matter of compliance verification - it is an opportunity to clarify expectations, understand operational realities, and promote continuous improvement. The frequency and intensity of supervisory activity are determined by a combination of factors, including business scale, transaction volume, technology footprint, and prior compliance history.
- Enforcement and Market Integrity: GCGRA's enforcement program is intended to be proactive, intelligence-led, and firmly grounded in due process. It is designed not only to penalize violations, but to deter misconduct, disrupt illegal activities, and reinforce the credibility of the legal market. Key enforcement tools will include:
  - A centralized case management system and investigative protocols
  - Test purchasing operations and digital surveillance tools

- Strategic partnerships with domestic law enforcement and international regulators
- A clear, graduated penalties regime to ensure consistency and fairness
- Public disclosure of enforcement actions to enhance transparency and deterrence.

As of December 2024, GCGRA enforcement actions have resulted in approximately 6,000 illegal websites being blocked and 11 high-volume offshore operators being served with formal cease-and-desist letters. These actions have contributed to a substantial decline in access to and participation in illegal gaming by UAE residents. The continued Implementation of GCGRA Strategy on combating illegal operators will remain a key priority for the GCGRA, alongside to supervising and enforcing compliance of the legal commercial gaming sector.

UAE's Enforcement Statistics

Metric	Value (as of Dec 2024)
Illegal websites blocked	6,000+
High-volume illegal operators shut	11

- Monitoring, Data Integration and Risk Analytics: At the heart of GCGRA's data-driven regulatory framework is the ongoing development of a Unified Player Database (UPDB), a centralized, secure platform that will aggregate player account information, transactional data, and behavioural analytics across all licensees. The UPDB will support cutting edge supervisory oversight, automated risk detection, and cross-operator consistency in enforcement and responsible gaming protections.

  Designed in accordance with international data privacy and cybersecurity standards, the UPDB will allow the GCGRA to:

  - Detect unusual or high-risk activity patterns
  - Monitor compliance with AML/CFT obligations
  - Support evidence-based policy adjustments
  - Advance the Authority's public interest goals, particularly in player protection and integrity assurance.

This integrated, outcomes-focused model reflects the GCGRA's core belief that effective regulation is grounded in risk mitigation, public protection, support for responsible innovation, and the promotion of a fair, secure, and sustainable commercial gaming market.

3. Key ML/TF Risks and mitigation approaches

Expanding regulated commercial gaming in the UAE cannot be done without assessing the underlying ML/TF risks of the industry and ensuring the necessary mitigation strategies are in place. These risks are especially pronounced given the UAE's status as a global financial center and the relative infancy of commercial gaming in the UAE.

Some of the key risks that the commercial gaming industry faces are outlined below, along with potential mitigation measures based on international best practices. To fully understand the ML/TF risks and inform appropriate risk-based measures to be adopted for the commercial gaming industry, the GCGRA will conduct an ML/TF Sectoral Risk Assessment.

The approaches and recommendations outlined in this paper should be considered once the sectoral risk assessment is finalized, to implement detailed risk mitigation strategies as part of the regulatory regime.

Summary of Key risks

Risk Area	Description	International Best Practices
Anonymous Transactions	Transactions without verified customer identity	Threshold for ID verification Biometric verification Limits for anonymous play
Exploitation of Player Accounts	Using player accounts for illicit fund movement	Strong KYC Ongoing monitoring Account controls
Third Party Payments	Payments or withdrawals by non-players	Regulated party transactions Senior approval for high-risk cases
Foreign Transactions	Cross-border transactions	EDD on foreign players (from high-risk jurisdictions) Cooperation with foreign FIUs
Multiple Payment Methods	Use of diverse payment methods to obscure fund source	Monitor payment methods Closed loop payments Risk scoring for new methods Implement closed loop
Casino/Betting Value Instruments	Use of chips/vouchers to launder money	Track chip/vouchers movements Restrict transfers Set buy-in thresholds
VIP & High-Value Players	Players who wager in high volumes or deposit large	EDD which includes source of funds/wealth validation

	amounts	
Employee Complicity	Staff aiding or ignoring suspicious activity	Whistleblower protections Staff due diligence Independent audits
Cash Transactions	Cash enables anonymous laundering	CTR requirements Limit cash deposits Monitor structuring patterns

3.1 Anonymous Transactions

Anonymous transactions in commercial gaming refer to transactions where customer identification is not undertaken, anonymous payment methods are used, or cases where identity verification is avoided.

The inherent danger is that anonymous transactions allow criminals to:

- Introduce funds to a Gaming Operator (for example multiple buy ins at a table using cash at amounts under ID thresholds).
- Layer those funds by placing bets (for example using chips to place bets at a table game); and
- Integrate those funds as legitimate winnings (for example combining all those funds as legitimate winnings).

There are numerous measures that have been adopted in other jurisdictions to ensure that the risk of anonymous transactions in the commercial gaming industry is mitigated and managed. Some of the best practices include:

- Account based play: Restrict the ability to play anonymously, by integrating the use of account linked to a person's identity and recording all transactions.
- Transaction thresholds: Establish transaction thresholds, where customer identification and verification could be required when the cash component is exceeded.

3.2 Exploitation of Player Accounts

Player accounts can be utilized in both online and land-based commercial gaming. These accounts can be appealing for criminals to park and store illicit funds or receive payments from third parties relating to predicate offending. The ML/TF typologies and/or techniques to exploit player accounts can include account takeovers, third parties being used as mules and smurfing. It is integral that Gaming Operators have in place appropriate risk-based

monitoring measures to detect potential instances.

To minimize the risks of exploitation of player accounts the following can be done:

- Customer Due diligence: Apply strong KYC/CDD processes, with enhanced due diligence for high-risk accounts.
- Ongoing Monitoring: Monitor account activity to identify unusual or suspicious behavior, for example significant changes in players betting patterns, significant deposits and withdrawal with no (or minimal) play, dormant accounts with significant balances.
- Source of Funds Verification: Verify the sources of large transactions by requesting supporting documentation.
- Account Security and Authentication: Implement protections such as multi-factor authentication and device tracking to help stop unauthorized access and account takeovers.
- Implement processes to manage data breaches (including notification to players) and consideration of potential ML/FT risks which may warrant reporting to the Financial Intelligence Unit.

3.3 Third Party Payments

Third-party payments/withdrawals occur when a player uses money received from another person or entity to gamble or when winnings or excess funds are paid out to someone other than the one who gambled. This poses considerable money laundering risks as it conceals the actual source and recipient of funds, enabling criminals to distance themselves from tainted proceeds.

The following are the best practices from other jurisdictions to mitigate and manage third-party payments:

- Payment limitations or prohibition: Set limitations and acceptance criteria on third party payments or prohibit such transactions.
- Verification: Document and verify the identity of both the third party and the player.
- EDD thresholds: Mandate EDD for third party payments that exceed a certain threshold.
- Senior management approval: For the high-risk third-party payments or transactions, it could be required to seek approval from the senior management before treatment.
- Monitoring or limitation for PEPs: Monitor or prohibit third party payment transactions involving PEPs.

3.4 Foreign Jurisdiction Transactions

Foreign jurisdiction transactions involve the movement of funds across international borders for gambling purposes. Such payments may include international wire transfers, foreign payment methods, or transactions through foreign financial institutions. The inherent risk is that such transactions could take advantage of regulatory discrepancies between jurisdictions and use them to circumvent AML/CFT controls, making it more difficult for authorities to track the movement of funds. Special AML/CFT considerations must be given to foreign players, especially where they are based in a high-risk jurisdiction, as it is often quite challenging to verify their identity, ascertain their respective sources of wealth, and assess their risk profiles.

To prevent financial crimes in relations foreign jurisdiction transactions, the following are some of the measures that could be adopted:

- EDD: Conduct enhanced due diligence on customers and transactions from high-risk countries.
- Monitoring PEP: Monitor foreign PEPs and their family members or close associates.
- Form of payments: Set clear guidelines regarding acceptable forms of foreign payments (e.g., certain types of payments may be restricted or prohibited).
- CTRs: Report any cash transactions with foreign currency that meet or exceed certain thresholds by submitting currency transaction reports.
- Funds verification: The source of wealth and source of funds for high-value foreign players must be verified.
- International Cooperation: cooperate with foreign regulators and FIUs regarding foreign transactions.

3.5 Multiple Payment Methods

Multiple payment methods risk refers to customers who use different payment instruments (cash, credit cards, wire transfers, cryptos, etc.) for gambling. The criminal risk is that individuals can layer transactions across different payment types to circumvent detection thresholds, transaction monitoring complexity, and obfuscate funds' traceability.

For better transparency and minimizing inherent risks, here are the best practices to consider regarding customers' payment methods:

- Integrated Payment Tracking: Implement tracking systems that provide more detailed analysis of all payments made by a customer. Certain methods may be prohibited for high-risk customers.

- Closed Loop: having in place measures to ensure withdrawals are via the same method as deposits into a player account.
- Assessment of New Payment Methods: New payment methods subject to risk assessment prior to implementation.
- Player Risk Assessment: Trigger review of player risk assessment where a customer has multiple payment methods.
- Monitoring and Detection Systems: Monitoring transactions across different payment methods to identify potential ML/TF typologies and techniques, for example U turn transactions.
- Acceptable Payment Combinations: It is crucial to establish internal rules that define which payment solutions can be used, decide whether all payment methods are used or only the ones approved.

3.6 Casino and Betting Value Instruments

Casino and Betting Value Instruments are value instruments which facilitate commercial gaming by players and store monetary value. There is a risk of funds that are exchanged to instruments pass through the gaming ecosystem with minimal gaming activity before being redeemed. Such examples may include purchasing chips with little play before cash-out, transferring them between players (e.g. chip sharing), and converting funds between forms of casino value (e.g., chips to vouchers to cash). The inherent risk is that those transactions can be used to mask the origin of funds by simulating legitimate gambling activity to legitimize the funds as gambling winnings.

To mitigate and manage the ML/TF risks of casino and betting value instruments, some of the best practices in other jurisdictions are:

- Preventative and Detective Measures: Gaming Operators having in place risk-based processes and controls to prevent and detect potential instances of exploitation (such as chip sharing/walking and early cash out). For example, verifying that there has been gaming activity for larger redemptions of value instruments and internal suspicious activity reporting when identified by employees.
- Define what types of sharing are acceptable (for example between family members).
- Due Diligence on Cash-for-Chip Transactions: Set thresholds for CDD on cash used to purchase value instruments.

3.7 VIPs and High-Value Players

VIP and high value players refer to customers that turnover a significant amount of funds in

gambling. Such players pose an increased ML/TF risk as their spending may increase the risk that their source of funds and/or wealth derives from illegitimate means.

To mitigate the risks, some of the recommendations for Gaming Operators based on international standards may include the following:

- Ongoing Monitoring and EDD: Conduct ongoing monitoring and apply enhanced due diligence for all high value customers.
- Verification of Source of Wealth and Funds: Confirm the source of wealth and funds for VIP customers and high-value players.
- Senior Management Oversight: Senior management pre-approval could be required for high value customers players.
- Specialized Staff Training: Specific training for staff managing VIP relationships.

3.8 Employee complicity

Employee complicitly can enable criminal organizations to launder proceeds through the commercial gaming industry. This risk level includes gaming employees who knowingly assist in money laundering (corrupt workers) or do not notice or report suspicious activities because they are not adequately trained. The inherent risk is that staff are the front-line defense against money laundering, and staff corruption or lack of competence can defeat even the best AML/CFT systems and controls. Therefore, it is integral that Gaming Operators hire appropriately suitable staff and have in place adequate training.

These are among the best ways that casinos can minimize internal collusion and protect the integrity of their operations:

- Comprehensive Employee Training: Conduct regular AML/CFT training for all applicable personnel (frontline staff, compliance staff, management). Training can include the red flags, reporting duties and the ML/FT risks the entity faces (including internal collusion).
- Pre-Employment and Ongoing Screening: Screen employees (for example criminal checks, PEP/targeted financial sanctions 'checks) prior to employment as well as on an ongoing basis.
- Strong Internal Controls and Segregation of Duties: Develop internal systems to prevent any one employee from having full control over high-risk transactions to minimize internal abuses.
- Whistleblowing Mechanisms: Create secure and confidential avenues for employees to report suspicions of corruption or collusion without fear of retaliation. Promote an environment which encourages ethical behaviour and transparency.

- Monitoring: Where relevant, monitor internal transactions and system access by employees, to detect indications of misconduct or suspicious activity.
- Independent Audits and Oversight: Ongoing independent audits of AML/CFT processes with a focus on staff complicity risks. Audits can also help identify weaknesses in controls or gaps in training.

3.9 Cash Transactions

Cash transactions use physical currency in gambling (i.e., buying chips, cashing out chips, and making deposits to gaming accounts). Using cash to buy casino or betting value instruments enables criminals to claim potential legitimate means of their funds. The inherent risk is that cash is anonymous and difficult to track, making it the currency of choice for criminals trying to launder the proceeds of their nefarious acts through casinos and into the financial system. It is therefore integral that a risk-based approach is undertaken by the commercial gaming industry and ensure that appropriate sources of funds checks are completed at a threshold dependent on the risk-based approach adopted by operators.

The following practices could be of interest as a means mitigating the risks that come from cash transactions:

- CTRs Threshold: Require Currency Transaction Reports (CTRs) for cash transactions and suspicious activity report for transactions over certain thresholds.
- EDD: Due diligence checks, which apply to all cash deposits equal to or greater than certain thresholds.
- Verification of Source of Funds: Verify that such funds are from legitimate sources for large cash transactions.
- Monitoring of Transaction Patterns: Implement monitoring systems to detect unusual or suspicious cash transaction patterns that could indicate structuring or other illicit activities.
- Ongoing Risk Assessments: Conduct regular assessments of customers who predominantly use cash, with a focus on identifying those who may pose heightened money laundering or terrorism financing risks.

4. Recommendations

4.1 Recommended Actions

The analysis of the UAE's current regulatory framework, including the detailed AML/CFT measures included in the GCGRA Executive Regulations, as well as the key inherent sectoral risks discussed above, leads to the following recommendations to facilitate effective implementation and ongoing development of AML/CFT activities within the UAE's commercial gaming sector:

1. The GCGRA regulations make direct references to the wider UAE AML/CFT framework. However, the coordination mechanism between the GCGRA, the Financial Intelligence Unit, and other regulators still needs to be developed further to ensure effective information sharing and coordinated oversight.
2. The GCGRA to utilize the findings of sectoral risk assessment and this paper to:
    a. Inform appropriate combatting measures to mitigate potential vulnerabilities.
    b. Devise regulatory practices such as issuance of regulatory guidelines to address priority areas and areas of concern such as:
        i. Governance of AML/CFT framework for licensed commercial Gaming Operators.
        ii. Customer Due Diligence (CDD) which will include Enhanced Due Diligence (EDD); and
        iii. Transaction Monitoring and Reporting.
3. Periodic reviews of the sectoral risk assessment and other risk-based techniques to identify emerging and evolving threats and vulnerabilities to the commercial gaming sector and achievement of a continuous feedback loop.

GSNAMLCFTPC | الأمانــة العامــة