

Overseas Gaming Management N.V.

AML/CFT Procedures

Version: 2.0

Date: 17th February 2025

Internal Use Only

Classification - Confidential

Version History:

Author	Date	Description	Version	Approval
A.Cacciattolo	4 th January 2025	Creation	1.0	Compliance Officer
A.Cacciattolo	17 th February 2025	Updated in Line with GCB Guidelines issued on January 2025	2.0	Compliance Officer

CONFIDENTIALITY STATEMENT

This is a confidential document between Overseas Gaming Management Limited (the 'Company') and the GCB (the 'Authority'). It contains confidential and/or proprietary information that may not be disclosed or discussed with anyone outside the aforementioned organisations without the written approval of the Company and the Authority.

Table of Contents

1	Introduction	5
1.1.	What is Money Laundering/CFT?.....	5
2	Responsibilities.....	6
3	Policy and Procedures	7
3.1	Eligibility	7
3.2	Account Activation	7
3.3	Know Your Customer (KYC) Procedures.....	7
3.4	Risk Levels	8
3.5	Risk Based Verification	9
3.6	Medium and High Level Risk Customer Information	10
4	Anti-Money Laundering (AML) Procedures.....	10
4.1	Training	11
4.2	Risk Calculation	12
4.3	PEPs – Politically Exposed Persons.....	13
4.4	Risk Monitoring	14
4.5	Monitoring of Transaction – Customer Risk	14
4.6	Business Relation Obligations	15
4.7	Reporting of Transactions	17
4.1.1	Identification of Unusual Transactions	18
4.1.2	Reporting of Unusual Transactions.....	19
4.1.3	Documentation of Unusual Transactions	19
4.8	Record Keeping	19
5	Employee Screening and Ongoing Training Program	20
5.1	New Employees.....	20
5.2	Casino Team	21
5.3	Audit Team.....	21
5.4	AML Compliance Team	21
5.5	Senior Management.....	21
5.6	Training Program.....	21
6	Payout Management	22
5.1	Process for Deposits.....	22
5.2	Process for Withdrawals	23

5.3 Acceptance and Funds Handling.....	24
7 Platform Capabilities.....	24

1 Introduction

This document outlines the procedures for player settlement, methods for verifying player identities, and mechanisms for monitoring transactions to prevent fraud. It provides a clear framework to ensure the integrity of financial transactions within the gaming environment.

Effective Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) policies are critical for several reasons. First, they safeguard the integrity of financial transactions in the gaming industry by detecting and preventing illicit activities such as money laundering and terrorist financing.

Adhering to AML/CFT regulations also ensures compliance with legal and regulatory standards set by financial and gaming authorities. Non-compliance can result in significant penalties, including fines, legal action, and damage to the operator's reputation.

Additionally, robust AML/CFT policies build consumer confidence by reflecting a commitment to ethical practices and responsible gaming. Players are more likely to trust platforms that prioritize transparency, security, and regulatory compliance.

Furthermore, effective AML/CFT measures help to mitigate operational risks tied to financial crimes. Through stringent procedures for identity verification, transaction monitoring, and suspicious activity reporting, gaming operators can reduce the risk of regulatory breaches and financial losses.

In summary, comprehensive AML/CFT policies are essential for maintaining the integrity of financial transactions, ensuring regulatory compliance, strengthening consumer trust, and mitigating operational risks within the gaming industry.

1.1. What is Money Laundering/CFT?

Money laundering (ML) is the process of disguising illegally obtained funds to make them appear legitimate, often undermining financial integrity and facilitating further criminal activity. It occurs in three stages:

1. Placement - where illicit funds enter the financial system through casinos and other cash-intensive businesses;
2. Layering - where transactions such as fund transfers, currency exchanges, and structured deposits obscure the source of funds; and
3. Integration - where laundered money is reintroduced into the economy through investments in assets or businesses. While commonly linked to drug trafficking, ML also stems from crimes like human trafficking, fraud, corruption, and tax evasion.

Terrorist Financing (TF) involves providing financial support to terrorist activities, individuals, or organizations. Unlike money laundering, which deals with illicit funds, TF can involve legally obtained money that is channelled toward illegal objectives. Terrorists use various financial methods, such as cash smuggling, structuring transactions, wire transfers, and prepaid cards, to conceal the destination of funds rather than their source.

Proliferation Financing (PF) refers to funding the development, acquisition, or distribution of nuclear, chemical, or biological weapons and related materials. This poses a significant threat to global security and is subject to strict international controls.

Targeted Financial Sanctions (TFS) require financial institutions to freeze the assets of individuals and entities designated under UN Security Council resolutions and EU sanctions. In Curaçao, compliance is mandatory, and casinos must ensure that no funds or assets are made available to sanctioned parties. Casinos must regularly update their AML/CFT policies based on changes to sanction regulations and report any frozen funds to the Financial Intelligence Unit (FIU).

We at Overseas Gaming are committed to implementing stringent Anti-Money Laundering (AML) measures in line with Curacao's regulatory requirements to prevent and detect illicit financial activities.

2 Responsibilities

The Compliance Officer holds the responsibility of overseeing all transactions and verifying the identities of registered players. Additionally, they are tasked with defining criteria to promptly identify any suspicious activities and devising protocols to address these issues while mitigating risks to the lowest possible level.

3 Policy and Procedures

3.1 Eligibility

To access Overseas Gaming Management's gaming offerings, players are required to create an account through our brand. Only registered users are permitted to place wagers on the available games. Upon completing the registration process and agreeing to the terms and conditions along with the privacy policy, players can proceed to make deposits and commence playing.

During registration, players are prompted to input the following details for verification/identification purposes:

- First and last name.
- Password (entered twice for confirmation which should be complex as defined in the information security policy).
- A valid email address.
- Date of birth.
- Place and country of residence.
- Mobile Number (with the prefix of the country of residence selected).

Successful registration necessitates players to be at least 18 years old, with only one player account allowed per individual. However, if you registering from Estonia the player must be at least 21 years old in line with the country's regulations. The system automatically rejects registrations from underage individuals. Additionally, residents of restricted countries are barred from registering due to stringent anti-gambling regulations in those regions.

Furthermore, a background check is conducted to identify any players who may be categorized as Politically Exposed Persons (PEPs). In such instances, the Risk Manager evaluates whether to accept the registration or not based on specific criteria.

3.2 Account Activation

Prior to the player's initial login, an email containing an activation link is mailed to the address provided during registration. This email does not include any sensitive information such as the player's username. Upon clicking the activation link, the player gains access to their account and can proceed to make a deposit. If such an account has not been activated deposits are not permitted.

3.3 Know Your Customer (KYC) Procedures

Verifying player identities is a top priority for the Company. Therefore, players must confirm their identity when depositing or withdrawing certain amounts. Verification documents can be submitted through the customer support email listed on the website or uploaded directly within the player's account. Acceptable documents include scanned copies of ID cards,

passports, driver's licenses, recent utility bills showing the player's address, and, if needed, scans of credit cards or bank statements.

It is a must to implement Customer Due Diligence (CDD) measures in the following cases:

- When a player conducts financial transactions amounting to NAf. 4,000 (equivalent to €2,0000 or more).
- When processing occasional transactions exceeding the equivalent of NAf. 4,000 (equivalent to €2,000).
- If there are indications of potential money laundering or terrorist financing.
- If doubts arise regarding the accuracy or completeness of previously obtained customer identification

Until the verification process is successfully completed, the player will not be permitted to withdraw any funds. It is of utmost importance that the player provide the documentation requested within a reasonable timeframe (i.e. 30 days) or else the account might be deactivated by the Company.

Withdrawals are restricted to the same account originally used for deposits. If this option is unavailable, players may withdraw using an authorized method previously used or via bank transfer. For bank transfers, staff processing the payment must verify that the designated account or payment method is registered in the player's name. Cash withdrawals are not permitted under any circumstances.

Additionally, a risk assessment is conducted to categorize players based on their risk level. High-risk players undergo an enhanced due diligence process, requiring them to provide evidence of ownership for all payment methods used, as well as proof of the source of funds.

3.4 Risk Levels

Upon registration, each player is assigned a risk score within our system, categorized as 1 (Low), 2 (Medium), or 3 (High):

- **Low Risk (1):** Players classified as Low Risk gain immediate access to the site once Know Your Customer (KYC) procedures are completed. An automated system continuously monitors their behaviour to detect any unusual activity, such as large increases in deposits or wagers, and flags significant deviations from their usual activity patterns.
- **Medium Risk (2):** Players in this category are subject to the same monitoring as Low Risk players and are additionally placed on a risk watch list, which management reviews weekly. Enhanced due diligence may allow for reclassification to Level 1 (Low Risk), while certain behaviours may warrant an upgrade to Level 3 (High Risk).

Withdrawals for Medium Risk players are restricted, requiring senior management approval before processing.

- **High Risk (3):** Players identified as High Risk are prohibited from engaging in any activities on the website until enhanced due diligence procedures are completed. If a player is upgraded to Level 3 from a lower level after initiating a withdrawal request, the withdrawal will be suspended until enhanced due diligence has been fully conducted.

Players flagged for enhanced due diligence are notified during registration. If their risk status changes post-registration, withdrawal requests will be blocked, and they will be requested to provide additional documentation. In cases where concerns persist regarding age or identity, users may be prompted to upload a picture of themselves holding their identification. Only senior personnel can amend the player risk rating.

3.5 Risk Based Verification

The level of identification and verification required is determined based on the assessed risk:

- **Low Risk:** Verification at this level involves collecting essential personal details, including the player's First Name, Last Name, Place and Country of Residence, and Date of Birth. These details are then validated to confirm the player's identity.
- **Medium Risk:** In addition to the basic personal information required for Low Risk players, Medium Risk verification requires providing a Residential Address, Date and Place of Birth, and Nationality. These details must be authenticated with identity documents that include a photograph.
- **High Risk:** Similar to Medium Risk verification, High Risk verification requires all personal information specified above (Residential Address, Date and Place of Birth, and Nationality) along with photographic identification. Additional validation procedures may apply based on the specific risk factors associated with the player.

Verification procedures may utilize documentary sources. In instances where these sources do not confirm the customer's residential address, the customer will be requested to furnish documentation dated within the last six months. Such documents may include recent financial statements, utility bills, official conduct certificates, or government-issued documents.

Overseas Gaming Management may also leverage electronic sources such as E-ID, Bank-ID, or electronic commercial databases for verification purposes. Verification procedures are routinely scrutinized through daily checks, including IP checks and geolocation data. In cases where verification sources lack references to the customer's residential address, additional

documentation may be required, or the Company may seek corroborative evidence such as IP addresses or device location information.

If the Company encounters difficulties in conducting comprehensive verification, it will resort to additional measures, including Enhanced Due Diligence (EDD), to ensure thorough verification.

3.6 Medium and High Level Risk Customer Information

In the remote gaming industry, opening an account is essential. To enhance security, the Company has implemented a customer risk profiling system. This system utilizes statistical data from official economic indicators to create behavioural models, which serve as benchmarks for evaluating customer activity. For non-high-risk customers, direct collection of source of wealth information is not required. However, once the Customer Due Diligence (CDD) threshold is reached, source of wealth acquisition proceeds as follows:

- **Medium Risk:** The Company gathers statistical data on median net income by country, allowing for insights into expected sources of wealth. Therefore, Source of Wealth (SoW) declarations are not requested for this category, as existing statistical models provide adequate insight. Where declarations are made, individuals should identify the origin of their wealth—such as employment or business activities. The declared sources must be consistent with the individual’s activity throughout the business relationship.
- **High Risk:** For high-risk customers, comprehensive source of wealth information and supporting documentation are required. Additionally, source of funds may be requested if there are significant deviations from the customer’s expected profile. Information on the anticipated level and nature of these funds—including their expected value and frequency—may also be requested as necessary.

The Company does not rely solely on declarations for verification; supporting evidence is required. For instance, if an individual’s wealth is reportedly from employment, the Company may request supporting documents such as bank statements to verify this claim.

4 Anti-Money Laundering (AML) Procedures

Payments between players and Overseas Gaming Management are exclusively facilitated through provided methods, subject to change at the Company's discretion. Inter-player fund transfers are strictly prohibited.

To ensure compliance with anti-money laundering (AML) regulations, all transactions undergo meticulous monitoring to detect any potential money laundering activities. If the

Company gathers sufficient evidence indicating a player's involvement in such illicit activities, they will promptly report the individual to the FIU Curacao. Any transactions deemed suspicious will be reported to the Money Laundering Reporting Officer (MLRO), who will then notify the case of the FIU if necessary, utilizing a Suspicious Transaction Report (STR) form.

The appointed individual overseeing the AML function will be entrusted with the responsibility of overseeing and implementing robust anti-money laundering (AML) and counter-terrorist financing (CTF) measures in accordance with regulatory guidelines. In the event of the MLRO's absence, whether due to vacation leave or other reasons, the duties will be temporarily assumed by the company's director until the MLRO resumes his/her responsibilities.

Comprehensive procedures, including anti-money laundering protocols, are outlined in the Terms and Conditions. Any revisions to these terms are communicated in writing to all players before they come into effect.

4.1 Training

In collaboration with the Money Laundering Reporting Officer (MLRO) and any relevant third parties, comprehensive training presentations on our Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) policies and procedures will be provided to all new employees and close collaborators.

New employees are mandated to undergo these training sessions within the initial month of their employment and are required to successfully complete a quiz/test at the conclusion of the training. Upon completion, proof of participation will be endorsed by their respective reporting manager and securely stored in their employee file.

Additionally, all staff members will review the training material in preparation for their annual performance evaluations. During these reviews, any significant updates or modifications to the policies and procedures will be highlighted for awareness.

The training sessions are designed to ensure that employees are well-informed about:

- The statutory requirements concerning money laundering and terrorist financing.
- Their individual responsibilities under the applicable regulations.
- Internal reporting protocols that may be relevant.
- The Company's policies and procedures aimed at preventing money laundering and terrorist financing.
- Identification, verification, record-keeping, and other protocols to prevent money laundering and terrorist financing.
- The identification and handling of suspicious transactions.

- Their personal liability in cases of failure to report pertinent information or suspicions, as per regulatory requirements and internal procedures.
- Ongoing developments in the field, including updates on current methodologies, techniques, and trends related to money laundering and terrorist financing.

4.2 Risk Calculation

Overseas Gaming Management implements a risk-based approach concerning Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT), focusing on various risk factors:

- **Countries Monitored by the Financial Action Task Force (FATF):** Countries identified by the FATF as having insufficient AML/CFT controls are subject to strict monitoring. Players attempting to register from these countries are either blocked from registration or automatically assigned a higher-risk classification.
- **High-Risk Countries Selected by the Licensee:** Based on the licensee's internal risk assessment, certain countries identified as posing increased AML/CFT risks lead to automatic placement of players from these regions into the higher-risk category.
- **Significant Transactions Over a Rolling 30-Day Period:** Transactions exceeding a substantial threshold within a 30-day rolling period are flagged for additional scrutiny. Deposits are then temporarily blocked, and enhanced due diligence (EDD) must be completed before the funds are released.
- **High-Risk Payment Channels:** Players using high-risk payment methods, such as prepaid credit or debit cards, are automatically reclassified into the high-risk category to mitigate potential AML/CFT concerns.
- **Quarterly Risk Reviews by the MLRO:** The Money Laundering Reporting Officer (MLRO) conducts quarterly assessments to identify emerging high-risk indicators. Any new risks are promptly integrated into the Customer Due Diligence (CDD) system, with relevant updates communicated to all staff.
- **Monitoring of Subjects in AML/CFT Warning Lists:** A list of individuals or entities flagged in AML/CFT-related warnings is maintained and closely monitored to ensure enhanced oversight.
- **Source of Funds Verification:** Source of funds undergoes thorough examination, particularly for players who are subject to enhanced due diligence procedures, where applicable.

By meticulously considering these risk factors, the Company ensures robust AML/CFT practices are in place to mitigate potential risks associated with money laundering and terrorist financing.

4.3 PEPs – Politically Exposed Persons

As part of our commitment to Anti-Money Laundering (AML) compliance, Overseas Gaming Management N.V. implements enhanced due diligence measures when dealing with foreign Politically Exposed Persons (PEPs), whether as customers or beneficial owners. These measures include:

- Risk Management Systems – Establishing vigorous mechanisms to identify whether a customer qualifies as a PEP.
- Senior Management Approval – Obtaining authorisation from senior management or the Compliance department before initiating or continuing a business relationship. This shall apply to new and existing customers, as well as occasional transactions.
- Source of Wealth and Funds Verification – Taking reasonable steps to verify the source of a PEP's wealth and funds by requesting a declaration from the customer and cross-checking information with independent, reliable sources. If public sources are insufficient, additional documentation may be required.
- Enhanced Ongoing Monitoring – Conducting continuous, risk-based monitoring of the business relationship to detect suspicious activity.

Additionally, reasonable steps shall be taken to identify domestic PEPs and individuals holding prominent positions within international organizations. If a higher risk is determined, the enhanced due diligence measures outlined above will also apply.

While all PEPs are subject to stricter due diligence, risk assessments are conducted on a case-by-case basis to tailor controls accordingly. These requirements extend to the family members and close associates of PEPs.

Screening for PEP status occurs during customer onboarding and continues throughout the business relationship. If a customer who was not initially identified as a PEP later attains PEP status, Overseas Gaming Management N.V. will implement the required enhanced measures within 30 days. Failure to comply will result in the termination of the business relationship.

4.4 Risk Monitoring

All user activities are thoroughly recorded and tracked. In particular, high-risk actions undergo enhanced and frequent monitoring. Senior management holds weekly meetings to assess reports on these high-risk activities. This manual review process works alongside the automated flagging system that is already operational.

The system is designed to identify irregularities and is protected by security controls. These controls enable the imposition of limits on a player's exposure, ensuring effective risk management.

Key areas under the system's surveillance include:

- Transactions surpassing NAF 4,000 (EUR 2,000), or exhibiting similar high deposit patterns or as deemed respectable by the Company
- Users originating from jurisdictions with elevated risk profiles in line with the FATF.
- Deposits made through payment channels associated with higher risk.
- Monitoring of Politically Exposed Persons (PEP) and those on the sanction lists.
- Identification of deposit or wagering activities that deviate significantly from a player's established average.
- Scrutiny of unreasonable player strategies, which may indicate potential risk or fraudulent behaviour.

4.5 Monitoring of Transaction – Customer Risk

In order to ensure robust supervision of transactions carried out within the Company's operations, and to bolster the monitoring protocols outlined previously, individuals will be sorted into risk categories according to their behaviour and accompanying data.

Low Risk

Persons meeting the prescribed criteria will be classified by the Company as low-risk individuals if they have not been previously categorized under any other Risk Class as described within this framework.

- Exhibit transaction or deposit volumes exceeding €2,000.
- Do not trigger any additional alerts or raise suspicions.

Customers identified as low risk will be subjected to Customer Due Diligence (CDD) procedures and will be required to furnish a valid identification document (such as an ID card or Passport) to verify their identity through reputable and independent sources.

Medium Risk

Individuals who meet the specified criteria will be categorized by the Company as presenting a medium risk. Such players are characterized by:

- The amounts deposited, the methods of payment used, and the timeframes associated with transactions contribute to the classification of a customer as medium-risk.
- Notably, attention is given to identified alerts or transactions that raise suspicion, particularly those exhibiting inconsistencies in geolocation.

An automated alert indicating medium risk is activated when a customer exceeds deposit thresholds exceeding EUR 5,000 within a month. Furthermore, agents possess the authority to manually elevate the customer's risk level to high upon detection of additional alerts or inconsistencies.

Customers classified as having a Medium Risk status will undergo Enhanced Due Diligence (EDD) verification procedures along with continuous monitoring to ensure compliance with regulatory standards and to mitigate potential risks effectively.

High Risk

Characteristics indicative of a high-risk customer include:

- Deposit amounts, payment methods, and transaction periods that escalate a customer's risk profile.
- Association with or are identified as Politically Exposed Persons (PEP).
- Ties to countries identified as high-risk (either through residency or citizenship).
- Presence of current suspicions related to money laundering activities.

An automated alert signaling high risk is activated when a customer surpasses deposit thresholds exceeding EUR 10,000 within a month or as stipulated by the Company.

Customers categorized as high-risk will undergo Enhanced Due Diligence (EDD) verification procedures, accompanied by continuous monitoring, to ensure adherence to regulatory requirements and to effectively mitigate potential risks.

4.6 Business Relation Obligations

The record-keeping protocols outline the types of Anti-Money Laundering (AML) data to be preserved and specify the minimum duration for retaining such data on the technical infrastructure utilized by the Company and in line with the Implementing Procedures. Given the varied responsibilities across different departments involved in collecting, processing, and storing data for various purposes, distinctions are drawn between data sets and types. This differentiation adheres to the requirements outlined in supplementary procedures

regarding risk-based documentation requests based on risk categorizations detailed in additional protocols.

Moreover, this procedure establishes a framework for the proper storage of AML-related documents on the designated technical infrastructure. It acknowledges the potential infringement of privacy legislation due to mishandling of personal data.

Identification Records

Documentation referred to in this context will be collected following the risk categorization specified in the particular guidelines.

This includes records related to players:

- Personal details obtained during registration or at a later stage as requested by the Company.
- Results of automated identity verification assessments.
- Copies of identification papers.
- Proof of residential addresses provided by the player at registration stage or during the business relationship.
- Additional documentation solicited based on the player's risk categorization, aiding in pinpointing the individual player (e.g., documentation verifying the source of wealth).

Records related to employees:

Information regarding personnel is collected during the initial hiring process and subsequent stages. This includes personal details obtained upon employment, curriculum vitae (CV) accompanied by certificates of good conduct, and records or certificates confirming completion of Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) training sessions.

Transaction Records

Due to the extensive scope of potential contractual and business associations involving a variety of individuals and entities, and the potential diversity of their arrangements, no classification based on the nature of these relationships has been conducted. As a general guideline, all transactional data should be digitally archived on the technical infrastructure

of the Company, pertaining to the specific identity on whose behalf the transaction was conducted. Records may include, but are not limited to:

- Method utilized for making deposits and/or withdrawals.
- The source and destination of funds.
- Approval of credit card transactions handled by clearing firms designated by the Company members; and
- Transaction volumes.

AML Legislation Records

The subsequent documentation required to substantiate and comply with the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR) should be recorded as outlined in section 4.7 (Record Keeping):

- Internal reports submitted to the Money Laundering Reporting Officer (MLRO).
- Any written determinations issued by the MLRO or Designated Employee, particularly providing explanations for the decision not to file a Suspicious Transaction Report (STR) with the FIU Curacao.
- All STRs submitted to the FIU, along with any subsequent follow-up submissions.
- Reports produced by the monitoring function (MLRO) and presented to senior management, including recommendations, assessments of Politically Exposed Persons (PEPs), and other pertinent information.
- Written considerations from senior management deliberating on the MLRO's recommendations and outlining steps for implementation.
- Internal Anti-Money Laundering (AML) audits.
- Documentation verifying AML/CFT training provided to employees.

4.7 Reporting of Transactions

Within its internal procedures, we are required to comply with the National Ordinance for Identification of Services, in addition to detecting and reporting any unusual transactions, whether intended or completed. It is essential for the casino to have appropriate procedures in place that address the following key areas:

- Identification of Unusual Transactions – Implementing methods to recognize transactions that deviate from normal patterns or raise suspicion.
- Documentation of Unusual Transactions – Keeping detailed records of unusual transactions for review and reporting purposes.
- Reporting of Unusual Transactions – Ensuring that unusual transactions are promptly reported to the relevant authorities as required by law.

4.1.1 Identification of Unusual Transactions

At Overseas Gaming ,recognising unusual transactions requires a deep understanding of each player. The purpose of gathering player information is to assess the associated risks and create a customer profile to predict their behaviour within the business relationship.

In line with NORUT legislation, we established objective and subjective indicators to assist management in guiding staff to identify and properly document unusual transactions. All such transactions must be reported to the compliance officer in the format approved by management. Supporting documents, such as copies of identification, cash-out slips, and any other relevant records, must also be submitted as supplementary materials. The compliance officer is responsible for maintaining a proper filing system for these records.

If any internally reported transactions are not submitted to the Financial Intelligence Unit (FIU), the reasons for this must be fully documented and signed off by the compliance officer and/or management.

To adhere to FATF Recommendation 11, shall pay special attention to complex or unusually large transactions and any patterns that lack a clear economic or lawful purpose.

What is Considered as Unusual Transactions?

- Transactions related to money laundering or terrorism financing that are reported to the Police or the Department of Justice.
- Transactions involving a natural or legal person, group, or entity listed under the Sanctions National Ordinance (N.G. 2014 no. 55).
- Transactions of NAf. 5,000 or more, regardless of whether the payment is made electronically, or through other non-physical methods. This includes, but is not limited to:
 - Cashless transactions of NAf. 5,000 or more, such as transfers from the casino's bank account to a local or international bank account at the client's request.
 - Accepting or releasing a deposit of NAf. 5,000 or more at the client's request.
 - Sale of chips (including tokens and credits) to a customer for NAf. 5,000 or more.
 - Cashing out an amount of NAf. 5,000 or more.

A transaction may be an individual occurrence or a series, combination, or pattern of transactions totalling NAf. 5,000 or more, assessed per gaming day.

- Presumed Money Laundering or Terrorist Financing Transactions: Transactions that raise suspicion of being related to money laundering or terrorist financing.

4.1.2 Reporting of Unusual Transactions

It is required to report any unusual transactions, or attempts to conduct unusual transactions, to the Financial Intelligence Unit (FIU) without delay in line with Article 11 of the NORUT. To ensure compliance, the casino must have established procedures for both internal and external reporting of unusual transactions, which must be clearly communicated to all relevant personnel.

All individual or series of unusual transactions, as outlined in the Regulation Indicators for Unusual Transactions, must be reported internally immediately. Supporting documentation should accompany each report.

4.1.3 Documentation of Unusual Transactions

We will register with the FIU and gain access to the goAML reporting portal upon validation by the FIU. The goAML portal supports bulk reporting, and the casino's account manager at the FIU should be contacted to determine eligibility for this service.

The compliance officer is responsible for preparing reports of all unusual transactions for external reporting to the FIU, in line with the FIU's reporting regulations. These reports and accompanying documents must be submitted in English through the goAML reporting portal.

Both the casino and its directors, officers, and employees are legally protected from criminal and civil liability for any breach of confidentiality when disclosing information to the FIU in accordance with reporting requirements.

4.8 Record Keeping

In accordance with the NOIS, NORUT, Sanctions National Ordinance (N.G. 2014, no. 55) and the Kingdom Sanction Act (N.G. 2016, no. 54), our record-keeping protocols dictate the collection and retention of the following information:

- Documentation detailing the implementation of the risk-based approach, including the Business Risk Assessment (BRA) and any related policy and procedural documentation.
- Customer Due Diligence documentation, as outlined in Section 9.2(b) of the Part 1 Implementing Procedures.
- Records pertaining to established business relationships, including transactional data, in accordance with Section 9.2(c) of the Part 1 Implementing Procedures.
- Internal reports submitted to the Money Laundering Reporting Officer (MLRO), along with justifications for any decisions not to file Suspicious Transaction Reports (STRs) with the FIU.
- Any STRs filed and subsequent follow-up submissions.

- Documentation verifying AML/CFT training provided to employees.
- Records of conduct certificates or other documentation used for employee screening.
- Agreements related to outsourcing activities.

This information will be securely stored on our servers and retained for a period of 5 years from the date when a customer ceases to be a participant, determined by their last transaction date.

Additionally, we will retain all records of reports and inquiries related to AML/CFT activity. These records will include details such as the date, nature of the inquiry, name of the authority or enquirer, powers being exercised, participants involved in the inquiry, and transactions implicated.

Our record-keeping practices will always adhere to applicable Data Protection and Privacy guidelines, and adjustments will be made as necessary to align with relevant laws and regulations.

5 Employee Screening and Ongoing Training Program

We are committed to maintaining the highest ethical standards in our operations and ensuring compliance with all relevant laws and regulations regarding financial transactions. To achieve this, the company will implement and enforce robust policies and procedures, including the thorough screening of employees for criminal records.

Additionally, we will develop and deliver training programs for all staff involved in handling transactions that may be deemed unusual, based on the indicators set forth in the Ministerial Decree on Indicators for Unusual Transactions (N.G. 2015 no. 73). This training will include clear guidelines on employee conduct and ongoing education to foster awareness and compliance with anti-money laundering (AML) and counter-terrorist financing (CTF) measures.

Training will be tailored to specific roles within the organization, ensuring that relevant topics are covered for each department. At a minimum, training will address the following key areas:

5.1 New Employees

All new employees who will interact with customers or handle their transactions, regardless of their seniority level, must receive comprehensive training on the nature and processes of money laundering, terrorist financing, and the importance of reporting any unusual transactions to the designated officer. They will be introduced to the company's internal

policies, procedures, and regulations related to money laundering, terrorist financing, weapons proliferation, and the reporting requirements associated with these activities. The training will also cover money laundering techniques and trends specific to the gambling industry, as well as customer due diligence practices. Employees will be educated on both objective and subjective indicators for identifying and reporting unusual transactions.

5.2 Casino Team

This team serves as the first line of defence against money laundering. They will undergo an introductory course covering the fundamentals of Anti-Money Laundering (AML) and its significance. In addition, they will receive specialized training on how money launderers may attempt to exploit casinos for illicit activities. Staff members will also be trained on the appropriate steps to take if they identify potential money laundering activities. Those involved in account opening will be instructed on the importance of verifying the customer's identity to prevent fraudulent activities.

5.3 Audit Team

Individuals responsible for overseeing, monitoring, and testing money laundering controls will receive training on regulatory changes, emerging money laundering tactics, enforcement actions, and how these developments affect the organization.

5.4 AML Compliance Team

The individuals managing the AML program require specialized training to stay informed about new trends and regulatory changes that affect the organization's risk management. This may include attending conferences or AML-focused presentations for in-depth learning.

5.5 Senior Management

Senior Management which includes Managers and Board of Directors must receive advanced training on all aspects of money laundering, terrorist financing, policies, procedures, and regulations. Additionally, money laundering risks and concerns should be regularly communicated to the board to ensure they remain aware of the reputational risks these issues pose to the organization.

5.6 Training Program

Regular refresher training should be organized to ensure staff members remain updated on the latest developments, techniques, methods, and trends related to money laundering and

terrorist financing. To demonstrate adherence to these training requirements, the casino must maintain comprehensive records that include the training content, the names of employees who attended, the dates the training was provided, the results of any assessments measuring staff understanding of AML and CFT obligations, and an ongoing training plan for continuous education.

6 Payout Management

Payments will exclusively be accepted and processed through accounts held with licensed financial institutions or authorized payment providers, which have not been prohibited for use by the Authority. Overseas Gaming Management will engagement with Payment Service Providers, such engagement will commence upon receipt of the license reactivation from the Authority.

All funds deposited by players or owned by the licensee will be allocated to the corresponding player accounts. Transactions involving cash deposits or withdrawals between the Company and its players will not be facilitated.

An inactive account procedure may be implemented to identify dormant players, who may incur a monthly fee until activity resumes. Prior notification of at least 30 days will be provided to players regarding any fees deducted. This inactivity process will adhere to guidelines outlined in the Authority's Player Protection Directive and other relevant legislation. Senior management will determine the necessity and criteria for implementing an inactive account process.

5.1 Process for Deposits

The deposit process at Overseas Gaming Management follows a structured series of steps to ensure transparency and security for players. Initially, players are required to register on the app and complete necessary Know Your Customer (KYC) procedures to establish their identities. Following registration, players are directed to the Deposits page where they are presented with a range of popular deposit options tailored to their country. These options typically include credit cards, debit cards, and eWallets which are approved by the Financial Services Authority (FSA).

Once a player selects their desired deposit method and specifies the amount, they are redirected to a certified Payment Service Provider (PSP) for processing. Upon submission of the transaction, the Company awaits approval from the card acquirer or eWallet. Once approval is received, the Company updates both the player's account and the database with the transaction details, ensuring accuracy and accessibility for future reference.

The Company takes stringent measures to safeguard player funds, ensuring that all balances are covered by designated bank accounts and PSP wallets. This guarantees that player balances are always at least equivalent to the funds held in these dedicated accounts. Regulatory requirements mandate that 90% of these funds must be covered within designated bank accounts or equivalent accounts with documented segregation as player accounts.

Additionally, the Company's Board receives regular reports to monitor the segregation of player funds against system player balances, providing an extra layer of oversight. Daily reconciliation processes are implemented to compare Protected Player Funds accounts with system player account balances, with additional funds deposited promptly if necessary to maintain compliance and uphold player trust.

5.2 Process for Withdrawals

Players who wish to withdraw funds from their available balance can do so using an approved payout method. To initiate a withdrawal request, the player navigates to the Accounts page on our website, where they are presented with their available balance eligible for withdrawal. Here, they select the desired withdrawal amount and their preferred payout method. It's essential to note that the domain stipulates that withdrawn funds must first be returned via the method of deposit. For instance, if the player initially deposited funds using a credit card, the withdrawal must be processed back to that same credit card, or to the eWallet or bank account used for bank transfer deposits, where applicable.

Subsequently, the Company's internal risk and fraud processes rigorously examine and re-validate the withdrawal request before approving it for payout. This verification procedure encompasses several steps, including scrutiny of Know Your Customer (KYC) documentation, validation of true identity, manual checks to detect duplicate accounts, and, if necessary, requests for additional KYC documentation.

Upon approval by the Company, the payout request is forwarded for processing and submission to the Payment Service Provider (PSP). The PSP then communicates the outcome of the transaction, confirming whether it was successful or not. Simultaneously, the Company database is updated to reflect the adjusted player balance in light of the withdrawal.

Finally, the website undergoes an update to display the revised player account balance, ensuring that players have real-time access to their updated financial status.

5.3 Acceptance and Funds Handling

All wagers deemed valid and active must originate from funds that have been securely escrowed. This necessitates that the funds be readily available in the player's designated account, commonly referred to as the "wallet." This availability can be achieved through successful transfer transactions or by obtaining assurance from the card issuer or original funding source.

Funds residing in a player's wallet can be utilized to place wagers by being temporarily placed in escrow, or they can be withdrawn back to their originating source or account. However, it's important to note that funds cannot be transferred between different users' accounts.

Comprehensive records of all fund movements, whether inbound or outbound, are accessible to the player. These details encompass transactions to and from external accounts as well as funds allocated for wagers at any stage of the process. They are prominently featured within the player's wagering summary and are also readily viewable on their wallet page.

Any modifications to the fund balance resulting from deposits or withdrawals are fully elucidated, providing players with a clear depiction of their financial status before and after each transaction.

The regulations governing the outcome of wagers, inclusive of scenarios where no winning wagers transpire, are consistently and openly available on the site. This ensures transparency and fairness for all participants. Additionally, due to the system's state-based architecture, any interruptions in service will not lead to loss of data or funds. Instead, there may be a temporary inability to place wagers during such periods. To address this, the system has been meticulously engineered as a High Availability (HA) platform at every level, thereby mitigating the impact of any discontinuity in service.

7 Platform Capabilities

Overseas Gaming Management will utilize their proprietary, in-house developed platform to support their operations. This advanced system is designed to generate all necessary reports required for the Company's daily activities. The platform is specifically capable of extracting key reports at the end of each day or month, as needed. These reports include:

- A detailed summary of cashable balances in players' accounts, broken down by the different currencies used during gameplay.

- A comprehensive list of unprocessed withdrawals, indicating the amounts deducted from players' cashable balances that have not yet been transferred by the licensee to the players' designated wallet, bank account, or payment card.

It is important to emphasize that these reports will exclude any data related to test accounts, ensuring that only legitimate player transactions are reflected for accuracy and relevance.

Currently, the Company does not offer jackpots within its games. However, should the Company decide to introduce jackpot features in the future, they commit to informing the appropriate regulatory body prior to incorporating such features into their live operations.