

ANTI-MONEY LAUNDERING POLICY

VER. 1.0. dated April 08, 2025

ABUDANTIA B.V.

registration number: 126608

registration number: Groot Kwartierweg 10, Livestrong Building, Curacao

Version control

Policy	Approval Date	Approver
Anti-Money Laundering Policy Ver. 1.0.	April 08, 2025	eMoore N.V.

TABLE OF CONTENTS

1. Introduction

- 1.1. Purpose and Scope
- 1.2. Regulatory Framework

2. Key AML Concepts

- 2.1. Definition of Money Laundering, Terrorist Financing, Financing of proliferation
- 2.2. Common Typologies and Red Flags

3. Organizational Structure and Governance

- 3.1. Management Board
- 3.2. MLRO
- 3.3. Compliance Unit
- 3.4. Three lines of defense model

4. Customer Risk Assessment Framework

- 4.1. Risk-Based Approach (RBA) to Customer Risk Assessment
- 4.2. Key Risk Factors in Customer Risk Assessment
- 4.3. Customer Risk Assessment Process

5. Ongoing monitoring and transaction review

- 5.1. Continuous Monitoring
- 5.2. AML Specialist Review
- 5.3. Source of Wealth (SOW) Verification

6. Customer Due Diligence (CDD)

- 6.1. Initial Customer Due Diligence
- 6.2. Enhanced Due Diligence
- 6.3. Simplified due diligence
- 6.4. Mitigation and Ongoing Monitoring

7. Transaction Monitoring and Reporting

- 7.1. Recognition of unusual transactions
- 7.2. Regulatory Reporting Obligations and Compliance measures
- 7.3. Prohibition of disclosure
- 7.4. Record-Keeping and Documentation Requirements

8. Compliance and Internal controls

- 8.1. Compliance measures
- 8.2. Implementing Risk Mitigation Controls
- 8.3. Periodic Review and Adjustment of Risk Policies and Procedures

9. Employee Screening, Training and Awareness

- 9.1. AML Training Programs strategy and importance
- 9.2. Employee screening

1. INTRODUCTION

1.1. Purpose and scope

The purpose of this Anti-Money Laundering (AML) Policy is to establish a framework to prevent, detect, and report any activity related to money laundering, terrorist financing, and other financial crimes within Abudantia B.V.

As a licensed gaming operator under Curacao law, Abudantia B.V. is committed to complying with all applicable AML regulations and international best practices. This policy outlines the principles and procedures that Abudantia B.V. follows to ensure a robust AML compliance program, safeguard the integrity of gaming operations, and mitigate the risk of financial crime.

This policy applies to all employees, management, and third-party service providers of Abudantia B.V. involved in customer interactions, financial transactions, or regulatory compliance. It covers all gaming activities, including but not limited to:

- Player registration and identity verification (Know Your Customer – KYC);
- Transaction monitoring and suspicious activity detection;
- Customer due diligence (CDD) and enhanced due diligence (EDD) procedures;
- Record-keeping and reporting obligations to relevant authorities;
- Internal controls and staff training on AML compliance.

1.2. Regulatory Framework

AML internal policies and procedures are based on industry-leading standards, best practices and methodologies from:

- Curaçao Gaming Control Board (GCB) AML Requirements
- Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of Weapons of Mass Destruction by GCB
- Financial Action Task Force (FATF) Recommendations
- EU AML Directives (AMLDs) – Applied Best Practices (covering all six directives)
- EU's High-Risk Third Countries List
- United Nations Office on Drugs and Crime (UNODC) AML Guidelines
- Sanctions Compliance & PEP Screening, including: United Nations (UN) Sanctions List, EU Sanctions List, US OFAC Sanctions (SDN List), Dutch Kingdom Sanctions Act (specific for Curaçao), Other international sanctions lists
- The Gambling Act (UK) & UKGC AML Guidelines
- American Gaming Association (AGA) AML Best Practices
- Malta Gaming Authority (MGA) AML Rules
- The Three Lines of Défense Model
- Key principles of corporate governance

The Company implements sound internal policies and procedures to combat money laundering and the financing of terrorism, and strictly complies with current anti-money laundering, combating the financing of terrorism and financing of proliferation legislation as well as regulations, in particular the laws and regulations regarding customer due diligence, the reporting of unusual transactions and keeping adequate records of clients and transactions (NOIS, NORUT, Sanctions National Ordinance, Kingdom Sanction Act). These include among others:

- The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92);
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99);
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);

- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015 no. 30);
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48).

These laws and regulations and any additional regulations issued pursuant to the NOIS, NORUT, the Sanction National Ordinance and the Kingdom Sanction Law form the main legal basis for the Curaçao Gaming Sector to combat money laundering, the financing of terrorism and the proliferation of weapons.

2. KEY AML CONCEPTS

2.1. Definition of Money Laundering, Terrorist Financing, Financing of proliferation

All acts done with money of illegal origin to change its identity so that it appears to have originated from a legitimate source, can be considered **money laundering** (ML). It is the process of making dirty money look clean. Money Laundering consists of three phases:

- **Placement.** During this stage, the money launderer introduces the illegal proceeds into the financial system through financial institutions, casinos, shops and other cash intensive businesses. This is done among other things by buying chips for cash, then redeeming value without playing or with minimal playing, funding casino accounts with credit and debit cards, prepaid cards, checks and cryptocurrency and then requesting for pay out and inserting funds into gaming machines and immediately claiming those funds as credits;
- **Layering.** This stage involves converting the proceeds of crime into another form to disguise the audit trail, source and ownership of funds. It can involve transactions such as transfers of funds from one account to another, sometimes to or from other casinos or jurisdictions, currency exchange, structuring and refining and gambling accounts held for storing moneys and hiding them from the authorities;
- **Integration.** The re-entry of funds into the economy in what appears to be normal business or personal transactions. Examples are: the purchase of luxury assets, financial investments, investing in gaming companies or commercial investments.

Financing of Terrorism (FT) is the financing of terrorist acts, of terrorists and terrorist organizations. A terrorist act is an act to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.

The most basic difference between financing of terrorism and money laundering involves the origin of the funds. Terrorist financing uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds. Money laundering always involves the proceeds of illegal activity. There is a need for the terrorist group to disguise the link between it and its legitimate funding sources. In doing so, the terrorists use methods similar to those criminal organizations use to launder money like cash smuggling, structuring, wire transfers, purchase of monetary instruments, use of debit and credit cards. While ML is concerned with obscuring the source of funds, FT is mostly concerned with obscuring the end recipient of the funds.

Financing of proliferation (FP) is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

2.2. Common Typologies and Red Flags

To effectively combat money laundering, terrorist financing, and other financial crimes, Abudantia B.V. maintains a comprehensive monitoring system to detect suspicious activities. The following money laundering typologies and red flags serve as key indicators that may require further investigation and reporting to regulatory authorities. While no single indicator automatically signifies illicit activity, a combination of these factors may warrant additional scrutiny.

2.2.1. Common Money Laundering Typologies

- **Structuring (Smurfing).** Players attempt to avoid detection by breaking large transactions into smaller amounts over time, ensuring that individual deposits or withdrawals remain below reporting thresholds. Frequent small deposits followed by a single large withdrawal, or vice versa.

- Chip Dumping and Collusion. In peer-to-peer games, such as poker, colluding players intentionally lose hands to another player as a means of transferring illicit funds. Suspicious betting patterns where one player consistently wins against a specific opponent despite statistical improbability.
- Rapid Movement of Funds with Minimal Play. Players deposit large amounts, place minimal bets, and withdraw the remaining balance, suggesting an attempt to ‘clean’ illicit funds through the platform. High turnover of deposits and withdrawals without significant gaming activity.
- Third-Party Payments and Unexplained Transactions. Accounts receiving deposits from unrelated third parties or withdrawing funds to accounts not belonging to the registered player. Players using multiple payment sources that do not match their identity details.
- Multiple Accounts and Identity Manipulation. Players creating multiple accounts under different names or email addresses but using the same IP address, device, or payment details. Attempts to bypass verification procedures by providing fraudulent identity documents.
- Use of Cryptocurrencies and Anonymous Payment Methods. Customers funding their accounts with high-risk payment methods, such as prepaid cards, e-wallets, or cryptocurrencies, without a clear source of funds. Frequent conversion between fiat and cryptocurrencies with no gaming activity.
- Transactions Involving High-Risk Jurisdictions. Players depositing or withdrawing funds to/from countries known for weak AML enforcement or being on international sanction lists.
- Abuse of Bonuses and Promotional Offers. Players exploiting welcome bonuses or promotions across multiple accounts to convert bonus funds into withdrawable balances. Suspicious betting strategies that aim to maximize withdrawals with minimal risk.

2.2.2. Red Flags Indicating Potential Money Laundering

The following behaviors and transactional patterns are considered potential red flags that require enhanced scrutiny:

- Player Behavior and Account Activity

Reluctance to provide KYC documentation or frequent submission of incorrect/inconsistent information.

Unusual betting behavior that does not align with typical gaming activity, such as erratic wagers or sudden changes in bet size.

Repeated requests to change withdrawal methods or payment accounts.

Excessive use of VPNs, proxy servers, or frequently changing IP addresses.

Players attempting to bypass AML controls or asking customer service about compliance thresholds.

Customers who refuse or are unable to provide proof of source of funds, particularly in cases where they have previously self-excluded, indicating potential circumvention of gambling restrictions.

- Payment and Transaction Patterns

Frequent deposits and withdrawals without any corresponding gaming activity.

Use of multiple credit cards, bank accounts, or payment methods that are not linked to the player's identity.

Large transactions in high-value amounts with no clear economic rationale.

Disproportionate deposits relative to the player's declared financial background.

Multiple chargebacks, refunds, or reversed transactions without a valid explanation.

- Geographic and High-Risk Customer Indicators

Players from jurisdictions known for lax AML enforcement, tax havens, or sanctioned countries.
Transactions involving politically exposed persons (PEPs) or individuals linked to criminal organizations.
Accounts showing logins from multiple countries in short time spans, indicating possible account takeovers or proxy use.

2.2.3. Response to Identified Red Flags

When a red flag or suspicious pattern is detected, Abudantia B.V. will take the following steps:

- Conduct Enhanced Due Diligence (EDD) – Request additional documentation or information from the customer, such as proof of income, source of funds, or business relationships.
- Internal Investigation – The AML Compliance Officer will analyze the transaction patterns and determine if there is a reasonable suspicion of money laundering or financial crime.
- Report Suspicious Activity – If warranted, a Suspicious Transaction Report (STR) will be submitted to the relevant Curacao regulatory authority.
- Cooperate with Law Enforcement – Provide necessary records and assistance to regulatory bodies or financial intelligence units (FIUs) as required by law.
- Account Closure and Fund Freezing – If a player is found to be engaged in illicit activities, the account may be permanently closed, and funds may be frozen in compliance with AML regulations.

2.2.4. Staff Responsibility

All employees must be vigilant in identifying potential AML risks and report any suspicious activity to the AML Compliance Officer without delay. Failure to comply with AML policies may result in disciplinary action or legal consequences.

3. ORGANIZATIONAL STRUCTURE AND GOVERNANCE

3.1. Management Board

The Management Board plays a central role in overseeing the implementation and ongoing effectiveness of the internal AML policies, procedures and controls.

This includes ensuring that a robust framework for risk management, internal controls, and compliance measures is in place to mitigate the risks associated with money laundering, terrorist financing, and other forms of financial crime. The Board is ultimately responsible for setting the company's strategic direction in relation to money laundering prevention and ensuring compliance with both internal policies and external regulatory requirements.

The Management Board is committed to combat the abuse of its facilities, products and services for the purpose of money laundering, terrorist financing and the proliferation of weapons of mass destruction purposes.

The Management Board ensures that risk governance is deeply embedded within the company's overall operational framework. It provides a comprehensive and structured approach to risk mitigation, enabling the company to align with international best practices, industry standards, and evolving regulatory expectations. In doing so, the Management Board works proactively to create an environment that fosters ethical business practices, transparency, and accountability.

To ensure strong oversight and robust corporate governance, the Management Board is responsible for establishing and maintaining a comprehensive AML framework that aligns with regulatory requirements and business objectives. This includes:

- Approving and Overseeing AML Policies and Procedures. Reviewing and endorsing all key AML policies, frameworks, and procedures to ensure they are effective, up to date, and compliant with regulatory obligations.
- Ensuring Adequate Resources for AML Compliance: Allocating sufficient personnel, training, technology, and financial resources to support AML/CFT functions, compliance monitoring, and overall risk management.
- Promoting a Strong Compliance Culture: Embedding ethical business practices and regulatory adherence into the company's operations, ensuring that AML/CFT principles are integrated at all levels of the organization.
- Monitoring and Enhancing AML Controls: Conducting ongoing evaluations of the company's AML infrastructure, ensuring the effectiveness of internal controls, and implementing enhancements where needed.
- Engaging with Internal and External Stakeholders: Maintaining open communication with regulators, auditors, compliance teams, and other key stakeholders to ensure transparency and proactive risk management.

Additionally, the Management Board plays a critical role in assessing and strengthening the company's AML effectiveness by:

- Reviewing AML Compliance and Audit Reports: Regularly analyse risk management assessments, transaction monitoring results, and compliance audits to identify potential vulnerabilities.
- Implementing Corrective Measures: Addressing any identified weaknesses in AML controls by enforcing remedial actions and process improvements.
- Supporting Innovation in AML Technologies: Encouraging the adoption of advanced monitoring tools and methodologies to enhance customer due diligence, risk detection, and compliance efficiency.

3.2. MLRO

To ensure that the Company's AML Policy and procedures are adhered to, the Company designated a Money Laundering Reporting Officer (the "MLRO"):

MLRO contact details:

Name: Vadym Riabokin

Email: legal@abudantia.com

The Money Laundering Reporting Officer serves as the senior officer at management level and independent from the games operations, responsible for the detection and deterrence of money laundering and terrorist financing. MLRO acts as the primary authority for AML/CFT compliance and risk oversight.

MLRO officer has timely access to customer identification data and other CDD information, transaction records, and other relevant information. The MLRO acts as the primary liaison between the company and regulatory authorities, ensuring that the organization remains fully compliant with applicable laws and reporting obligations.

Key responsibilities of the MLRO include:

- Designing and implementing the AML program;
- Verifying adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing;
- Review compliance with the company's policy and procedures;
- Organizing training sessions for the staff on various compliance-related issues;
- Analyzing transactions and verifying whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
- Reviewing all internally reported unusual transactions for their completeness and accuracy with other sources;
- Keeping records of internally and externally reported unusual transactions;
- Designing an internal procedure about when reporting of unusual transactions will lead to blocking/freezing of user accounts, taking into account the risk of tipping off the player;
- Executing closer investigation of unusual transactions if necessary;
- Preparing the external report of unusual transactions;
- Making necessary changes to the AML program;
- Remaining informed on the local and international developments on money laundering and terrorist financing and making suggestions to management for improvements; and
- Preparing periodic information on the company's efforts against money laundering and financing of terrorism and financing of proliferation.

Given the critical role of the MLRO in protecting the organization from financial crime risks, this position requires strong analytical capabilities, regulatory expertise, and a proactive approach to risk mitigation. The MLRO has direct access to senior management and is empowered to take necessary actions to safeguard the integrity of the company's operations.

3.3. Compliance Unit

The Compliance Unit serves as a cornerstone of the company's AML/CFT framework, ensuring that all policies, procedures, and controls are effectively implemented and continuously enhanced to meet regulatory requirements and industry best practices.

It provides oversight and support to the MLRO while promoting a strong compliance culture throughout the organization. Key responsibilities of the Compliance Unit include:

- Policy Implementation and Oversight: Ensuring that AML/CFT policies, procedures, and internal controls are properly executed across all business operations.

- Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD): Overseeing the application of CDD and EDD measures, particularly for high-risk customers, transactions, and jurisdictions.
- Regulatory Compliance and Adaptation: Monitoring changes in AML/CFT regulations and updating internal policies and processes to ensure continued compliance with legal requirements.
- Transaction Monitoring and Investigations: Supervising the effectiveness of transaction monitoring systems, investigating suspicious activity, and ensuring timely reporting of suspicious transactions.
- Internal Compliance Reviews and Audits: Conducting periodic compliance assessments and independent testing of AML controls to identify gaps and implement necessary improvements.
- Collaboration with Other Departments: Working closely with fraud prevention, legal, finance, and IT teams to strengthen AML detection and mitigation efforts.
- Training and Awareness Programs: Developing and delivering AML training initiatives to ensure employees remain informed of regulatory obligations and best practices.
- Regulatory Reporting and Liaison: Coordinating with external auditors, regulatory authorities, and financial intelligence units (FIUs) to fulfill reporting obligations and facilitate compliance examinations.

The Compliance Unit operates in close partnership with the MLRO to proactively enhance AML/CFT measures, mitigate emerging financial crime risks, and uphold the company's commitment to regulatory integrity.

3.4. Three lines of defense model

The company adopts the internationally recognized Three Lines of Defense model to ensure a structured and effective approach to AML prevention. This framework enables clear role delineation among various functions, fostering accountability, independent oversight, and continuous improvement of risk management measures.

3.4.1. First Line of Defense – Business Units

The First Line of Defense consists of the business units that engage directly with customers, including customer service, onboarding, and transaction processing teams. These teams are responsible for the initial assessment and ongoing monitoring of customer risk factors, ensuring compliance with internal AML/CFT policies and regulatory obligations.

Key responsibilities of the First Line of Defense include:

- Implementing customer due diligence (CDD) and enhanced due diligence (EDD) during onboarding and throughout the customer relationship.
- Ensuring compliance with AML/CFT policies by following established procedures for identity verification, record-keeping, and transaction processing.
- Monitoring transactions for unusual or suspicious activity, utilizing automated detection tools and real-time monitoring systems.
- Escalating high-risk cases or suspicious transactions to the Compliance Unit and MLRO for further review and investigation.
- Maintaining secure and accurate records of customer documentation and transactional data in compliance with AML/CFT regulations.
- Providing AML awareness training to frontline employees to enhance their ability to detect and prevent financial crime.

By integrating risk-conscious procedures into daily operations, the First Line of Defense serves as the company's first safeguard against financial crime.

3.4.2. Second Line of Defense – AML, Compliance & Risk Management

The Compliance Function and MLRO form the Second Line of Defense, providing expert guidance, independent oversight, and structured governance to enhance the effectiveness of risk management efforts.

Key responsibilities of the Second Line of Defense include:

- Defining and maintaining the company's AML/CFT policies, frameworks, and risk-based methodologies.
- Conducting independent reviews of customer due diligence and transaction monitoring activities performed by the First Line of Defense.
- Ensuring compliance with regulatory requirements and guidelines from relevant authorities, including Curaçao's AML/CFT framework.
- Developing and refining risk scoring models to ensure accurate classification of customers into Negligence, Low, Medium Low, Medium, and High-risk levels.
- Providing ongoing training and advisory support to frontline employees to improve their ability to identify and mitigate risk effectively.
- Monitoring transactions and customer behaviour through advanced analytics, automation tools, machine learning, and other technological solutions to identify potential risks proactively.
- Escalating significant risks, suspicious transactions, and regulatory breaches to the Management Board for corrective action.

The Compliance Function and MLRO play a crucial role in ensuring that the company remains aligned with evolving AML/CFT requirements while supporting operational efficiency and business growth.

3.4.3. Third Line of Defense – Internal Audit & Independent Review

The Third Line of Defense provides independent assurance that the company's risk management framework is functioning effectively and meeting regulatory standards. Internal Audit and other external independent review mechanisms assess the adequacy and effectiveness of the risk governance framework, compliance and internal controls system ensuring that all AML/CFT measures are operating as intended.

Key responsibilities of the Third Line of Defense include:

- Conducting periodic audits and reviews of the company's AML/CFT policies, processes, and internal controls.
- Identifying gaps, deficiencies, or areas for improvement in AML controls and recommending corrective actions.
- Evaluating the adequacy of compliance training programs and compliance practices across all levels of the organization.
- Providing independent feedback to the Management Board on the effectiveness of AML risk mitigation measures and policy implementation.
- Assessing the alignment of the company's AML/CFT efforts with international best practices and regulatory expectations.
- Supporting continuous improvement by ensuring that findings from audits and compliance reviews are integrated into strategic planning and operational enhancements.

3.4.4. Integration of the Three Lines of Defense Model

The company ensures seamless integration of the Three Lines of Defense model into its corporate governance and risk management framework.

- The First Line of Defense remains responsible for operational AML processes, transaction monitoring, and frontline compliance.
- The Second Line of Defense provides oversight, policy guidance, and ensures compliance with AML/CFT obligations.

- The Third Line of Defense delivers independent assessments, ensuring continuous improvement and accountability across all risk management functions.

By adopting the Three Lines of Defense model, the company enhances its ability to prevent, detect, and mitigate financial crime, ensuring a compliance-driven corporate culture while maintaining regulatory adherence and operational efficiency.

4. CUSTOMER RISK ASSESSMENT FRAMEWORK

The company's Customer Risk Assessment Framework (CRAF) is designed to ensure a structured, data-driven, and comprehensive approach to identifying, assessing, and mitigating the risks associated with money laundering (ML), terrorist financing (TF), and other financial crimes. The framework aligns with Curaçao's AML/CFT regulatory requirements and integrates industry best practices to safeguard the company's operations, reputation, and compliance standing.

Customer risk assessment is a continuous and dynamic process, with risk factors being monitored throughout the customer lifecycle. By employing a risk-based approach (RBA), the company ensures that resources are allocated efficiently to mitigate the highest risk exposures while maintaining a seamless and compliant customer experience.

4.1. Risk-Based Approach (RBA) to Customer Risk Assessment

The company employs an RBA to classify customers based on their risk levels, allowing for differentiated levels of due diligence and ongoing monitoring. The five-tiered risk model consists of the following levels:

Negligence Risk (1) – Customers with minimal exposure to ML/TF risks, typically residing in highly regulated jurisdictions with strong AML/CFT frameworks, low crime rates, and high-income economies. These include countries with well-developed financial and legal systems that actively enforce compliance standards.

Low Risk (2) – Customers with standard risk factors who meet all due diligence criteria and pose minimal AML/CFT concerns. They usually originate from countries with stable regulatory environments (EU countries), but may have slightly lower compliance enforcement compared to negligence risk jurisdictions. These customers engage in typical gaming behaviour with no unusual transaction patterns.

Medium Low Risk (3) – Customers requiring additional scrutiny due to minor risk indicators, including geographic location, transaction behaviour, or gaming patterns that slightly deviate from standard player profiles. This may include customers from countries with not so strict AML frameworks or jurisdictions with low and moderate risk exposure.

Medium Risk (4) – Customers exhibiting moderate risk indicators, such as high transaction volumes, frequent large deposits and withdrawals, connections to higher-risk jurisdictions, or irregular gaming behaviour indicative of potential ML/TF activities. These customers may be from countries with known AML soft rules, limited regulatory oversight, or regions that required extra supervision.

High Risk (5) – Customers with significant ML/TF risk exposure, high-net-worth individuals from high-risk countries, and those engaged in industries vulnerable to financial crime. This category also includes customers exhibiting aggressive betting strategies, rapid movement of funds, or use of multiple accounts to obscure financial trails. Additionally, customers from countries under FATF monitoring or blacklisted jurisdictions (e.g., North Korea, Iran) fall under this category due to the severe regulatory deficiencies and sanctions imposed on these regions.

Risk classification is determined through a weighted scoring methodology that evaluates various risk factors and assigns an overall risk score to each customer. The methodology incorporates both quantitative and qualitative criteria to ensure a comprehensive assessment.

Quantitative criteria include measurable financial and transactional parameters such as:

- Transaction volume, deposit, and withdrawal frequency
- Geographic risk exposure based on country risk ratings
- Payment methods used (e.g., cryptocurrency, prepaid cards, or high-risk financial instruments)
- Gaming behaviour, including bet size, frequency, and volatility

- Historical compliance record and any past suspicious activity reports

Qualitative criteria focus on subjective and contextual risk factors, including:

- Behavioural patterns and deviations from typical gaming profiles
- Business relationships and affiliations
- The complexity of ownership structures in corporate accounts
- Media exposure and reputational risks
- Regulatory and legal considerations related to online gambling

By integrating both quantitative and qualitative elements, the company ensures a nuanced and dynamic risk assessment framework that adapts to evolving risk landscapes and regulatory expectations specific to the online gaming industry.

4.2. Key Risk Factors in Customer Risk Assessment

The risk classification of customers is based on multiple factors that help the company evaluate potential exposure to financial crime risks. These factors include, but are not limited to:

- Geographical Risk – The country or jurisdiction in which the customer resides or conducts business plays a significant role in risk assessment. High-risk jurisdictions include those identified by the Financial Action Task Force (FATF) as having deficiencies in AML/CFT controls.
- Customer Profile Risk – This includes factors such as the nature of the customer’s business, their occupation, source of wealth, and affiliations with high-risk industries.
- Transaction Risk – The frequency, volume, and complexity of transactions conducted by the customer. Unusual transaction patterns, rapid movement of funds, and structuring activities are indicators of increased risk.
- Delivery Channel Risk – The method by which customers interact with the company, such as online platforms, mobile applications, or in-person engagements. Digital and remote interactions typically pose higher risks due to the potential for anonymity and fraud.
- Product & Service Risk – The types of products and services used by the customer, including gaming activities, financial transactions, and other relevant services. High-risk products include those with high liquidity, anonymity, or cross-border transfer capabilities.
- Behavioural Indicators – Sudden changes in transaction behaviour, inconsistencies in provided information, reluctance to provide documentation, or attempts to evade due diligence measures.

4.3. Customer Risk Assessment Process

The company’s customer risk assessment process is divided into three key stages:

- Initial Risk Assessment
- Risk Reassessment at 4,000 NAF Transaction Volume
- Ongoing Monitoring and Periodic Risk Reassessment.

4.3.1. Initial Risk Assessment

The Initial Risk Assessment (IRA) is the first step in evaluating the potential money laundering (ML) and terrorist financing (TF) risks posed by new customers. This assessment occurs during the onboarding process and before the customer makes their first deposit. The primary objectives of the IRA are to:

- Identify high-risk individuals early and prevent them from engaging with the platform.
- Classify customers based on their country of residence and self-reported financial details.
- Ensure compliance with AML/CFT regulatory requirements and FATF guidelines.
- Establish a foundation for ongoing monitoring and risk-based due diligence.

Onboarding Process and Initial Data Collection

The onboarding process is the first point of risk assessment, where every customer is required to provide specific details. The system then automatically verifies this information against predefined risk factors.

Additionally, the customer's country of residence is assessed based on an internal country risk rating aligned with FATF recommendations. The country risk rating plays a fundamental role in determining the initial risk classification. Countries are categorized into five risk levels, ranging from Negligence Risk (1) to High Risk (5). Customers from jurisdictions classified as high-risk (e.g., countries under FATF monitoring or subject to international sanctions) are automatically flagged for enhanced due diligence (EDD) or denied service altogether. Conversely, customers from well-regulated, low-risk jurisdictions are subject to standard due diligence measures. A full list of country classifications is provided in CRA Policy.

Mandatory Information Collected at Registration:

- Full name: To ensure identity verification and screening against global watchlists.
- Country of residence: Selected from a predefined list to determine the country's AML risk level.
- Date of birth: To verify age eligibility and match against potential identity fraud attempts.
- Permanent residential address: To cross-check country risk and assess potential address inconsistencies.
- Customer self-declaration: A required checkbox confirming the customer is playing on their own behalf and not using another person's identity.

Automated Screening and Immediate Risk Assessment:

- Once the registration form is submitted, the system automatically cross-references customer details with: Global Sanction Lists (UN, OFAC, EU, UK, etc.), Politically Exposed Persons (PEPs) Databases, FATF High-Risk Jurisdictions and Monitored Countries.
- If a match is found in the sanction or PEP lists, the account is immediately blocked, preventing access to deposits, withdrawals, or gameplay.
- Customers from high-risk or FATF-monitored jurisdictions may either be denied service outright or subject to Enhanced Due Diligence (EDD), depending on the country's specific risk rating and other specific factors.

Pre-Deposit Risk Evaluation

Before making their first deposit, customers must provide additional financial self-assessment details through an interactive pop-up form. These details help gauge the expected financial activity of the customer and detect inconsistencies in later transactions.

Self-Declared Financial Information Required:

- Estimated Monthly Deposit Range:
 - o €0 - €1,000
 - o €1,000 - €3,000
 - o €3,000 - €10,000
 - o €10,000 and more
- Source of Income (Dropdown Selection):
 - o Salary / Employment Income
 - o Business / Self-employment Income
 - o Investment Income
 - o Inheritance / Gifts

- Other Income

Country-Based Risk Assessment

The customer's country of residence plays a crucial role in determining their initial risk classification.

The system assigns a risk rating based on FATF recommendations and internal risk models:

- Negligence Risk (Low-Risk Countries) – Highly regulated jurisdictions with strong AML frameworks (e.g., Switzerland, Denmark, etc.)
- Low to Medium Risk Countries – Countries with stable regulatory environments and low financial crime risks (mainly EU based countries).
- Medium to High-Risk Countries – Jurisdictions with known AML deficiencies and limited regulatory oversight.
- High-Risk Countries – Countries under FATF monitoring or blacklisted jurisdictions (e.g., North Korea, Iran, Myanmar). Customers from these regions are automatically flagged for review and almost 100% account closure.

Risk-Based Customer Classification

Once all initial information is gathered and validated, the system assigns a preliminary risk score to the customer based on:

- Geographical risk factors (country of residence and nationality).
- Screening results (sanctions, PEP, and high-risk country status).

This risk score determines:

- Negligence-Risk Customers – Allowed to proceed without additional verification.
- Low-Risk Customers – Allowed to proceed without additional verification.
- Medium-Low-Risk Customers – Allowed to proceed without additional verification.
- Medium-Risk Customers – Subject to additional review before making transactions.
- High-Risk Customers – Subject to strict EDD requirements or account restrictions / account closure.

Additional Verification for Medium and High-Risk Customers

If a customer falls into the Medium, or High-Risk categories based on country risk or self-reported financial information, they must provide further details before their first deposit is processed. These additional verification steps include:

Enhanced Due Diligence (EDD) Requirements:

- Place of birth – To cross-reference with high-risk nationality lists.
- Nationality – To assess potential risk exposure from multiple citizenships.
- Identity number (National ID, Passport, or Driver's License) – For verification against government databases and fraud prevention measures.

By implementing this multi-layered Initial Risk Assessment, the company ensures that high-risk individuals are detected and assessed before engaging in financial transactions, gameplay, etc. thereby reducing exposure to money laundering risks while maintaining compliance with global AML/CFT regulations.

4.3.2. Risk Reassessment at 4,000 NAF Transaction Volume

Triggering the new Risk Assessment Process

Upon reaching a cumulative transaction threshold of 4,000 NAF (total deposits + total withdrawals), an automatic risk evaluation is triggered. This threshold applies to both deposit and withdrawal transactions combined. At this stage, a Customer Support or Payment Support agent initiates a Know Your Customer (KYC) verification, requiring proof of identity and proof of address. This step ensures compliance with AML/CFT regulations, strengthens fraud prevention measures, and facilitates a reassessment of the customer's risk profile.

KYC Verification Process

Acceptable Proof of Identity (POI) Documents. Customers must provide one of the following valid identity documents:

- Government-issued passport (biometric page visible)
- National ID card (front and back if applicable)
- Driver's license (front and back if applicable)
- Residence permit (for non-citizens residing in a country)
- Any other legally recognized government-issued identification

The POI document must:

- Be valid (not expired)
- Contain the customer's full name, date of birth, photograph, and unique identification number
- Be clear and readable, with no obstructions or modifications

Acceptable Proof of Address (POA) Documents. Customers must provide one of the following documents:

- Utility bill (electricity, water, gas, internet, or landline phone)
- Bank statement or credit card statement
- Government-issued residence certificate
- Tenancy agreement, accompanied by an official letter confirming residency
- Tax statement or letter from a tax authority

The POA document must:

- Clearly display the customer's full name and residential address
- Match the registered address in the customer's profile

Once KYC is successfully completed, a comprehensive risk reassessment is conducted using an automated quantitative risk-scoring model.

For a more detailed understanding of the risk-scoring model, please refer to the Company's CRA policy.

Final Summary

Each player will have an assigned risk profile that incorporates multiple factors, ensuring a comprehensive assessment of potential AML risks. Based on the Declared Monthly Deposit Amount criterion, transactional thresholds are established, and appropriate KYC and AML procedures are enforced accordingly. This risk-based approach enables the detection of suspicious financial activities and ensures compliance with international AML regulations.

The cumulative risk scoring model is calculated using a weighted formula, incorporating various criteria. This score determines the player's Inherent Risk Level, classified from Negligence to High.

Once this classification is determined, transaction limits and AML requirements are adjusted accordingly.

This enhanced framework ensures robust AML compliance while maintaining a frictionless user experience.

Assigning the Customer Risk Profile

After evaluating all criteria, the total Inherent Risk Score is calculated, and the customer is assigned a risk classification:

Risk Score	Risk Category
1-2	Negligence
2-3	Low
3-4	Medium Low
4-5	Medium
5+	High

4.3.3. Regular (periodical) risk reassessment

Frequency of Risk Reassessment

Risk reassessment is conducted at regular intervals based on the player's assigned risk level. The frequency of these reassessments ensures that any changes in player behaviour, financial transactions, or external risk factors are identified and addressed promptly.

Risk Reassessment Schedule:

- **Negligence/Low Risk – Every 18 months**
- **Medium Low / Medium Risk – Every 12 months**
- **High Risk – Every 6 months**

Impact of Risk Reassessment

Each reassessment is performed using the same 7 risk criteria, allowing for a dynamic evaluation of the player's risk profile. As a result of reassessment:

- The player's risk level may change, leading to adjustments in monitoring and compliance measures.
- The transactional limit for the player may be updated, ensuring risk-appropriate controls remain in place.
- Enhanced Due Diligence (EDD) measures may be triggered if an increase in risk is detected.

By implementing a structured risk reassessment process, we ensure ongoing compliance with AML regulations and proactively manage potential financial crime risks.

Once concrete period is triggered, a comprehensive risk reassessment is conducted using an automated quantitative risk-scoring model. For a more detailed understanding of the risk-scoring model, please refer to the Company's CRA policy.

Final Summary

Each player will have an assigned updated risk profile that incorporates multiple factors, ensuring a comprehensive assessment of potential AML risks. Based on the Declared Monthly Deposit Amount criterion, transactional thresholds are established, and appropriate KYC and AML procedures are enforced accordingly. This risk-based approach enables the detection of suspicious financial activities and ensures compliance with international AML regulations.

The cumulative risk score is calculated using a weighted formula, incorporating all seven criteria. This score determines the player's Inherent Risk Level, classified from Negligible to High. Once this classification is determined, transaction limits and AML requirements are adjusted accordingly.

This enhanced framework ensures robust AML compliance while maintaining a frictionless user experience.

Assigning the Customer Risk Profile

After evaluating all criteria, the total Inherent Risk Score is calculated, and the customer is assigned a risk classification:

Risk Score	Risk Category
1-2	Negligence
2-3	Low
3-4	Medium Low
4-5	Medium
5+	High

5. ONGOING MONITORING & TRANSACTION REVIEW

Ongoing Transaction Monitoring (OTM) is a critical component of the risk-based approach to Anti-Money Laundering (AML) compliance. It ensures continuous oversight of player activity and financial transactions to detect and mitigate potential risks. This monitoring process is proactive and dynamic, adapting to changes in customer behaviour and regulatory requirements.

Each player is assigned an individual transaction limit, beyond which an AML specialist conducts an in-depth review. This serves as a mitigation measure, ensuring early detection of suspicious activities and preventing financial crime.

Ongoing Transaction Monitoring consists of three progressive stages.

5.1. Continuous Monitoring

All player transactions undergo real-time monitoring through automated systems that flag unusual activities based on predefined risk criteria and reaching the maximum limit on transactions. The monitoring system also collect all key information's, including:

- Geographical Risk – The player's country of residence or business operation significantly impacts the risk level. High-risk jurisdictions include those identified by the Financial Action Task Force (FATF) as having deficiencies in AML/CFT controls. Players operating in or transacting with these jurisdictions face heightened scrutiny.
- Customer Profile Risk – This includes factors such as:
 - o Their source of wealth (e.g., salary, inheritance, business ownership, or high-volume investments).
 - o Associations with high-risk entities or industries.
- Transaction Risk – The frequency, volume, and complexity of transactions are carefully monitored. Key risk indicators include:
 - o Large, irregular transactions that deviate from historical patterns.
 - o Rapid movement of funds, particularly between unrelated accounts or jurisdictions.
 - o Structuring transactions to avoid AML reporting thresholds.
 - o Usage of multiple payment methods or third-party funding sources.
- Delivery Channel Risk – The method by which customers interact with the company affects risk assessment:
 - o Low risk: Deposits and withdrawals through regulated financial institutions (e.g., personal IBAN accounts, credit/debit cards linked to known banks).
 - o Medium risk: E-wallets and third-party payment providers that have robust AML controls.
 - o High risk: Anonymous funding methods such as cryptocurrency deposits, prepaid cards, or cash deposits through intermediaries.
- Product & Service Risk – The type of gaming products used can indicate potential financial crime risks:
 - o Low risk: Established betting markets, such as major football leagues (e.g., UEFA Champions League, English Premier League).
 - o Medium risk: Niche markets, such as esports or virtual sports betting.
 - o High risk: Small, regional sporting events with low visibility, which are vulnerable to match-fixing (e.g., local handball leagues, lesser-known tennis matches).

- Casino games risk: Unusual patterns in slots, poker, or live dealer games (e.g., a player closes almost the entire table in poker, erratic bet sizing, high turnover with no clear strategy).
- Behavioural Indicators – Player actions that may indicate an increased AML risk:
 - Frequent use of VPNs or proxy servers to mask their real location.
 - Multiple account registrations under different identities.
 - Refusal or delays in providing KYC documents.
 - Abrupt changes in deposit or withdrawal behaviour.
 - Unusual betting patterns that suggest syndicate betting or match-fixing.

5.2. AML Specialist Review

When a player's transactions exceed their pre-set individual transaction limit or trigger multiple risk indicators, an AML specialist conducts a detailed manual review. The review includes:

- Examining the customer's transaction history and comparing it with historical behaviour.
- Identifying suspicious activities, such as rapid fund movements or structuring transactions.
- Cross-checking against known high-risk indicators, including connections to flagged entities or jurisdictions.
- Reviewing gameplay patterns, such as the type of games played (slots, poker, sportsbook), playing behaviour, and financial engagement.
- Investigating payment methods, including frequency, payment providers, and withdrawal methods.

Following the review, the AML specialist may increase or decrease the player's risk level, adjust their transaction limit, or recommend further scrutiny, request additional documentation (including Source of Wealth).

5.3. Source of Wealth (SOW) Verification

If an AML review raises additional concerns, the final mitigating measure is a Source of Wealth (SOW) request. This process requires the player to provide supporting documentation demonstrating the legitimacy of their funds. Examples of acceptable documentation include:

- Bank statements showing the origin of funds.
- Tax declarations confirming income sources.
- Salary slips or employment contracts verifying occupational earnings.
- Investment records, property sale agreements, or business ownership documentation.

Failure to provide adequate documentation within a specified timeframe may result in account suspension, reporting to financial authorities, or other regulatory actions.

Ongoing Transaction Monitoring is a risk mitigation strategy that ensures continued compliance with AML regulations. The first level of mitigation is an in-depth AML specialist review upon hitting transaction thresholds. If concerns persist, the second level of mitigation is the Source of Wealth request, adding an additional layer of due diligence.

By employing this structured approach, the organization effectively minimizes exposure to illicit financial activities while ensuring a secure and compliant gaming environment.

6. Customer Due Diligence (CDD)

Customer Due Diligence (CDD) is a fundamental component of AML compliance, ensuring that casinos have a thorough understanding of their customers' identities, financial activities, and risk levels. The level of due diligence applied depends on the assessed risk associated with a particular customer. CDD measures are divided into Initial Customer Due Diligence (ICDD), Enhanced Due Diligence (EDD) for higher-risk customers, and Simplified Due Diligence (SDD) for low-risk customers.

6.1. Initial Customer Due Diligence (ICDD)

ICDD is conducted when a customer establishes a business relationship with the casino, which occurs when:

- A player opens an account.
- A player reaches a cumulative transaction threshold of NAf. 4,000 (including deposits and withdrawals).

ICDD Requirements

At the point of account creation, casinos must collect minimum personal details, including:

- Full name
- Permanent residential address
- Date of birth
- PEP (Politically Exposed Person) screening
- Sanctions screening

Once the NAf. 4,000 threshold is reached, additional CDD measures must be conducted, including a full customer risk assessment and identity verification.

Transaction Threshold Implications

- If the threshold is reached due to a deposit, the player can continue gaming but cannot make additional deposits or withdrawals until verification is complete.
- If the threshold is reached due to a withdrawal request, the account is fully frozen until verification is completed.
- If the required CDD documentation is not provided within 30 days, the casino must terminate the business relationship and assess whether to file a report with the Financial Intelligence Unit (FIU) for suspected money laundering or terrorist financing.
- If no suspicion of financial crime exists, funds should be returned to the same bank account or wallet they were originally deposited from.

6.2. Enhanced Due Diligence (EDD)

Enhanced Due Diligence (EDD) applies to higher-risk customers or transactions that pose increased money laundering or terrorist financing risks. A risk-based approach determines when EDD is necessary.

Triggers for EDD:

- **Geographical Risk:** The customer is a resident of a jurisdiction with weak AML regulations (e.g., FATF high-risk countries, or countries under monitoring).
- **Anonymity-Favouring Products:** Use of anonymous payment methods such as prepaid cards or privacy-focused cryptocurrencies.
- **Unusual Transaction Patterns:** Large, rapid, or structured transactions that appear inconsistent with a customer's profile.

- New Business Practices or Technologies: Customers engaging with new or high-risk financial instruments or payment channels.

EDD Measures

When EDD is required, the casino must conduct additional checks, including:

- Obtaining further customer details, such as occupation, previous address, and information available in public databases.
- Determining the source of funds (SOF) or source of wealth (SOW) to validate the legitimacy of the customer's financial activity. Acceptable sources include:
 - o Salary payments (employment contracts, payslips)
 - o Pension releases
 - o Inheritance or legal settlements
 - o Property or asset sales
 - o Gambling winnings, etc.
- Requesting justification for transactions exceeding predefined thresholds.
- Requiring senior management approval before establishing or continuing a high-risk business relationship.
- Implementing enhanced transaction monitoring, including increased frequency of reviews.

For high-risk players, periodic SOW checks may be required, even when no suspicious transactions occur.

6.3. Simplified Due Diligence (SDD)

Simplified Due Diligence applies to lower-risk customers where the risk of money laundering or terrorist financing is minimal. A casino may use SDD in cases where:

- The customer is from a jurisdiction with strong AML oversight.
- The customer has a transparent financial background.
- The type of gaming activity does not present significant risk.

SDD Measures

- Limiting the collection of personal information to only essential details.
- Delaying identity verification until the customer reaches the threshold.
- Using alternative verification methods, such as third-party databases, instead of requiring official documentation.
- Reducing the frequency of customer risk reviews.
- Lowering the intensity of ongoing transaction monitoring, within reasonable limits.

SDD cannot be applied in cases where:

- There is a suspicion of money laundering or terrorist financing.
- A customer falls into a higher-risk category, than Negligence, Low or Medium-low risk categories.

6.4. Mitigation and Ongoing Monitoring

CDD is not a one-time process; it requires continuous assessment and updates. If new risk factors emerge, the casino must adapt its due diligence measures accordingly.

- First-line mitigation: If risk indicators are flagged, an AML specialist reviews the case.

- Second-line mitigation: If concerns persist, the casino requests Source of Wealth (SOW) verification to ensure financial legitimacy.
- Final action: If a customer fails to comply with CDD or presents a high financial crime risk, the casino may terminate the business relationship and report to regulatory authorities.

By implementing robust CDD procedures, casinos can proactively identify and mitigate financial crime risks, ensuring compliance with AML regulations while maintaining a secure and transparent gaming environment.

7. TRANSACTION MONITORING AND REPORTING

During its business activity, the Company follows strict reporting procedures to detect and report unusual transactions. These procedures include:

- Recognition of unusual transactions
- Documentation of unusual transactions
- Reporting of unusual transactions to the authorities.

7.1. Recognition of unusual transactions

An unusual transaction is a transaction inconsistent with the Client's profile. Therefore, the first key to recognizing that a transaction or series of transactions is unusual is to know enough about the Client. The purpose of collecting Client information is to assess the risk that may be associated with the Client and to build a Client's profile to assess how the Client is going to act within the framework of the business relationship.

During its cooperation with the Client, the Company collects relevant information about the Client to recognize unusual transactions.

7.1.1. The Company provides its Employees with the corresponding mandatory training programs and guidelines that enable them to recognize any unusual transaction, document and immediately report to the Compliance Officer about such.

7.1.2. All these unusual transactions must be reported to the Compliance Officer in the format approved by management. All additional documents available, such as copies of identification documents, cash out slips, and other records must be also submitted as supplements. The Compliance Officer shall keep an adequate filing system of these records.

7.1.3. If internally reported transactions are not reported to the Financial Intelligence Unit ("FIU") by the Company, the reasons therefore shall be adequately documented and signed off by the Compliance Officer and/or Company's management. In order to implement FATF recommendation, the Company pays special attention to all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

7.1.4. The Company recognizes the following transactions as unusual:

- Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;
- Transactions involving individuals or entities indicated on international sanction lists;
- Presumed money laundering transactions or terrorist financing: transactions where there is cause to presume that they can be related to money laundering or terrorist financing;
- Transactions in the amount of NAf. 5,000 or more, regardless whether the transaction is made in cash, by check or other form of payment, or through electronic or other non- physical means. This includes but is not limited to:
 - A cashless transaction in the amount of NAf. 5,000 or more. A cashless transaction is a transfer from a bank account of the casino to a local or international bank account, at the request of the client.
 - Accepting or releasing a deposit in the amount of NAf. 5,000 or more at the request of the client;
 - Sale to a customer of chips in the amount of NAf. 5,000 or more. "Chips" include but is not limited to tokens and credits.
 - A cash out in the amount of NAf. 5,000 or more;

Note: A transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount of the monetary equivalent of NAf. 5,000 or more and is considered per gaming day.

7.1.5. The following is a list of possible red flags which the Employee should consider before taking a decision on making a report to MLRO:

- Client does not cooperate in the carrying of CDD;
- Client attempts to register more than one account;
- Client deposits considerable amounts during a single session by means of multiple pre-paid cards;
- Client deposit funds well in excess of what is required to sustain his usual betting patterns;
- Client makes small wagers even though he has significant amounts deposited, followed by a request to withdraw well in excess of any winnings;
- Client makes frequent deposits and withdrawal requests without any reasonable explanation;
- Noticeable changes in the gaming patterns of the Client, such as when the Client carries out transactions that are significantly larger in volume when compared to the transactions he normally carries out;
- Client enquires about the possibility of moving funds between accounts belonging to the same gaming group;
- Client carries out transactions which seem to be disproportionate to his wealth, known income or financial situation;
- Client seeks to transfer funds to the account of another Client or to a bank account held in the name of a third party;
- Client displays suspicious behaviour in playing games that are considered as high risk.

7.1.6. The Company employs automated transaction monitoring systems to support the identification of suspicious activities. These systems are designed to flag transactions based on predefined risk indicators, thresholds, and behavioral patterns. Alerts generated by the system are reviewed by trained compliance personnel, who assess the relevance and severity of each case.

7.1.7. Every unusual transaction shall be properly recorded and documented, including:

- Client details and transaction records;
- Copies of identification documents and receipts;
- Any other supporting documents.

7.2. Regulatory Reporting Obligations and Compliance measures

The Company immediately reports unusual transactions to the Financial Intelligence Unit, providing all necessary supporting documents. For this purpose, the Company has clear procedures for both internal and external reporting of unusual transactions, which shall be communicated to its Employees.

All unusual individual transactions or series of transactions, as mentioned in the Regulation Indicators Unusual Transactions, must be reported internally, without any delay. Also supporting documents must be submitted as part of the reporting.

Company uses the goAML reporting portal, through which Company prepares and submits reports (incl. bulk reporting) on unusual transactions, along with all supporting documents in English.

Company and its Employees are legally protected from any liability when reporting unusual transactions to the Financial Intelligence Unit.

7.3. Prohibition of disclosure

Company and its senior management and employees shall not disclose any details or information in connection with a report filed to the FIU or a request for information made by the FIU.

They are not permitted to disclose information to the customer nor to third parties. The reason for this is not to jeopardize an analysis or investigation into Money laundering or Terrorist financing. This is also the reason why caution is advised when a casino takes action to terminate a relationship or otherwise block additional transactions following reporting to the FIU.

Drastic action should only be taken when there is no other way out, since any unjustified action may alert the player. In such circumstances, it would be more advisable to increase on-going monitoring and submit additional reports to the FIU on any other suspected instances of ML/TF.

7.4. Record-Keeping and Documentation Requirements

The Company retains any data, information, documents and records associated with the business relationship with the Client (due diligence information, including copies or records of passports, identity cards, driving licenses or similar documents, information on suspicious activity reports made to the authorities, or suspicious activity which was reported internally by staff and subsequently not required to be reported to the authorities, having been analysed by the MLRO, etc.) for a period of 5 (five) years after the business relationship with the Client is ended, or after the date of the occasional transaction.

The Company ensures that information and transaction records (both domestic and international) it retains are:

- sufficient to permit reconstruction of individual transactions as to provide, if necessary, evidence for prosecution of criminal activity;
- available to domestic competent authorities based upon appropriate legal authority;
- shall be presented to the officials upon request.

Format of record-keeping:

- original documents;
- photocopies or scans of original documents;
- computerized or electronic form records;
- electronic files or hard copies of the results of electronic/subscription services checks carried out.

Access to retained information, documents and records is strictly restricted to authorized Company's personnel who necessarily require it for their official duties. The Company employs robust security measures, including access restrictions, authentication systems, encryption, and user activity monitoring, to ensure the confidentiality and integrity of stored data. Any unauthorized access or disclosure constitutes a violation that may result in disciplinary action or legal consequences.

As the Company collects and retains personal data in the course of its business activity while cooperating with its Clients, all data processing shall be conducted lawfully, transparently, and with appropriate safeguards to ensure data security and confidentiality. Personal data shall be handled strictly within the scope of legal and regulatory requirements.

Personal data shall be collected, processed, and retained solely for the purpose of compliance with AML and CTF regulations. It shall not be used for any other purposes unless explicit consent has been obtained from the data subject, or if such is directly required by law.

All collected personal data shall be stored in a secure environment, with appropriate technical and organizational measures in place to prevent loss, alteration, unauthorized access, or misuse. To safeguard data, the Company implements different data protection methods and tools, such as encryption, access control mechanisms, and backup systems, etc.

Where the Company engages third-party service providers for data storage and/or data processing, such providers are contractually obligated to maintain equivalent high levels of data security and confidentiality. The Company ensures that all engaged third parties adhere to strict data protection standards.

Employees who handle personal data undergo mandatory training on data protection principles, internal security policies, and best data protection practices. This ensures compliance with all legal and organizational data security requirements.

In the event of unauthorized access, data loss, or security breaches, Employees must immediately report the incident to the Compliance Officer. The Company will take appropriate remedial actions to mitigate risks, prevent further breaches, and, where necessary, notify relevant authorities.

Personal data is retained for a period of five (5) years after the business relationship with the Client is ended, or after the date of the occasional transaction. After this period, the data shall be securely deleted, anonymized, or otherwise rendered inaccessible, unless a longer retention period is directly required by law. The deletion process ensures that data cannot be reconstructed or retrieved.

8. COMPLIANCE AND INTERNAL CONTROLS

8.1. Compliance measures

It is the policy of the Company to implement and maintain comprehensive written policies and procedures that clearly articulate its commitment to preventing the misuse of its operations, services, and products for the purposes of money laundering, terrorist financing, or the proliferation of weapons of mass destruction. These policies and procedures form the foundation of the Company's Anti-Money Laundering (AML), Counter-Financing of Terrorism (CFT), and Counter-Proliferation Financing (CPF) program and reflect the Company's adherence to the applicable legal and regulatory framework in Curacao.

The basic elements Company implements in an anti-money laundering compliance program are:

- A system of internal policies, procedures and controls;
- A designated compliance officer with day-to-day oversight over the AML program;
- An employee screening program and ongoing employee training program; and
- An independent audit function to test the AML program

The Company maintains a structured process for monitoring legal and regulatory developments to ensure all compliance policies and procedures remain current and responsive to changes in the risk landscape and regulatory environment.

All compliance measures are formally documented, and any amendments to policies or procedures shall be approved by senior management or the Board of Directors. The approved documentation must be accessible to relevant staff at all times and be effectively communicated throughout the organization. This ensures that all employees are fully informed of their obligations and the internal expectations for behavior and conduct.

As part of its compliance framework, the Company maintains and applies the following core policies and procedures:

- Business Risk Assessment Policy
- Customer Risk Assessment Policy
- Customer Due Diligence Policy
- Record Keeping Procedures
- Reporting Procedures
- Customer Acceptance Policy
- Customer Risk Assessment Procedures
- Internal Controls, Governance, and Compliance Management Policy
- Communication, Employee Training, and Employee Screening Procedures and Guidelines

These documents serve to:

- Define how the Company identifies and mitigates business and customer-specific risks;
- Establish clear protocols for onboarding and verifying customers;
- Ensure proper documentation, reporting, and retention of client and transactional data;
- Promote consistent internal control mechanisms and effective governance; and
- Provide structured processes for employee training, awareness, and integrity screening.

The Company's compliance function is supported by a designated Compliance Officer, who is responsible for overseeing the application and effectiveness of all policies and internal controls, and for reporting any deviations from expected practices. These internal controls are designed to enable early detection of unusual activity and ensure timely intervention and reporting to the appropriate authorities when necessary.

8.2. Implementing Risk Mitigation Controls

As part of its ongoing commitment to combat money laundering, terrorist financing, and the proliferation of weapons of mass destruction, the Company implements a structured system of risk mitigation controls. These controls are designed to identify, assess, manage, and minimize risks that may arise in the course of business operations, and are integral to the Company's broader AML/CFT/CPF compliance framework.

Risk mitigation controls are embedded into all relevant operational processes and are applied proportionately to the level and nature of the identified risk. These controls are tailored to address both inherent and emerging risks associated with clients, products, services, delivery channels, and geographic exposure.

Key Elements of Risk Mitigation Controls:

- Client Risk Assessment and Risk-Based Approach (RBA). All clients are subject to risk profiling based on predefined risk indicators. Enhanced due diligence measures are applied to high-risk clients, while simplified procedures may be used for low-risk profiles, in accordance with applicable legislation.
- Transaction Monitoring Controls. The Company uses both automated tools and manual review procedures to monitor customer transactions for suspicious or unusual activity. Patterns inconsistent with the customer's known profile are subject to further scrutiny and escalation.
- Escalation and Reporting Procedures. When a transaction or client behavior triggers a red flag, an internal reporting mechanism is activated. Designated employees report the activity to the Compliance Officer using approved formats. If warranted, the Compliance Officer evaluates and submits a report to the Financial Intelligence Unit (FIU) of Curacao.
- Segregation of Duties and Internal Oversight. Roles and responsibilities related to the AML/CFT/CPF framework are clearly defined and segregated to ensure independent oversight. Employees responsible for client onboarding, transaction processing, and compliance oversight operate under a system of internal checks and balances.
- Control Reviews and Updates. Risk mitigation controls are reviewed regularly to ensure they remain effective and relevant. Controls may be revised in response to internal audits, regulatory inspections, operational incidents, or emerging industry typologies.
- Sanctions Screening and Watchlist Monitoring. Clients and transactions are routinely screened against local and international sanctions lists, including those maintained by the United Nations, European Union, OFAC, and other competent authorities. Any matches or alerts are subject to immediate review and escalation.
- Recordkeeping of Risk Assessments and Controls. All risk assessments, monitoring outcomes, control adjustments, and reporting activities are documented and retained in accordance with legal recordkeeping obligations. These records support transparency and enable auditability by competent supervisory authorities.
- Control Testing and Independent Review. The effectiveness of risk mitigation controls is assessed through internal compliance reviews and independent audits. Any deficiencies identified are documented and addressed with corrective action plans, which are tracked and reported to senior management.

8.3. Periodic Review and Adjustment of Risk Policies and Procedures

The AML compliance program must be monitored and evaluated at least annually by an adequately resourced internal audit department or an outside independent party. The audit must be independent,

thus performed by people not involved with the company's compliance staff. Those performing the audit must be sufficiently qualified to ensure that their findings and conclusions are reliable.

These tests must include at least:

- An evaluation of the company's anti-money laundering, counter terrorist financing and counter terrorist financing and counter financing of proliferation manuals;
- Customer's file review;
- Compliance management;
- Performance of transaction testing;
- Assessment of training adequacy;
- Assessment of compliance with applicable laws and regulations;
- Evaluation of the system's ability to identify unusual activity;
- Interviews with employees who handle transactions and with their supervisors;
- A sampling of unusual transactions on and beyond the threshold(s) followed by a review of compliance with the internal and external policies and reporting requirements; and
- An assessment of the adequacy of the record retention system.

The audit team should also consider whether the board was responsive to earlier audit findings.

The scope of the testing and the testing results must be documented, with any deficiencies reported to senior management and/or the Board of Supervisory Directors, and to the designated officers with a request to take prompt corrective actions by a certain deadline. These corrective actions could also include enhancement of controls and procedures.

9. EMPLOYEE SCREENING, TRAINING AND AWARENESS

9.1. AML Training Programs strategy and importance

Under the leadership of the MLRO the Company develops ongoing employee training programs for all employees, including those who handle unusual transactions.

Training includes setting out rules of conduct governing employees' behavior and their ongoing education to create awareness of the casino's policies against money laundering and terrorist financing. Most areas of the institution should receive training, and the target audience should include most employees. But each segment should be trained on topics and issues that are relevant to them. Training must at least address the following topics:

- New Employees:
 - The nature and process of ML and TF;
 - Internal policies, procedures, and reporting requirements;
 - ML risks and trends in the Company's business sector;
 - Customer due diligence and indicators for identifying unusual transactions.

A general training of the nature and process of ML and TF and the need to report any unusual transactions to the appropriate designated officer shall be provided to all new Employees who will handle Clients or their transactions, irrespective of their level of seniority.

Employees shall be made aware of the existing internal policies, procedures and regulations concerning ML, TF, proliferation of weapons and the reporting requirements. They shall also be trained on the ML methods and trends in the gambling sector. Employees shall receive an explanation on customer due diligence and objective and subjective indicators for reporting unusual transactions.

- Dealers, Cashiers, and Slot Department Personnel:
 - A general AML course covering the role in identifying suspicious activity;
 - Training on how money launderers use casinos for ML.
 - Instruction on internal reporting procedures and Client' identity verification.

Dealers, Cashiers, and Slot Department staff are the Company's first line of defense against ML. They shall complete a basic training course to understand why AML is important and learn the key concepts. They also shall have extra training on how criminals may try to use the Company for ML. Additionally, they shall be familiar with the Company's procedures so they know exactly what to do if they spot suspicious activity. Personnel involved with Client's account opening shall be learnt about how to understand the need to verify the identity of the Client.

- Audit Staff:
 - Regulatory updates and enforcement actions.
 - New ML methods and trends.
 - Their role in ensuring ML compliance within the Company.

Those Employees charged with overseeing, monitoring and testing ML controls shall also be trained about changes in regulation, ML methods and enforcement, and their impact on the Company.

- AML Compliance Staff:

- Advanced AML regulations and risk management strategies;
- Updates on new ML trends and techniques;
- Attendance at industry conferences and specialized AML training sessions.

These are the Employees who run the AML program. They will have specialized training to be able to stay on top of new trends or changes that impact the Company and the way it manages risk. This requires attending conferences or AML-specific presentations to go into greater detail.

- Supervisors and Managers:

- Comprehensive knowledge of AML/ CFT policies, procedures, and regulations;
- Leadership responsibilities in enforcing AML compliance.

A higher level of instruction covering all aspects of money laundering, terrorist financing policies, procedures and regulations must be provided to those Employees with the responsibility to supervise or manage the staff.

- Senior Management and Board of Directors:

- The risks and reputational damage associated with ML.
- Their oversight role in ensuring regulatory compliance.

ML issues and dangers shall be regularly and thoroughly communicated to the board. This to keep board members aware of the reputational risk that ML poses to the Company.

The Company develops training or contact for it. Delivery of the training may include educational pamphlets, videos, in-person lectures and explanatory memos.

Regular refresher training shall be provided to ensure Employees stay informed of evolving ML methods and regulatory changes. By ensuring a well-structured training program, the Company can effectively mitigate financial crime risks and comply with AML/CFT obligations.

To demonstrate compliance with aforementioned staff training guidelines, the Company maintains records that include:

- Details on the content of the training programs;
- The names of the staff members who have received the training;
- The date on which the training was provided;
- The results of any testing carried out to measure staff understanding of ML and TF requirements;
- An ongoing training plan.

9.2. Employee screening

The Company shall adhere to its policies and procedures for screening its Employees for criminal records and other AML requirements to ensure that Company's business is conducted to a high ethical standard and that all laws and regulations pertaining to financial transactions are followed. To minimize the risk of financial crime and illicit activities, the Company requires all Employees to undergo comprehensive background checks before and during their employment.

To assess the suitability of Employees from an AML perspective, the Company will apply the following due diligence procedures:

- Evaluation of Professional Competence and Qualifications:

The Company will verify that each employee possesses the necessary qualifications, expertise, and training to perform their role effectively. This includes ensuring that the individual has completed required AML and anti-fraud training in accordance with industry best practices and regulatory requirements. References from previous employers may be obtained to assess professional conduct, work history, and adherence to compliance standards. Where applicable, verification of academic and professional credentials will also be conducted, particularly for Employees in roles involving financial oversight or access to sensitive operational data.

- Assessment of Character and Integrity:

All Employees will be subject to thorough background screening to evaluate their integrity and conduct. This process may include a criminal record check to confirm that the individual has no prior convictions for financial crimes, fraud, money laundering, or other offenses that could pose a risk to the Company. Additionally, candidates may be screened for any negative media exposure, including adverse mentions in public records, news reports, and social media, which may indicate past unethical behavior or financial misconduct. The Company may also review applicants against global sanctions lists, politically exposed persons (PEPs) databases, and other relevant sources in accordance with international AML compliance obligations.

- Ongoing Monitoring and Reporting:

The Company will conduct periodic reviews of Employees to ensure continuous compliance with AML policies. This process may include updated criminal background checks, reassessment of media and public records, and verification that employees remain in compliance with internal AML procedures.

Employees play a crucial role in maintaining the integrity of the Company's AML framework. They are expected to follow all established AML policies, exercise due diligence in their duties, and report any suspicious activity in accordance with internal procedures. Any Employee found to be negligent in their AML responsibilities or involved in misconduct will face disciplinary action, up to and including termination. Engaging in activities that facilitate money laundering or intentionally disregarding AML policies is strictly prohibited. Employees must also maintain strict confidentiality regarding Know Your Customer (KYC) data, transaction monitoring, and all other AML-related procedures in line with the Company's privacy and data protection policies.

The Company will regularly review and update its AML procedures and Employee screening processes to align with evolving regulatory requirements and international AML standards. Ongoing training will be provided to Employees to ensure they remain informed of the latest AML developments, compliance obligations, and best practice.

SIGNED AND APPROVED:

C. Drommond

// EMOORE N.V., MANAGING DIRECTOR

DATED: APRIL 08, 2025

