

Rozairo N.V

AML/CFT Policy

Approved by the Board of Directors
December 2024

Abraham de Veerstraat 1

A handwritten signature in blue ink, appearing to read 'Theoddis Andreadis', written over a horizontal line.

Theoddis Andreadis
Director
15/01/2024

Contents:

- 1. Purpose of the Policy**
- 2. Online Gaming Industry Specifics**
- 3. Key Definitions**
- 4. Money Laundering**
- 5. Terrorism Financing**
- 6. Risk- Based Approach (ML/ TF risks' detection)**
- 7. Customer Due Diligence (CDD, EDD)**
- 8. Transaction Monitoring**
- 9. PEPs**
- 10. Sanctions Management, FATF blacklist, license restrictions**
- 11. Suspicious Activity Reporting Guidelines**
- 12. Money Laundering Reporting officer (MLRO)**
- 13. Senior Management Responsibility**
- 14. Employee Training Policy**
- 15. Record Keeping**
- 16. AML Compliance Audit**

1. Purpose of the Policy

The purpose of the **Anti-Money Laundering Policy (the AML Policy)** is to combat money laundering and terrorism financing, implement best AML/CFT industry standards, and promote company-wide compliance with the local and international Anti-Money Laundering/ Counter Terrorism Funding (AML/CFT) legislation. The AML Policy's uniform framework is based on robust AML/CFT measures, including the identification and mitigation of the inherent risks associated with customers, products and services, payment methods, countries, and delivery channels.

The design, implementation, and monitoring of the AML policy's framework is approved by approved by the Company's Board of Directors (BoD) and is subject to an annual review. In addition to the annual review process, the AML Policy may be amended from time to time to reflect material changes in the AML/CFT legislation or operator practices. Furthermore, a nominated officer may put forward suggestions to Implement urgent internal and third-party AML audit recommendations as regards risk probability and risk impact.

First and foremost, the AML Policy is a reflection of the main international objectives highlighted by the current AML/ CTF legislation in Curacao i.e. the upcoming National Ordinance for Games of Chance (LOK), the Criminal Code of Curacao, The National Ordinance on Offshore Games of Hazard (PB 1993, no.63) (NOOGH) as well as National Ordinance Penalization of Money Laundering (NOPML), the National Ordinance on the Reporting of Unusual Transactions (NORUTO), and the National Ordinance on Identification of clients «hen Rendering Services (NOIS).). The AML Policy also reflects the international legislation and policy initiatives such as Recommendations of the Financial Action Task Force (The **FATF** Recommendations), the European Anti-Money Laundering Directives (the 4th, 5th and the 6th AML Directives) , and the Wolfsberg Principles.

To summarize, the AML Policy was drafted with the view of complying with the recommendations of the AML/CFT supervisor in Curacao, namely the Curacao Gaming Control Board. The Company's directors, officers, and personnel are committed to upholding the set of standards set in the Policy. The Policy applies to all persons at all levels working for the Company and third-party consultants whose services are enlisted from time to time for audit purposes.

2. Online Gaming Industry Specifics

Rozario N.V. is a Curacao-based legal entity, which currently runs the following websites:

Pampago.com

Vaivalendo.com

3. Key Definitions

AML Policy- The Policy on Prevention of Money-Laundering Terrorist Financing.

Anti-Money Laundering and Courter-Financing of Terrorism Program: programs are established to fight against money laundering and terrorist financing and consist of written internal policies, procedures and controls, overseen by AML compliance team headed by: MLRO, who is also responsible for AML training as well as arranging an independent review to audit the program.

Alert : a notification that an analysis of red discrepancies is required based on defined red flags and underlying typologies.

AML/CFT Supervisor: the Curacao Gaming Control Board (GCB) and a relevant local master license holder where applicable.

Automated Screening Tool (AST): Software systems that automate the customers' screening process including against sanctions lists.

Beneficial Owner : a natural person who ultimately owns or controls an account through which a transaction is being conducted.

Blacklist: An internal list of names (Including places, persons, entities, and individuals) that are screened to identify any sanctions exposure, in addition to government and vendor-maintained sanctions lists.

The FATF blacklist: is a list of countries that FATF has determined are noncooperative in the international fight against money laundering and terrorist financing.

Comprehensive Sanctions: Sanctions that prohibit all transactions and activity with a sanctioned country by the sanctioning country except in rare, specific instances.

Criminal Proceeds: Any property derived from or obtained, directly or indirectly, through the commission of a crime. **Customer-** a person that opens an account and transacts with the Company.

Customer Relationship: a customer relationship encompasses all contact with a prospective customer during onboarding and while using the Company's services and products.

Customer Due Diligence: a set of internal controls that internet gambling operator establish a customers' identity, predict with relative certainty the types of transactions in which the customer is likely to engage, and assess the extent to which the customer exposes it to a range of risks (i.e., money laundering and sanctions). Organizations also need to Know their customers through CDD to guard against fraud and comply with the requirements of relevant legislation and regulation.

'High-risk third country': a third country, which is flagged by the European Commission under the provisions of paragraph (2) of Article 9 of the EU Directive by means of delegated powers and by FATF, and which has strategic deficiencies in its national AML/CFT regime that pose significant threats to the financial system of the Union, and a third country which is classified by the Company as high risk, according to the risk assessment referred to in Article 58a of the Law. **Due diligence-** The investigation and examination of a company or group, conducted in the process of preparing for a business transaction. Due diligence should be completed before entering into any financial transaction or business relationship.

Economic Sanctions: The imposition of trade or financial restrictions and penalties by one or more countries against another country, entity, or individual with the purpose of changing a behavior. Economic sanctions can include actions such as tariffs, trade restrictions, and financial limitations.

Egmont Group of Financial Intelligence Units -The Egmont Group consists of a numerous national of financial intelligence units (FIUs) that meet regularly to find ways to promote the development of FIUs and to cooperate, especially in the area of information exchange, training and the sharing of expertise. The goal of the group is to provide a forum for FIUs to improve cooperation in the fight against money laundering and the financing of terrorism, and to foster the implementation of domestic programs in this field.

Embargo : an official government action to ban trade or commercial activity with a specific country, sometimes involving a specific trade product (e.g., a grain embargo or an oil embargo).

Enhanced Due Diligence (EDD): In conjunction with Customer Due Diligence, EDD calls for additional measures aimed at identifying and mitigating the risk posed by higher risk customers. It requires developing a more thorough knowledge of the nature of the customer, the customer's business and understanding of the transactions in the account than a standard or lower risk customer.

European Union (EU): The modern EU was founded in the Treaty of Maastricht on European Union, signed in 1992 and effective in 1993. The EU is a politico-economic union of member states located primarily in Europe. European Union Directive on Prevention of the Use of the Financial System for the Purpose of money Laundering and Terrorist Financing- First adopted by the European Union in June 1991 and updated in 1997, 2005, 2015, 2018 and 2020 the directive requires EU member states to prohibit and manage the risks of money laundering and terrorist financing.

Exclusions List : A list of names that are excluded from the screening process. These are names that the compliance team has verified do not actually match a name on a sanction list.

Financial Action TaskForce (FATF) :FATF was created in 1989 by the Group of Seven industrial nations to foster the establishment of national and global measures to combat money laundering. It is an international policy-making body that sets anti-money laundering standards and counter- terrorist financing measures worldwide. Its Recommendations do not have the force of law. 35 countries and two international organizations are members. In 2012, FATF substantially revised its 40 + 9 Recommendations and reduced them to 40. FATF develops annual typology reports showcasing current money laundering and terrorist financing trends and methods.

Financial Intelligence Unit (FIU): A central national agency responsible for receiving, analyzing, and transmitting disclosures on suspicious transactions to appropriate authorities.

First Line of Defense- within the governance structure of a sanctions compliance program, the first line of defense (also referred to as the "front line") includes relationship managers and other customer-facing employees who are closest to the customers and counterparties during the onboarding and contacting phase of relationships. The first-line defense is responsible for ensuring that adequate information is obtained so that effective screening of customers and their owners and controllers can be performed. In general, the first-line defense owns and manages the collection of SDD information.

Greylist: A greylist is a list of entities that are suspicious or higher-risk for causing a negative impact to a firm. Within the context of sanctions, the greylist includes the names of countries with strategic deficiencies in anti-money laundering and counterterrorism financing regimes. Moreover, these countries have also not made sufficient progress or otherwise committed to action plans to address deficiencies identified by FATF.

Minor — under the 18 years of age.

Inherent Risk- The level of sanctions risks that exist before controls are applied to mitigate them. There are four main inherent risk categories: customers, products and services, countries, and delivery channels. Inherent risk is linked to the risk assessment process, which evaluates the effectiveness of an institution's risk controls. Inherent risk considers the likelihood and impact of noncompliance prior to considering any mitigating effects of risk management processes.

Investigation: The process of obtaining, evaluating, recording, and storing information about an individual or legal entity with whom one is conducting business, in response to an alert indicating a possible sanctions violation. Investigations often begin with simple checks before progressing to further investigation such as account review, customer outreach, and possible escalation to the compliance function.

Know Your Customer (KYC): Anti-money laundering policies and procedures used to determine the true identity of a customer and the type of activity that is 'normal and expected,' and to detect activity that is "unusual" for a particular customer.

Know Your Employee (KYE): Anti-money laundering policies and procedures for acquiring a better knowledge and understanding of the employees of an institution for the purpose of detecting conflicts of interests, money laundering, past criminal activity and suspicious activity.

Layering- The second phase of the classic three-step money laundering process between placement and integration, layering involves distancing illegal proceeds from their source by creating complex levels of financial Transactions designed to designed the audit trail and to provide anonymity.

Mandatory Sanctions Lists: Supranational sanctions lists, such as those including targets designated by the United Nations Security Council Resolutions (UNSCR), which must be screened against. Depending on the country in which a business is located and operates, local sanctions regimes may be required (i.e., mandatory') and would need to be included within a firm's sanctions compliance program.

Money Laundering: The process of concealing or disguising the existence, source, movement, destination or illegal application of illicitly - derived property or funds to make them appear legitimate. It usually involves a three part system: placement of funds into a financial system, layering of transactions to disguise the source, ownership and location of the funds, and integration of the funds into society in the form of holdings that appear legitimate. The definition of money laundering varies in each country where it is recognized as a crime.

Money Laundering Reporting Officer (MLRO): A term used in various international rules to refer to the person responsible for overseeing a firm's anti-money laundering activities and program and for filing reports of suspicious transactions with the national FIU. The MLRO is the key person in the implementation of anti-money laundering strategies and policies.

Monitoring: An element of an institution's anti-money laundering program in which customer activity is reviewed for unusual or suspicious patterns, trends or outlying transactions that do not fit a normal pattern. Transactions are often monitored using software that weighs the activity against a threshold of what is deemed 'normal and expected' for the customer.

Office of Foreign Assets Control (OFAC): the agency within the US Department of the Treasury responsible for administering and enforcing economic sanctions issued as part of US foreign policy and by international organizations like the United Nations against targeted foreign countries. It often works in consultation with other agencies, such as the Department of State, to oversee national security goals. A core component of the agency's responsibilities is the creation and maintenance of the Specially Designated Nationals (SDN) list.

Politically Exposed Person (PEP) : According to FATFs revised 40 Recommendations of 2012, a PEP is an individual who has been entrusted with prominent public functions in a foreign country, such as a head of state, senior politician, senior government official, judicial or military official, senior executive of a state-owned corporation or important political party official, as well as their families and close associates. The term PEP does not extend to middle- ranking individuals in the specified categories. Various country regulations will define the term PEP, which may include domestic as well as foreign persons.

Red Flag (similar to alert): A warning signal that should bring attention to a potentially suspicious situation, transaction or activity.

Regulatory Agency: A government entity responsible for supervising and overseeing one or more categories of financial institutions. The agency generally has authority to issue regulations, to conduct examinations, to impose fines and penalties, to curtail activities and, sometimes, to terminate charters of institutions under its jurisdiction.

Risk Appetite: The amount of risk that a firm is willing to accept in pursuit of value or opportunity. A firm's risk appetite reflects its risk management philosophy and comfort level for undertaking business in situations in which there could be an elevated sanctions risk. In turn, risk appetite influences the firm's culture and operating style and guides resource allocation. An organization's risk appetite is determined through the risk-assessment process and formalized in a Risk Appetite Statement or Framework. A business should determine its risk appetite based on the resources it has to invest in controls, staffing and measures to protect its reputation. Firms can have an overarching risk appetite (i.e., enterprise-wide) and/or have risk appetites defined on a more granular level (e.g., by department).

Risk Assessment: A tool that allows a business to identify and assess the extent to which it may be exposed to risks.

Risk-Based Approach: The assessment of the varying risks associated with different types of businesses, clients, accounts and transactions to maximize the effectiveness of an anti-money laundering program.

'Senior Management : an officer or employee of the Company with sufficient knowledge of the Company's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure and need not to be a member of the Board of Directors.

'Structuring" : small transfers or small deposit amounts from customers that are trying to avoid recordkeeping requirements or trigger AML flag alerts from any company (EMI).

Sanctions- Sanctions are punitive or restrictive actions taken by individual countries, regimes, or coalitions with the primary purpose of provoking a change in behavior or policy. Sanctions can restrict trade, financial transactions, diplomatic relations, and movement. They can be specific or general in their implementation and enforcement. Sanctions are also referred to as restrictive measures.

Sanctions Evasion- The deliberate attempt to remove or conceal the involvement of sanctioned places, entities, or individuals in a transaction or series of transactions. When sanctions evasion is successful, a business that would have been flagged, taxed, restricted, or prohibited is allowed to proceed unhindered.

Sanctions Due Diligence (SDD) - A similar process to Know Your Customer (KYC) / Customer Due Diligence (CDD) that focuses on the risks specific to sanctions, taking into account governance and risk assessment. SDD builds upon the KYC/CDD information an organization collects as part of its existing AML program. SDD is applied throughout the life cycle of a relationship at the start of a relationship (i.e., onboarding); when new products are introduced, in response to trigger events during a relationship, such as a "match" generated by a screening tool; during periodic reviews; and when a relationship ends.

Sanctions List: A document or database listing individuals, legal entities, and countries with whom it is illegal to do business.

Sanctions Regime: A set of sanctions that have a common nexus or theme. These are either referred to by the issuer of the set of sanctions or by the intended purpose of the set of sanctions. For example, the 'OFAC sanctions regime' or the 'North Korea sanctions regime.' Depending on the context, a sanctions regime may be limited to unilateral sanctions or may include multilateral sanctions.

Sanctions Compliance- The act of adhering to the sanctions-related legislation, regulations, rules, and norms that make up the complex sanctions landscape.

Second Line of Defense: The sanctions compliance function, the larger compliance function, and the human resources and technology departments comprise the second line of defense within the governance structure of a sanctions compliance program. The sanctions compliance officer ensures ongoing monitoring of sanctions compliance to enable the escalation of identified issues. In general, the second line exists to ensure that SDD procedures and processes applied by the first line are designed properly, firmly established, and applied as intended. The second-line defense reviews the effectiveness of controls used to mitigate sanctions risks; provides information to the first line; and investigates possible noncompliance with sanctions restrictions.

Simple Checks :One of the first steps in an investigation, simple checks are those initial actions taken to discount or confirm a sanctions link; an example of a simple check includes comparing data about a sanctions target with a firm's Know Your Customer (KYC) data.

Specially Designated Nationals and Blocked Persons list (SDN list) : A list of individuals and companies, published by OFAC, that are owned, controlled by, or acting on behalf of a targeted country. The list also includes groups and people, such as terrorists or drug traffickers, who are associated with a specific crime as opposed to a country. The US Department of the Treasury maintains the list and may name a person or company as an SDN. When the government identifies a person or company as an SDN, it blocks their assets and forbids US persons to do business with them. The government may also impose fines and imprison lawbreakers.

Suspicious Activity : irregular or questionable customer behavior or activity that may be related to a money laundering or other criminal offense, or to the financing of a terrorist activity. May also refer to a transaction that is inconsistent with a customer's known legitimate business, personal activities, or the normal level of activity for that kind of business or account.

Suspicious Transaction Report (STR) : A government filing required by reporting entities that includes a financial institution's account of a questionable transaction. Many jurisdictions require financial institutions to report suspicious transactions to relevant government authorities such as its FIU on a suspicious transaction report (STR), also known as a suspicious activity report or SAR.

Terrorist Financing :The by which terrorists fund their operations in order to perform terrorist acts. There are two primary sources of financing for terrorist activities. The first involves financial support from countries, organizations or individuals. The other involves a wide variety of revenue – generating activities, some illicit, including smuggling and credit card fraud.

Third line of Defense:The third-line defense within the governance structure of a sanctions compliance program is the internal audit, which involves independent reviews of the controls applied by the first two lines of defense. It independently evaluates the risk management and controls of the bank through periodic assessments, including the adequacy of the bank's controls to mitigate the identified risks. It also evaluates the effectiveness of the staffs execution of the controls, the effectiveness of the compliance oversight and quality controls, and the effectiveness of the training.

Third-Party Database: Third-party databases can be a good source of both primary and secondary information sources. Examples of third – party database include rating agencies, stock exchanges, and legal databases.

Unilateral Sanctions : These are sanctions imposed by a single country against a targeted entity. These are generally considered less effective than multilateral sanctions. Still, they serve to target specific offensive practices or behalf of imposing nations.

United Nations (UN): An international organization that was established in 1945 by 51 countries committed to preserving peace through cooperation and collective security. Today, nearly every nation in the world belongs to the UN. See also Vienna Convention. The United Nations contributes to the fight against organized crime with initiatives such as the Global Program against Money laundering (GPML), the key instrument of the UN Office of Drug Control and Crime Prevention in this task. Through the GPML, the UN helps member states to introduce legislation against money laundering and to develop mechanisms to combat this crime.

Unusual Transaction - Transaction that appears designed to circumvent reporting requirements, is inconsistent with the account's transaction patterns or deviates from the activity expected for that type of account.

Wolfsberg Group: an association of global financial institutions, including Banco Santander, Bank of America, Bank of Tokyo-Mitsubishi UFJ, Barclays, Citigroup, Credit Suisse Group, Deutsche Bank, Goldman Sachs, HSBC, J.P. Morgan Chase, Société Générale, Standard Chartered Bank and UBS. In 2000, along with Transparency International and experts worldwide, the institutions developed global anti-money laundering guidelines for international private banks.

Abbreviations

AML - Anti-Money Laundering

AMLCO/MLRO - Anti-Money Laundering Compliance Officer or Money laundering Reporting Officer of the Company

BoD — Board of Directors of the Company

CDD- Customer Due Diligence

EDD - Enhanced Due Diligence

CFT- Combating the Financing of Terrorism

EU — European Union

FATF – Financial Action Task Force

NOOGH- The national Ordinance on Offshore Games of Hazard (Landsverordening buitengaatsse hazardspelen, P.B. 1993, no. 63)

PEP- Politically Exposed Person **UN**- United Nations

4. Money-laundering

Organized crime operations are based on money laundering, often on an international scale. The illegal origin of criminal proceeds from such crimes as financial fraud, tax evasion, violations of sanctions, bribery, illegal arms trade, drug trafficking, extortion, kidnapping etc. is disguised during its processing, including their identity, source and the destination and equals money-laundering. Therefore, the goal of money-laundering is to make the criminal proceeds appear legitimate from the time the money is placed into the financial system (placement stage), layered in order to hide the audit trail through the web of complex financial transactions at various financial institutions (the layering stage), to the time it is integrated back into the financial system through the purchase of luxury items or cash-intensive businesses (integration stage). Money-laundering has social, economic, legal and regulatory implications on the world economy and leads to increasing costs of monitoring businesses from a compliance standpoint. The gambling and betting industry therefore is considered high risk since online platforms are vulnerable to money-launderers since online gambling transactions are cross-border and services are often anonymous in a non-face-to-face business. VIP accounts, money services businesses and multiple accounts are just a few challenges that the industry is known for. Based on the results of the complex business risk assessments, Rozairo N.V.'s main priority is to detect and deter money-laundering threats as well as mitigate such risks in the following areas:

- Using the online platform as a player-to-player transfer route to funnel funds between sellers and buyers and cashing out when necessary.
- Depositing funds obtained from illicit operations and/or using the online platform as "parking", rather than with the goal of engaging in online gambling or online sports betting.
- Verification fraud and identity theft (customer due diligence covering documentation verification, age verification and location verification)
- Operation of multiple accounts and high transaction volumes

This list is not exhaustive and whereas additional risks may materialize from time to time, the Company implements robust KYC procedures to identify high-risk customers, utilizes advanced proprietary software to detect suspicious transaction patterns, offers regular AML trainings to the employees, and conducts regular audits of AML controls and systems.

5. Terrorism- Financing

Providing funds via different methods and sources for carrying out terrorist activities defines the term terrorism financing, including but not limited to direct funding for the planning and execution of terrorist acts or financial support enabling terrorism such as training, recruitment, and propaganda. Money laundering and terrorism financing are two separate crimes which, nevertheless, are often mentioned together. Countering the financing of terrorism is as important as combating money-laundering but its pattern is largely different and is known to comprise small donations from legitimate sources in the form of charitable donations, personal income or business revenue. Illegitimate sources of funds include fraud, criminal activities and money laundering whereas the methods of transfers differ from payment institutions to HAWALA, cash mules and cryptocurrencies, inter alia. Overall, the FATF (The Financial Action Task Force) Recommendations 2012-2023 identify customer due-diligence, record-keeping, and reporting suspicious activity as main preventive measures that help businesses combat money-laundering. Furthermore, the FATF produced strategic guidance on the AML/ CFT risk-based approach for online casinos where it highlights the vulnerability of online casinos, and gaming sector as regards money laundering (ML) and terrorist financing (TF) risks (page 59, Vulnerabilities of Casinos and Gaming Sector – March 2009) due to the key industry threats associated with the ever evolving techniques of online gambling fraud within the context of limited AML/CFT controls or regulatory responses in many jurisdictions. From the payment methods standpoint, the volume of remote gambling transactions taking place over the online platforms with 24/7 accessibility is so large and the payment methods are so varied, that it is of paramount importance to develop efficient internal controls based on the periodic reviews of the results of the internal AML/CFT risk-assessments. Notably, the 2022 Supranational Risk Assessment Report by the European Commission identified the “gambling sector” and online gambling, as a “high risk” area of AML/CFT concern due to “the non-face-to face element, huge and complex volumes of transactions and financial flows” involving cryptocurrencies among other payment instruments. Prepaid cards have been identified as a highly popular method to acquire materials for the terrorist attacks and therefore it is important to conduct staff training based on newly available information.

The non-exhaustive list of conduct that may be indicative of terrorist financing risk include the following examples:

- The parties to a transaction are based in a country or countries that are on a list of state sponsors of terrorism or a sanctions list.
- Adverse media/ negative news screening reports indicative of links to the terrorist organizations.
- Small regular deposits that are structured to avoid detection.

6. Risk - Based Approach (ML/TF risks'detection)

Company applies a risk-based approach in combating exploitation of its online platform for the purposes of ML and TF. The methodology the Company adopts is based on the Guidance of the Financial Action Task Force (FATF) as regards ML/ TF Risk Assessment and determines a risk level by evaluating types of risk, threats, vulnerabilities, controls, consequences, the likelihood of it happening, and the impact it may have on the business model in a particular geographical location.

Specifically, AML/CFT risk assessment categories center around the risks associated with:

- the range of Products and services the Company offers,
- transaction risks,
- players' risks.
- geographical risks
- employee risk.

Based on the analysis of the risk indicators, the risk model calculates a risk rating of low, medium or high which is then used to create a risk profile which is then assigned to the players and payment service providers at the onboarding stage and is reassessed and amended during the business relationship within the framework of periodic KYC/KYB reviews. Online casinos possess inherent high risks, so the Company strives to rely on its AML and Anti-Fraud key personnel to maintain effective Internal controls and CDD measures as reflected in relevant policies.

7. Customer Due Diligence Guidelines (CDD, EDD)

In the EU, the EU's 4th AML Directive (AMLD4) expanded CDD requirements to casinos and the entire gambling sector. It requires "identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source." It further requires CDD on customers placing a stake or collecting winnings of €2,000 or more. Furthermore, AML 5th Directive and AML 6th Directive, build upon these measures, clarify certain regulatory details, and toughen criminal penalties for non-compliance. For example, AMLD5 requires that licensed operators ensure that a casino's customers are correctly identified as a part of their risk-based casino anti-money laundering assessments. Whereas Curacao AML legislation is loosely based on these principles, the Company takes into account the EU legislation as well as FATF Recommendations when approving its KYC policy on an annual basis.

When establishing a business relationship with customers it is imperative to identify whether a customer wishing to use the Company's online platform poses any money-laundering, terrorist financing or proliferation financing threats to its ecosystem. CDD forms the basis of the risk-based assessment for risk scoring purposes based on the analysis of types of suspicious activities including behavioral indicator, transactional indicators, customer profile and product and services' indicators. In the context of AML, customer due diligence process is a procedure which includes the identification of the potential customer, verification of his/her identity and age, collection of additional information to construct an economic profile of the account holder, assign a risk rating, and monitor his/her behavioral and transactional patterns for any deviations that may be construed as a violation of AML/CFT legislation and policies. Research into the customers can be done via open-source tools such as social media checks, property ownership checks, employment checks, insolvency checks etc. Due Diligence measures may be simplified when the analysis of the initial customer data places such applications in a low-risk category, whereas Enhanced Due Diligence (EDD) is applied to cases that require additional screening due to the system flagging certain data entries such as PEPs (politically exposed persons), customers from high-risk jurisdictions etc.

The Company has created a risk scoring system by categorizing customers in accordance with set risk profiles which are construed from the physical location of the customers, their transactional behavior and the products they use. The integrity of the Company's gaming environment is maintained through the application of protocols based on utilizing advanced technology and third-party databases including a proprietary anti-fraud system for onboarding and transaction monitoring, artificial intelligence tools (AI), biometric identification in some instances and RegTech screening tools such as WorldCheck, LexisNexis, SEON etc.

Activities or type of players that may indicate a higher risk include the following categories:

1. Unusual requests that do not fall within the recommended guidelines such as to by pass KYC verification process etc.
2. Requests to withdraw winning via another payment method which differs from the one that was used for the original placement of the bet.
- 3 Anonymous customers
- 4 Economic profile is inconsistent with the increase in gambling activity
4. Attempts by the same individual to create multiple accounts
5. Drastic changes in the gambling pattern
6. High-value staking/ high transaction volume
7. Additionally, the Company conducts due diligence checks on business relationships such as counterparties, agents, affiliates, and third-party service providers to ensure the partners comply with AML standards and regulations.

8. Transaction Monitoring

Transaction monitoring in the betting and gambling industries is a critical component of regulatory compliance and anti-money laundering (AML) efforts. Given the high volume of transactions and the potential for misuse, these industries are closely monitored by regulatory bodies to prevent illicit activities such as money laundering, fraud, and financing of terrorism. The Company's objective is to mitigate challenges arising from the high volume and velocity of transactions where makes challenging to monitor each transaction effectively, and the use of cryptocurrencies and other digital payment methods that complicate the monitoring process.

In a nutshell, the Curacao regulatory landscape focuses on defining the indicators that may suggest the transaction is of an unusual nature so that it may be reported to the Curacao Financial intelligence Unit (FIU Curacao). Therefore, an adequate transaction monitoring system is a vital part of complying with the licensing requirements in Curacao.

The Company's anti-fraud team is in charge of operating a proprietary anti-fraud system which analyses players' data on the basis of the automatic checks performed through a number of electronic systems such as WorldCheck and manual checks performed by a team of analysts via various data sources. Any discrepancies identified by the first line of defense are escalated to the Team lead and then may be ultimately reported to the AML/CFT Officer in writing through an Internal suspicious activity report (SAR).

This system is an automated monitoring system which allows to monitor transactions in real-time, flagging suspicious activities based on predefined rules and thresholds. The anti-fraud team uses machine learning and data analytics to enhance detection capabilities and reduce false positives. Additionally, the system is configured in a such a way as to focus on high-risk transactions, such as large cash deposits, frequent transfers, and cross-border transactions and the parameters reflect current and emerging threats to capture bad actors by flagging suspicious activity internally, and, where necessary, to financial intelligence units (FIUs).

Components of Rozairo N.V.'s transaction monitoring system:

Automated System: Advanced software solutions are employed to monitor transactions in real – time. These systems use algorithms and machine learning to identify patterns and anomalies that may indicate suspicious activities.

Risk Assessment: customers and transactions are assessed for risk based on various factors, including the amount and frequency of transactions, geographic location, and customer behavior.

Alert Generation: When suspicious activity is detected, the system generates alerts that are reviewed by compliance officers. Alerts are based on predefined rules and thresholds, such as unusually large transactions or frequent deposits and withdrawals.

Common techniques include geolocation tracking, source of funds verification for high- value transactions, behavioral analysis by monitoring changes in betting patterns or gambling behavior that deviate from the norm for a specific customer as well as transaction velocity (quick movement of funds between accounts and/or frequent high-value transactions within a short period).

CDD: i s triggered in the following scenarios: creation of an online account; doubts about the authenticity of the provided information and documents; suspicious customer profile and/or transactional activity, unauthorized attempts to change the player's profile and a transaction or transactions that appear to be linked amount to 2000 euros or more. When a transaction or a series of transactions that appear to be linked amounts to more than 2000 euros, the CDD measures are applied automatically (the wagering of a stake, the deposit of

funds or the collection of the winnings through the withdrawal of the funds constitute a transaction in such cases). Periodic reviews of the existing records and ongoing monitoring of the transactional patterns of the regular players also form an integral part of the CDD measures. As part of combating money -laundering, fraud md terrorist financing, players' IP addresses are tracked via an embedded tool in the proprietary anti-fraud system in order to ensure the site is accessed from non-restricted countries. This measure also helps detect suspicious activity such as attempts to set up multiple accounts by the same individual, or block individuals who have been blacklisted or self-excluded. The proprietary software also monitors data as regards the players' transaction history, betting amount, information on wins and losses, players' geolocation, pattern of gambling activity and duration of playing. These tools may be used in instances where a customer risk's rating is deemed to be high due to presence of some behavioral or transactional triggers that point to u potential AML/CFT breach.

In cases where the CDD measures cannot be applied, the account gets locked during an attempt to complete CDD and ultimately the business relationship with the customer gets terminated due to the failure to satisfy AML/CFT legislative requirements and the funds are refunded back to the customer through the same payment channel and account used to deposit the funds.

EDD and ongoing monitoring are applicable to cases that receive a high-risk rating. Such examples may include doubts as to the authenticity of the documents, a high-risk third country location of the customer, a Politically Exposed Person (PEP) status of a potential customer, unusual behavioral patterns and therefore require additional investigations in the form of additional verification checks, adverse media screening or requests to provide additional documentation as regards the source of wealth, source of funds, utility bills, etc.

9. Politically- Exposed Persons (PEPs)

Enhanced Due Diligence (EDD) is a crucial process in the online betting and gambling industries aimed at preventing money laundering, fraud, and other illicit activities. EDD refers to the additional measures taken by companies to thoroughly verify the identity and background of their clients, particularly those posing higher risks. High-risk customers in the online gambling and betting setting are those who have high transaction volumes, deposit or withdraw large amounts, exhibit unusual betting patterns or are Politically Exposed Persons (PEPs). A PEP is an individual who recently held or is currently holding a prominent public position such as a head of state, member of the Parliament, government, directors of international organizations etc. Family members of PEPs and close associates are also considered PEPs, so their applications are also treated as high-risk by the Anti-Fraud team and relevant risk management procedures are activated when processing such requests through the senior management.

At Rozairo N. V. PEPs' cases are handled by the senior management team whose approval is necessary to transact with such individuals. Furthermore, an internal register of such cases is kept by the MLRO office.

10. Sanctions Management, FATF blacklist, license Restrictions

Sanctions screening is the process of checking individuals, organizations, and transactions against various sanctions lists to prevent illegal activities and ensure compliance with international regulations. The purpose of sanctions screening is to comply with international, national, and regional sanctions regulations, prevent financial crimes such as money laundering and terrorism financing and to protect the reputation and integrity of the betting and gambling industry and Rozairo N.V. in particular. Whereas EDD focuses on enhanced verification of high-risk customers, sanctions screening specifically checks against sanctions lists to identify prohibited entities.

As a Curacao-based entity with an EU-based payment agent Rozairo N.V. complies with the key sanctions list which are part of the international regulatory framework, including:

United Nations Security Council (UNSC) Sanctions

<https://www.un.org/securitycouncil/content/un-se-consolidated-list>),

European Union (EU) Sanctions

<https://www.eeas.europa.eu/eeas/European-union-sanction.en>

United States (OFAC) Sanctions: Office of Foreign Assets Control.

<https://sanctionssearch.ofac.treas.gov>

UK Sanctions: HM Treasury Sanctions.

<https://www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases>

Other jurisdictions: Local sanctions regulations.

In addition, the Company uses various databases such as WorldCheck Refinitiv and open-source databases for sanctions and PEP screening. In unlikely circumstances where a payee or a customer are identified as a designated person, payments will not be processed and an internal SAR/STR report will be submitted to the MLRO office for further regulatory processing if necessary.

FATF blacklist

The Company's primary goal in this regard is to prevent making payments to designated persons and sanctioned entities and/or serve customers from FATF black-listed countries such as Democratic People's Republic of Korea, Iran, Sudan and countries that are on the State Sponsors of Terrorism list by the U.S. Department of State i.e. Cuba, North Korea, Iran and Syria

(<https://www.state.gov/state-sponsors-of-terrorism/>)

License Restrictions

Company operates under the Curacao online gaming license and is therefore banned from offering its online services in Aruba, Bonaire, Curacao, France, the Netherlands, Saba, Statia, St. Maarten, Singapore and the USA. It does not operate in countries where there is a total ban on gambling such as China, Turkey, Brunei, Cambodia, Japan, Qatar, Lebanon, Poland inter alia or where the Company is required to obtain a local gambling license in order to operate locally (USA, UK, EU countries for instance).

11. Suspicious Activity Reporting Guidelines

Reporting suspicious activities in the gambling and betting industries is a critical component of maintaining the integrity of these sectors and preventing them from being exploited for illegal purposes such as money laundering, fraud, and corruption. Suspicious activity is reported for legal compliance purposes as failure to report can result in significant fines and legal consequences for individuals and businesses. It also helps ensure customer protection and helps safeguard customers from fraud and exploitation, ensuring a fair and safe environment for betting and gaming. Suspicious activity includes unusual transactions, structuring, unusual account activity and non-typical behavioral pattern, either too excessive or too disinterested in the betting outcomes, for instance. Unusual gambling patterns are investigated first to determine whether the exact nature of the transaction is just unusual or there are grounds to believe that it may be affiliated with the proceeds of a crime. According to article 1 of the Norut, it is an internet gambling entity's duty to report unusual transactions through the FIU Curacao's goAML portal which has been in use since January 1, 2021.

Therefore, if the nominated officer determines that the internally reported suspicious activity should be disclosed to the regulatory authorities, he does so via the portal to comply with the Company's AML/CFT reporting protocol and obligations. In the meantime, the business relationship with the suspected customer is to be paused or terminated, depending on the circumstances.

In cases where employees of the Company know, suspect or have reasonable grounds to believe that a person is attempting to finance terrorism or launder money, a relevant reporting protocol is activated, and a suspicion report must be submitted to the nominated officer who then determines whether there are grounds for further regulatory action.

In a B2C setting suspicious activity may include using several anonymous payment methods i.e. prepaid cards; location of the payment method does not correspond to the geolocation of the customer, depositing a large sum and withdrawing it after no gaming or little gaming activity; a withdrawal request to a third-party payment method.



In a B2B setting suspicious activity may include using an intermediary for document-related requests; source of wealth does not match the reported financial data; frequent changes of ownership in a short time; lack of willingness to provide due diligence documentation,

The Company keeps detailed records of all transactions and activities that seem suspicious, including dates, amounts, methods, and any other relevant details. As regards customers, the anti-fraud and AML teams document all available information about the individuals or entities involved, including names, addresses, account numbers, and identification.

12. The Money Laundering Reporting Officer (MLRO)

MLRO, or Money Laundering Reporting Officer is a designated individual who oversees compliance with AML regulations at Rozairo N.V. It is a crucial role which encompasses being authorized to communicate with the relevant authorities in Curacao as well as supervise a team of AML compliance officers and their day-to-day operations, including maintaining robust age verification protocols, promoting responsible gambling practices, preventing gambling-related addiction, promoting self-exclusion tools.

The MLRO is also responsible for disclosing suspicious activity, including suspicious transactions, to the FIU in Curacao. Internally, the AML/CFT Officer is requested to prepare quarterly AML reports for the Board of Directors to keep the Board members informed of any recommended changes that may be required to manage the AML/CFT compliance program.

13. Senior Management Responsibility

The Company's senior management is fully engaged in the process of assessment of inherent risk categories. It is required by the Board of Directors that a nominated AML/CFT Officer regularly updates the Members on any significant deviations related to the control environment and produces an annual report covering the operator's systems and controls that mitigate the risks of money-laundering, terrorist financing and proliferation financing. Periodic reviews of the relevant policies and procedures take place quarterly based on monthly risk assessments' results and the AML/CFT Officer may request the approval of the Board of Directors for any changes in Rozairo N.V.'s AML/CFT policy in order to remedy any identified weaknesses in the internal controls and risk management practices, should they arise.

14. Employee Training Program

Employees in the betting and gambling industries are on the front lines of AML compliance. Their ability to identify suspicious activities, report them effectively, and conduct due diligence is critical in preventing these sectors from being used for illicit purposes. By providing comprehensive training, fostering a culture of compliance, and ensuring that employees understand their role in AML efforts, the company strives to enhance the Company's defenses against money laundering and other financial crimes.

The Company's employees play a crucial role in Anti-Money Laundering (AML) compliance within the betting and gambling industries. Their actions and vigilance are essential in preventing these sectors from being exploited for money laundering and other illicit activities. They are made aware of the fact that failing to report potential breaches of AML Policies may lead to administrative and criminal charges.

The Company's employees, especially those in customer-facing roles or positions that involve handling financial transactions, must have a thorough understanding of the company's AML policies and procedures. This includes knowing the types of transactions that should be considered suspicious, the process for reporting such transactions, and the importance of maintaining customer confidentiality.

A key part of an employee's role in AML compliance is to be vigilant and identify any activities that seem unusual or do not fit with the normal behavior of a customer. This could include large and inconsistent bets, frequent changes in betting patterns, or transactions that seem to have no apparent purpose other than to move money through the system.

Once an employee identifies a potentially suspicious transaction, they must report it through the appropriate channels to the MLRO office. The reporting protocol involves filling out a Suspicious Activity Report (SAR) and using the company's internal reporting system. Employees are trained on how to report suspicions and the importance of doing so promptly on an annual basis or more frequently in line with the needs of a particular department.

Employees involved in customer onboarding or account management are responsible for conducting due diligence checks on customers. This includes verifying their identity, understanding the source of their funds, and ensuring that they are not listed on any sanctions or watch lists. Employees are trained on how to conduct such checks diligently and escalate any concerns where necessary.

Employees involved in AML compliance at the Company understand the importance of maintaining the confidentiality of their reports and any information related to suspicious activities. They are made aware of data protection laws and ensure that customer information is handled in compliance with these regulations.

15. Record- Keeping

The Company complies with all the relevant legislation as regards having an audit trail in cases where it is asked to assist in the investigations by law enforcement agencies. Generated records are retained in electronic form for a period of 5 years in accordance with the data protection regulations from the date of the establishment of a business, commercial or a professional relationship with an employee, a customer or a business partner.

Such a business relationship arises between the Company and a customer from the time when an account is open until the time when the relationship is terminated. During the relationship the Company undertakes to satisfy CDD measures stipulated in the legislation and carry out an ongoing monitoring of the account activity to adjust its risk rating where necessary.

16. AML Compliance Audit

Auditing procedures are systematic examinations of a company's financial records, operations, and compliance practices. Auditing begins with the planning stage, continues with collecting and analyzing data, and concludes with reporting and follow up to ensure the corrective actions are effective.

As such, maintaining effective defenses against financial crimes is at the cornerstone of the Company's AML Compliance Audits which are carried out annually and/or when there are significant changes in regulations, the nature of company's operations or detected non-compliance cases.

The audit program's focus is on Customer Due Diligence (CDD): Review the effectiveness of KYC (Know Your Customer) processes and the thoroughness of customer identification and verification procedures.

Transaction Monitoring: Assess the systems and procedures for monitoring and analyzing transactions to identify suspicious activities.

Suspicious Activity Reporting (SAR); Evaluate the timeliness and accuracy of reports submitted to regulatory authorities regarding suspicious activities.

Record Keeping: Ensure that all required records are maintained for the specified duration and are easily retrievable.

The results of the compliance audits allow the Company to establish internal controls which consist of policies and procedures designed to ensure compliance with law and regulation and aid the prevention of fraud.

