

ROZAIRO N.V

POLICY

**for Prevention and Combating of Money Laundering Terrorist Financing and Financing of
Proliferation**

Version Control

Version	Version Date	Approved By
3.0	12.08.2024	The Board
4.0	21.11.2024	The Board
5.0	14/02/2025	The Board

ABBREVIATIONS

MLCTF&FP	Money Laundering, Terrorist Financing and Financing of Proliferation
FATF	Financial Action Task Force
KYC	Know Your Customer
PEP	Politically Exposed Person
STR	Suspicious Transaction Report
MLRO	Money Laundering Reporting Officer
WMD	Weapons of Mass Destruction
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
RBA	Risk Based Approach
BRA	Business Risk Assessment
FIU	Financial Intelligent Unit

1. PURPOSE

THE POLICY

The Policy on Prevention of Money Laundering, Terrorist Financing and Financing of Proliferation (hereinafter — «the Policy») outlines the general unified standards and procedures of anti-money laundering and combating terrorism financing which must be adhered to by Rozairo N.V. (hereinafter — «the Company») its directors, officers and employees.

In any country or jurisdiction where the applicable anti-money laundering and terrorist financing laws and regulations, require the Company to establish higher standards, such country standards must adhere to.

Compliance with this Policy is mandatory and essential for ensuring that the Company is fully compliant with applicable anti-money laundering and terrorism financing laws and regulations of respective countries and jurisdictions.

Rozaro N.V. is committed to annual review and critical reassessment of this Policy in light of the company's business strategies, goals and objectives on an ongoing basis.

DEFINITION OF MONEY LAUNDERING TERRORIST FINANCING AND FINANSIAL PROLIFERATION OF WEAPONS OF MASS DISTRACTION

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have been derived from legitimate origins or constitute legitimate assets. Money laundering may generally occur in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from illegal or criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Broadly, the international anti-money laundering provisions are aimed at requiring firms to:

- identify customers and suspicious transactions at the placement and layering stages
- keep adequate records which should prevent the integration stage being reached, and also provide an audit trail for investigators, and
- report suspicious activity or behavior to the relevant regulatory or legislative authority.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, possibly for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money, such funding could be of cumulative nature over extended periods, and the associated transactions may not be complex.

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.

The FATF defines proliferation of weapons of mass destruction (WMD) as the transfer and export of nuclear, chemical or biological weapons, their means of delivery and related materials. The issue of proliferation received international attention for several years. A number of international conventions provide for measures to detect and prohibit proliferation, especially with regard to nuclear materials (such as the Nuclear Non-Proliferation Treaty). These treaties do not, however, consider the aspect of financing proliferation. In 2004, the UN Security Council issued Resolution 1540, requiring states to put in place a number of measures in order to prevent the proliferation of nuclear, chemical or biological weapons. Subsequently, the FATF started in 2007 to consider the threats related to proliferation financing and its interconnection with terrorism and terrorism financing.

The interconnection is based on the fact that proliferation might be a means for supporting the undertaking of terrorist activities. Its disruption is therefore essential for the prevention of terrorist acts. Moreover, the practical undertaking of proliferation financing often uses the same channels as terrorist financing. Measures to be applied in order to disrupt proliferation financing would therefore often be similar to the measures applied to counter terrorist financing.

2. SCOPE

Since the Company is not registered and does not operate as a bank or financial institution, complete formal compliance with the aforementioned sources is not mandatory. Nevertheless, the Company's owner and executives deem it important to adhere to the best practices that the above guidance represents. Hence, relevant provisions

of the above directives and legislation are voluntarily incorporated into the Company AML&CTF Policy and procedures.

As a reporting entity, the Company has mainly the following obligations:

- The obligation to know the client and to assess the risks of money laundering or terrorist financing;
- The obligation to report unusual transactions, within the meaning of the Regulations.

This Policy aims to comply with the rules and guidance is contained in the following laws:

National Ordinance Penalization of Money Laundering (NOPML), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the National Ordinance on Identification of clients when Rendering Services (NOIS), Caribbean Financial Action Taskforce (CFATF) and the FATF recommendations, Sanctions National Ordinance, Kingdom Sanction Act, Ministerial Decree with general operation of November 11, 2015, National Decree entering into force of Kingdom Sanction Law.

3. MONEY LAUNDERING TERRORIST FINANCING AND FINANCING OF PROLIFERATION RISKS

As any online funds' recipient and processing business, the Company is exposed to a variety of risks related to a potentially improper use of its business facilities in the interests of those involved in money laundering and terrorist financing. While these risks are inherent and cannot be entirely avoided, the Company believes that the risks could be identified and contained via effective use of the AML&CTF procedures, systems and personnel.

Rozairo N.V. representatives identified the following key MLTF&FP risks.

1. The risk of accepting the customers whose identities and/or addresses are hidden to conceal the direct relation to MLTF&FP activities (for example, use of multiple passports to conceal the identity or residential address.)
2. The risk of taking, as a deposit for online gaming via the Company's website, the funds that have, unbeknownst to the Company, been originated from illegal and/or terrorist-supporting sources (for example, transfer of gambling funds directly or indirectly from FATF-censured jurisdictions.)
3. The risk of providing an unintended financial conduit or repository for the funds originated in the course of illegal and /or terrorist-supporting activities (for example, temporary "parking" of funds without the direct use in e-gambling activities.)

4. The risk of the illegal funds transfers (withdrawal) by the customers via Company's website facilities (for example, placing the funds without intention of using them in betting activities).
5. The risk of unknowing conduct, by the Company, of certain functions of a financial institution for any of the customers beyond the usual business remit (for example, by saving, exchanging or transferring the customer funds at the customer requests).

The Company recognizes that in addition to the aforementioned risks there may exist various other unknown sources of MLTF&FP threats to the business. While identification and prevention of such threats is beyond the Company normal business capacity, the management believe that fostering the general alertness, risk awareness and the spirit of constructive skepticism among employees is the best general preventive measure that could prevent MLTF&FP risks from materializing.

In view of the management, MLTF&FP risks and business risks are intertwined inextricably hence assessment of MLTF&FP risks at the Company is a part of the systematic risk assessment regularly conducted by the Company's management.

4. BUSINESS RISK ASSESSMENT

The Company intends to operate predominantly in the Eastern part of the European Union with neighboring region containing jurisdictions with strategic deficiencies as per FATF. Such characteristics impose the requirement for the Company to be alerted in its approach towards various risks of regional nature that might influence the Company's business. For example, Rozairo N.V. has been careful in entering every market of its current operating exposure strictly conditional upon the proven market potential and the acceptable levels of legislative recognition conducive to the Company's business in a given country. By necessity, thus the conduct of general business risk assessment of Rozairo N.V. is country-based and country specific in nature.

In the Company's view, MLTF&FP risks and business risks are intertwined inextricably hence assessment of MLTF&FP risks at the level of the Company is a part of the systematic risk assessment regularly conducted by the management.

5. GENERAL ASPECTS OF MLTF&FP RISK ASSESSMENT

The risk assessment has the role of preventing the use of the Company by the clients in MLTF&FP activities or in activities that contravene the regime of international sanctions. In addition, the risk assessment allows the Company to determine the KYC measures that will be applied both in the procedure for the identification of a client, as well as during the Business Relationship, both for new clients and for the existing ones.

The risk assessment process for MLTF&FP threats is arranged along two different dimensions – nature and complexity of the risk; and value of the risk.

- Along the first dimension, there are a number of risk triggers that allow for identification of the nature and complexity of the risk, i.e. citizenship of the player, changes in the registration information, e-wallets selection, specifics of bets placed and others. A particular combination of triggers signals that the MLTF&FP risk is simple or complex in nature. Relative simplicity or complexity further determines the Company's response and mitigation measures towards the risk.
- Along the second dimension, an analytical attempt is made to assess the geographical scope and monetary value of a specific MLTF&FP risk. For example, the first deposited amount from a new client is usually accepted at the lowest allowable threshold, thus containing the MLTF&FP risk of improper use of the Company's Customer account for depositing the funds. Further continuation of relationships and ordinary deposit-betting-withdrawal patterns by the customer usually leads to increases in the values of allowable deposits and withdrawals. Gradually, the Company's relationship with a customer builds up thus allowing for equally commensurate increase in the volumes of business conducted.

Based on the criteria described above, the clients of the Company may be classified in one of the following risk categories: low risk, standard risk, high risk.

Depending on classification, different actions are called for from the CO and other employees involved in MLTF&FP verification.

When assessing the risk of ML&TF, the Company will consider at least the following:

- (a) the purpose of initiating a relationship;
- (a) the size of transactions to be performed by a client;
- (b) the regularity or duration of the Business Relationship;
- (c) regulations and sectoral instructions.

As any other online gambling operator, the Company is exposed to a variety of risks related to a potentially improper use of its business facilities in the interests of those involved in money laundering and terrorist financing. While these risks are inherent and cannot be entirely avoided, the Company believes that the risks could be identified and contained via effective use of the AML&CTF procedures, systems and personnel.

6. MLTF&FP RISK AND FINANSIAL PROLIFERATION ASSESSMENT

Risk assessment process for MLTF&FP threats is arranged along two different dimensions – nature and complexity of the risk; and value of the risk.

Along the first dimension, there are a number of risk triggers, which allow for identification of the nature and complexity of the risk, i.e., citizenship of the player, changes in the registration information, e-wallets selection, specifics of bets placed and others. A particular combination of triggers signals that the MLTF&FP risk is simple or complex in nature. Relative simplicity or complexity further determines the Company response and mitigation measures towards the risk.

Along the second dimension, an analytical attempt is made to assess the geographical scope and monetary value of a specific MLTF&FP risk. For example, the first deposited amount from a new customer is usually accepted at the lowest allowable threshold for a given jurisdiction thus containing the MLTF&FP risk of improper use of the Company's Client account facilities for depositing the funds. Further continuation of relationships and ordinary deposit-betting-withdrawal patterns by the customer usually leads to increases in the values of allowable deposits and withdrawals. Gradually, the Rozairo N.V. relationship with a customer builds up thus allowing for equally commensurate increase in the volumes of business conducted.

7. THE RISK-BASED APPROACH

It is strongly believed that a robust risk identification process is foundational to a successful risk management program. It is conducted regular risk identification workshops as part of the Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) training program.

The Company employs a systematic approach to continuously monitor and revise the risk factors associated with the clientele. This ongoing vigilance is tailored to accommodate fluctuations in market conditions, seasonal variances in business, and internal risk tolerance. In assessing the risk profile of the clients, it is considered several key indicators. The status of the clients it is scrutinized, including whether they are a Politically Exposed Person ("PEP") or a Person of High Risk and Reputation ("PIHR"), both categories automatically designated as a High Risk and rejected from the system as Players. It is also evaluated if the client is affiliated with local crime, substantiated by a police report, or if they are sanctioned, either circumstance elevating them to High-Risk status or subsequently are blacklisted from playing. An important component of the risk assessment involves examining the verification stage passed by the player, the player's country of residence, and their nationality. The attributed risk values these factors based on specific criteria, allowing them to further refine our risk profiling. A significant aspect of the risk analysis focuses on the financial activity of our clients. The preferred deposit method of each player is analyzed, also the range of their deposit sum, and their betting activity. These parameters are monitored and evaluated for risk, taking into account the payment solution provider, the total deposits made since registration, and the total betting amount. The detailed examination used extends to jurisdictions risk analysis, deposit analysis, and payment systems analysis. By meticulously monitoring these factors, it is ensured that the Company's risk mitigation

strategies remain robust and adaptable to changing circumstances. This comprehensive approach allows us to maintain the integrity of our operations while effectively managing potential risks.

The Company's Risk scoring model is robust in the sense that it considers a variety of factors that could affect the risk level of a customer, from political exposure to betting and deposit habits. This multi-dimensional approach is useful in capturing a comprehensive view of the risk landscape.

The Company employs a Risk-Based Approach and clearly defines the following points:

- a) Requirements for players' registration and the conduct of a single transaction over €2.000;
- b) Categories of players whose registration is not accepted.
- c) Criteria for classifying players in four categories based on risk assessment:
 - i. Low risk
 - ii. Medium risk
 - iii. High risk

Following the comprehensive assessment and classification of a client into low, medium, or high-risk categories, the company embarks on the corresponding due diligence measures, tailored to align with the identified risk level. For clients in the low-risk category, a Simplified Customer Due Diligence is conducted, while for those in the medium-risk category, a Customer Due Diligence is performed. Enhanced Customer Due Diligence is reserved for clients who fall into the high-risk category. Each of these procedures is meticulously executed in accordance with our risk mitigation strategy, tailored to respond optimally to the current scenario. This robust and adaptable approach ensures we maintain the highest standards of regulatory compliance and risk management across our operations.

The following factors, although not exhaustive, may contribute to the categorization of a player as high risk:

- Identification as a Politically Exposed Person (PEP),
- Presence of a non-clear criminal record,
- Involvement in an ongoing criminal investigation,
- Previous imposition of an administrative fine,
- Documented participation in illicit betting activities,
- Discrepancy between the individual's financial profile and observed business activities,
- Frequent receipt of reports or complaints regarding the individual from other players,
- Reluctance or refusal to provide the bookmaker with requested or supplementary information,
- Failure to meet the requirements stipulated by the licensing authority.

The company reserves the right to terminate business relationships under certain circumstances, such as if there are reasonable grounds to suspect a loss of formal purpose in the relationship or in a case of identity fraud (the Customer have presented stolen documents). Risks posed by customers that could jeopardize the continuity of the business relationship for any previously outlined reasons are not willingly accepted by the company.

8. INDICATIONS OF SUSPICIOUS, COMPLEX OR UNUSUAL TRANSACTIONS. OTHER RISKS

When performing risk assessment of the clients, the Company will also take into account some risk hypotheses / indications which may lead to the recognition of suspicious, complex or unusual transactions or other risks in terms of MLTF&FP according to the AML Instructions and as identified by the Company:

1. Potential complicity of employees;
2. Use of false or stolen identity documents by players;
3. Concealment of the identity of the Beneficial Owner;
4. Lack of appropriate KYC policies;
5. Accessing multiple gaming platforms or collections of games within the same platform;
6. Complicity in the provision of bonuses or other benefits;
7. B2C; the vulnerability is associated with the ability of clients to join the game and deliberately transfer funds ("chip dumping");
8. E-Wallet, being considered a payment method that makes difficult for the operator to identify the source of funds;
9. Remote gambling used as a front for cash deposits, which are then transferred to bank accounts, with apparent winnings from gambling as the source of funds;
10. Transactions, both individual and linked, that are unusual in character, complex, large and have no obvious economic, commercial or legal purpose in relation to the Company's business;
11. Transactions that present an unusual or complex pattern compared to the client's risk profile or the pattern of transactions associated with the client, similar products or services;
12. Transactions in excess of normal limits typical for a player. An example would be an attempt to withdraw the funds from the gaming account in small instalments but totalling the entire balance of the account during a short period of time;
13. High turnover financial transactions (deposits and withdrawals) unwarranted by the gaming activity of the player;

14. Transactions outside of the player's regular payment and withdrawal patterns. An example is a series of minor deposits followed by no-activity period and a subsequent request for withdrawal of the entire amount;
15. The customer requests unnecessary or unreasonable levels of secrecy. For example, the client is reluctant to share due diligent information, or he appears to want to disguise the true nature of his business;
16. If the customer's or Beneficial Owner's source of wealth or source of funds cannot be easily explained;
17. Transactions of the customer, who has a political connection, or any other relevant links to a PEP or a Family member of PEP or Persons known to be close associate of PEP (persons who may abuse, directly or indirectly, of a public position for private gain), if such connection/link becomes known to the Company;
18. The customer insists that the transfer of earnings be made to the account or in the name of another person;
19. Customers who constantly play against each other;
20. Clients who carry out transactions that appear to be disproportionate compared to the financial situation or income proven according to the documents certifying the source of the funds.

The Company recognizes that in addition to the indications of risks listed above there may exist various other unforeseen MLTF&FP risks. While prior identification of all such risks is not possible, the Company believes that fostering the general alertness, risk awareness and the spirit of constructive skepticism among employees are the best general preventive measures that could help timely identification recognition of suspicious transactions in terms of MLTF&FP risks.

In general, the Company will examine the context and purpose of all transactions that meet at least one of the following conditions:

- (a) Complex transactions;
- (b) Transactions with unusually high values;
- (c) Do not fit into the usual pattern (taking into account any reasonable or justified deviations from the pattern)
- (d) Do not have an obvious economic, commercial, or legal purpose.

In any of these cases, the Company will increase the degree and nature of the monitoring of the Business Relationship in order to determine whether such transactions or activities are suspicious.

The identification of an isolated risk factor does not automatically determine the classification of a client in a higher or lower risk class. For each client, the Company will evaluate the risk factors presented in this Policy to establish the degree of risk, which will be established because of the logical combination of the identified risk factors. The placement of a client in one of the risk categories can be changed at any time during the Business Relationship as a result of obtaining new information by the Company. If the client is subsequently placed in a higher risk category, the Company will apply the appropriate KYC measures.

In addition, the identified risk factors/ indications and their evolution will be continuously monitored by the compliance officer to determine the need to update the risk assessment section of this Policy.

9. INTERNAL CONTROLS

The Company internal controls are a set of policies and procedures aimed at securing the efficient and compliant business within Rozairo N.V. and provision of the safe and fair gambling environment for the customers.

10. AML&CTF DESIGNATED OFFICER

MLRO has practical knowledge of the Company business environment, risks inherent to the Company's business model and AML&CTF provisions as stipulated in the Regulations as amended. AML&CTF Compliance Officer also performs the duties of Money Laundering Reporting Officer at the Company and is responsible for reporting transactions suspicious from AML&CTF standpoint to FIU.

General duties of the AML&CTF Compliance Officer include monitoring of the Company's compliance with the AML&CTF obligations; assessment of the business risks both internal and external; oversight of the AML&CTF related communication and training for employees; and reporting of the findings and critical issues of the AML&CTF systems and procedures to the managers and executives of the Company. The AML&CTF Compliance Monitoring Officer/MLRO ensures that the Company keeps and maintains all required AML&CTF records and that Unusual Activity Reports are filed with FIU when required and appropriate.

The AML&CTF Compliance Officer is vested with full responsibility and authority to enforce the Company's AML&CTF Policy and working procedures. Responsibilities of AML&CTF Compliance Officer includes:

- Spearheads the global AML&CTF drive and is responsible for the overall AML&CTF strategy and policies of the Company.

- Conducts escalation and sanctioning in cases of internal non-compliance or lack of quality with AML&CTF strategy and policies.
- Represents AML&CTF activities at the senior management level.
- Manages central AML&CTF function and controls adequacy of policies, organizational structure and resources devoted to AML&CTF compliance.
- Drives communication to the senior management and other stakeholders with respect to issues concerning AML&CTF compliance.
- Maintains relationships between AML&CTF function and external auditors, regulators and other compliance authorities.
- Oversees and presents to the senior management overview and budget of the AML&CTF activities on a yearly basis.
- Contributes to the elements of the IT-systems related to AML&CTF compliance.
- Presents to senior management the yearly AML&CTF Compliance Report.
- Reports to senior management all cases of non-compliance or inadequate compliance with AML&CTF policies and procedures on ongoing basis, together with recommendations for improvement.

11. CUSTOMER DUE DILIGENCE

11.1 CUSTOMER IDENTIFICATION (KYC) AND SANCTIONS REQUIREMENTS

Customer due diligence measures are in place in the following circumstances:

- a) when establishing a business relationship with client (player) (begins from the registration stage);
- b) upon the collection of winnings, the wagering of a stake, or both, when carrying out transactions amounting to EUR 2 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
- c) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;
- d) when there are doubts about the veracity or adequacy of previously obtained customer identification data.

For transaction (deposit, withdrawal or wagering of a stake) over two thousand (€ 2000) euro in equivalent, customer due diligence is requested immediately. Whether the transaction is carried out in a single operation or in several operations which appear to be linked. Transactions are considered as linked if they are carried out by the same customer through the same game or in one gaming session. A transaction consists of the wagering of a stake or the collection of winnings.

Due diligence procedures, including AML&CTF policy are developed using the risk based approach.

The main responsible department for the Due Diligence process is Factoring and Monitoring (Anti-fraud) Department. In order to perform the due diligence controls, employees use automatic controls, manual reviews and electronic registers.

Enhanced Customer verification could be done in any time of the customers' activity, starting from registration process and continuing through all further processes – deposits, bets, withdrawals. Enhanced controls include full document verification plus any additional requirements until the employee of Anti-fraud department standards are met. For example – several documents, which confirms the address, photo with his ID in hands etc.

If the employee suspects the PEP application, he notifies his Head, who communicate and agrees further actions with the Operational Director and Management Board.

With respect to transactions or business relationships with PEPs, in addition to the KYC measures:

a) The Company have in place appropriate risk management systems to determine whether the customer is a politically exposed person;

b) Apply the following measures in cases of setting relationships with politically exposed persons:

obtain senior management approval for establishing or continuing business relationships with such persons;

take adequate measures to establish the source of wealth and source of funds that are involved in business relationships or transactions with such persons;

conduct enhanced, ongoing monitoring of those business relationships.

Before establishing a business relationship or executing an occasional transaction with a PEP, Anti-fraud department requests adequate documentation to ascertain not only the identity of PEP but also to assess his business reputation (e.g. reference letters from third parties).

11.2 Sanctions requirements for MLTF&FP controls:

Targeted financial sanctions require countries to freeze funds and assets and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of any designated persons or entities. All natural and legal persons in Curaçao are required to freeze without delay and without prior notice, the funds or other assets of designated persons and entities. This is to comply with United Nations Security Council resolutions and the Common Foreign and Security Policy of the European Union. Compliance with sanctions imposed by the UN Security Council is mandatory under the Charter of the United Nations. EU sanctions are binding for Curaçao on the basis of the Kingdom Sanctions Act

Financial Sanctions are prohibitions and restrictions put in place by the United Nations, United Kingdom and OFAC.

They generally target specific individuals or entities, or particular sectors, industries or interests.

The United Nations (UN) imposes financial sanctions and requires UN member states to implement them through Resolutions passed by the UN Security Council.

The United Kingdom (UK) imposes financial sanctions, implemented through a combination of statutory instruments (UK regulations) and primary legislation.

The Office of Foreign Assets Control ("OFAC") of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers.

In order to comply with the main Sanctions rules the Company takes the further steps:

Before undertaking any commercial transactions with Clients, Providers or Partners, seek to know the risks and the most relevant aspects of the transaction, with the aim of identifying potential Red Flags;

- Ensure that Sanctions Due Diligence is duly carried out;
- Ensure that The Company does not deal with Clients, Providers or Partners listed as sanctioned entities or individuals in the aforementioned Sanctions rules and regulations;
- Immediately suspend all activities whenever there are Red Flags as to the possibility of Sanctions violations
- Ensure in a contractual instrument that Clients, Providers and Partners represent that they are not subject to, do not, and will not violate Sanctions;
- Watch for Red Flags throughout the course of the business relationship;

The following are some examples of countries/territories and groups that have been the target of economic trade sanctions: **Russian Federation, Crimea, Cuba, Iran, North Korea, Sudan, Syria, Libya, South Sudan, and Venezuela.**

11.3 SHELL COMPANIES AND MONEY LAUNDERING

Shell companies are corporations created to protect or hide the assets of another company. They only exist on paper and have no physical location, staff, revenue, or significant assets, but they may have bank accounts or investments. While shell companies can be created quickly and affordably in the legal financial system to raise funds, hold stocks, or serve as limited liability trustees, they are not necessarily illegal. However, they are often used for unlawful purposes, particularly as part of money laundering operations. Shell companies can be established by registered agents in most countries to hide Ultimate Beneficial Ownership (UBO). This means that shell companies can be set up with a level of secrecy and then used to conceal illegal funds, evade sanctions, and circumvent anti-money laundering (AML) measures used by companies to detect suspicious financial activity.

To effectively manage the AML risk associated with shell companies and adhere to domestic legislation and FATF guidelines, Rozairo N.V. refrains from establishing any business relationships with such entities.

12. ESTABLISHMENT OF PURPOSE OF BUSINESS RELATIONSHIP

The business relationship between the Company and the client is a commercial relationship arising out of the licensed activities of the bookmaker, in which the client is involved. The business relationship between the client and the Company is likely to be contracted when the client is registered on the website.

At the inception of the business relationship, the Company take into account the following:

- The risk profile of the customer
- The appropriate customer due diligence measures
- Whether it is known or suspected that the customer might legalize revenue from illegal activities

Every customer request for establishment of business relationship is screened against blacklists and verified for the unusual features that might point to an intended abuse of the Company's systems and business practices for AML&CTF.

Rozairo N.V. only accepts individuals whose personal data, disposition and further behavior patterns specifically indicate an intention to lawfully and fairly use the Company's betting services. Such intention could be verified only in part at the inception stage of the business relationship, hence further controls are implemented as the relationship progresses.

13. CONFIRMATION OF ULTIMATE BENEFICIAL OWNER OF THE FUNDS

The ultimate purpose of procedures for monitoring AML-CTF compliance is to prevent the operation, under the guise of ordinary players and on the Company's platform, of the individuals related to or involved in money-laundering and terrorist funding activities. Establishing the identity of the ultimate beneficial owner of the funds is thus the key purpose of the AML-CTF controls at the Company. Operating Control Matrix sets up a number of barriers to prevent the suspect individuals from accessing the Company's legitimate services: credit card verification; denial of service to the customers using someone else's credit cards; single-currency settlement; withdrawal identity verification and many others. There are also delegated responsibilities – for example, for the e-wallets originated deposits, responsibility for customer verification and funds provenance lies with e-wallet.

14. MONITORING

14.1 MONITORING OF THE ACCOUNT ACTIVITIES

This component is central to the Company's AML&CTF efforts. Account monitoring is conducted on the ongoing basis by the officers responsible for various operating aspects of the business. The deposit and withdrawal policies are enforced personally by CFO and MLRO. This enforcement is conducted daily and supported by various thresholds set up to flag the potential problems.

14.2 Overall, monitoring of accounting activities consists of:

- Monitoring of new registrations
- Monitoring of deposit activity
- Monitoring gambling activity
- Monitoring account access
- Monitoring of account detail changes
- Monitoring withdrawal activity
- Monitoring of registration data to ensure it is kept up to date

14.3 Critical controlling measures with respect to MLTF&FP prevention are:

- denial of withdrawals for the inactive funds
- detection of the unusual payment patterns (i.e. deposit activity does not match the betting activity or large deposit movements unwarranted by the betting patterns)
- periodic screening of e-wallets used by the players
- pro-active recognition and prevention of players' fraudulent intentions or activities. This component is an indirect indication of probable MLTF&FP threats.

Employees of Rozairo N.V. seeks to identify the following indications of the potential MLTF&FP threats:

- Individual or linked transactions which are complex or unusually large with no apparent or lawful economic purpose, including those relative to a relationship;
- Unusual patterns of transactions with no apparent economic or lawful purpose, including those relative to a relationship;
- Transactions which exceed certain limits with no apparent economic or lawful purpose, including those relative to a relationship;
- Very high account turnover inconsistent with the balance;
- Transactions, which are outside of the customer's regular transaction activity.

15. REPORTING SUSPICIOUS ACTIVITIES AND TRANSACTIONS

All suspicious activities and transactions are recognized and recorded in the system. All suspicious activities / transactions, including attempted transactions reported internally first. The officers responsible for respective areas of transaction monitoring report the suspicious activities to MLRO immediately upon identification, together with a brief description of specific mitigating measures taken. Such reporting is performed in both oral and written form depending on gravity of an incident reported.

The Company's general approach is to file the written report only in cases of reasonable suspicion of substantial violation of Regulations or substantial threat to the business. A degree to which a particular violation or threat is deemed "substantial" is left to the discretion of the officer in charge of specific controlling area and their respective upper management. Due to the fast-moving nature of the business, the management feels that this approach is fully justified.

Employees' may report a suspected instance of ML/FT to the MLRO even when their immediate superior is in disagreement with them. The MLRO must determine if the information available can be considered as sufficient for STR to be made to the FIU

In addition, all transaction equal or exceeding the threshold of USD 2,500 or equivalent are considered unusual under the National Ordinance on the Reporting of Unusual Transactions related to the online gaming sector, and thus will be reported to the FIU Curacao via the GoAML portal under the objective indicator.

16. EMPLOYEES

16.1 STAFF RELIABILITY AND PROBITY

The business of Rozairo N.V. is an amalgamation of appropriately qualified people and past-paced technological innovation. Employees are one of the most valuable assets and a critical component of the Company's operating model. In an intense, gain-driven betting environment, staff reliability and probity is of paramount importance to an extent unseen in other businesses.

The Management of Rozairo N.V. recognizes this and, therefore, the employees are expected to:

- conduct their activities in accordance with direct instructions of the immediate supervisors
- exercise sound judgment in situations requiring initiative and unsupervised decision-making
- behave ethically towards the company, colleagues, clients and third parties
- be fair, honest, dependable and accountable in business dealings
- avoid business and personal actions that might cast appearance of impropriety or ethical ambiguity
- comply with the respective HR policies and regulatory requirements
- declare any actual or perceived conflicts of interest as soon as such conflicts become known
- maintain confidentiality and prevent the disclosure of the confidential information
- refrain from accepting inducements, incentives, gifts or other benefits from the colleagues and third parties that may lead to, or may be seen as leading to, an unfair advantage to third parties or to unfair treatment of the business
- communicate internally and with the third parties using clear and concise meanings, in a timely manner and via the established communication channels
- decline invitations from the mass media and the Internet-based platforms (forums, info-aggregators, news originators and others) to discuss the Company's business.

16.2 SCREENING

The company developed and supports the HR and control policies and procedures for effective initial screening of candidates and subsequent dealings with employees:

- All personnel undergo the initial procedure for personal identification.
- During the first interview, all candidates are required to complete the ID profile designed by HR Department. The ID profile includes a number of psychological tests designed to determine whether a candidate might inflict, under certain conditions, harm to the company.
- Upon completion of the ID profile and analysis by the HR Department, the recruiter conducts initial interviews with the candidates using a number of further psychological tests.
- Following the conclusion of the initial interview, the second interview by HR Director is conducted for the successful candidate.
- The next step in the hiring process is a conversation with the subject area manager, followed by the meeting with a member of the internal security department.
- Conduct, by a member of internal security department, of the background check on the candidate including, but not limited to, communication with the previous immediate supervisor of the job candidate; verification of the criminal record; examination of job references and communication with the sources; search in the open public sources and the Internet.

Having succeeded in the screening process in its entirety, the new employees are given the mandatory introductory course in their respective areas for three weeks and have to pass the exams as follows.

Stage 1: Employee adaptation and lectures on the bookmaking basics. Exam.

Stage 2: Lectures on the payment systems. Exam and issuance of the internal certificate.

Stage 3: Learning how to work with the software. Exam.

Stage 4: Lectures on dealing with customer complaints.

Stage 5: Training at the workplace and a final exam.

After successful completion of all five stages, the employee commences the duties in probation mode under close supervision of a member of the internal security department and the direct area manager.

For the candidates applying to executive positions, the hiring procedure involves a mandatory personal conversation with the CEO upon which the final decision to hire is made.

16.3 PROFESSIONAL SUPPORT AND TRAINING

The company supports professional efforts by its employees to remain at the forefront of the best practice and technological innovation in the e-gambling and betting industries. It is recognized that such support may take several forms including but not limited to the on-site and distance training, ad-hoc working groups, technical and situational seminars and some others.

The company offers training courses and conducts a series of seminars for the employees in the varied subject areas of direct interest to the business.

Trainings in Business Administration are conducted for managers of the company, which include five main blocks: building of the management platform, forming the levers of managerial effectiveness, integration of the management skills, the development of business in the global sphere, and also training courses of business English are conducted for all employees of the company.

Professional upgrade courses are conducted internally for the staff of Trading and Operational Departments by the divisional heads and Directors of respective departments.

Marketing Department staff participates in various training conferences on various aspects of marketing, including the practice of e-mail marketing; SEO optimization, ICE Totally Gaming, web analytics, etc.

The Finance Department staff participate in training courses on the subjects of management accounting, budgeting and planning, internal controls, and management finance.

16.4 AML TRAINING

The MLRO is responsible for the conduct of the introductory AML&CTF training course for every new employee and the subsequent AML&CTF updates in the “what?” and “how to?” format including:

- what is the employee role in the Company’s compliance effort and how to perform the individual compliance duties
- what are and how to identify red flags and indications of money laundering that may arise in the course of the employee daily duties
- what to do once the risk is identified (including how, when and to whom to communicate the initial suspicion and how to escalate the level of awareness of the threat for further processing and analysis) - what are the latest tools, updates and improvements in the AML&CTF investigations.

The MLRO keep a register of all trained employees of the Company dealing with monitoring of transactions, engaged in the management of the company, any authorized representatives and/or responsible persons.

17. RECORD-KEEPING

A complete history of each player's account transactions starting from the date of account opening and to his latest bet is saved on the computer system. The system keeps the following information:

- Primary customer data (required at the registration stage) i.e. country of the player, currency selected, e-wallets used and other. If a combination of risk triggers gives rise to a particular concern, the employees of Anti-Fraud Department and Payment and Anti-Fraud Department react according to the set of given circumstances.
- Comments by the employees of the respective departments concerning each player account.
- System also keeps records regarding profitability of each gaming account for the entire period of its existence – also utilized as an MLTF&FP risk trigger.

- All suspicious activities and transactions are recognized and recorded in the system. Upon receipt of the Report on suspicious activities and transactions, MLRO decides as to the further course of actions concerning possible reporting of the transactions to authorities and licensing authority.

All transactions history of a player including amendments, additions and deletions to the transactions are kept for records for 5 years' period. For customer due diligence data and information, the holding period is 5 years following the date of cancellation of customer relationships. Records are maintained on company servers and instantaneous back-up is performed.

Signature Page

Approved by the Board of Directors:



Theoklis Andreou

