

LOSARTEZ B.V. POLICY

for Prevention and Combatting of Money Laundering and Terrorist Financing

W

VERSION CONTROL

Version	Version Date	Approved By
2.1	30 March 2026	The Board

W

CONTENTS

VERSION CONTROL.....	1
CONTENTS	2
ABBREVIATIONS	3
1. PREAMBLE	4
THE POLICY	4
DEFINITION OF ML, TF & FP	4
TARGETED FINANCIAL SANCTIONS	5
RELIANCE ON THIRD PARTIES PROVIDERS	5
PURPOSE OF THE POLICY	6
2. RISK BASED APPROACH	7
DEFINITION	7
BUSINESS, CUSTOMER & SECTOR RISK ASSESSMENT	8
INTERNAL CONTROLS & AUDIT FUNCTION	13
AML&TF DESIGNATED OFFICER	14
3. CUSTOMER DUE DILIGENCE	15
INTRODUCTION.....	15
THE CDD MEASURES	15
ENHANCED DUE DILLIGENCE.....	17
SIMPLIFIED DUE DILLIGENCE	18
POLITICALLY AND SANCTIONS EXPOSED PERSONS.....	18
ESTABLISHMENT OF PURPOSE OF BUSINESS RELATIONSHIP.....	19
CONFIRMATION OF UBO OF THE FUNDS	20
IDENTIFICATION AND VERIFICATION SYSTEMS	20
4. MONITORING	22
ONGOING MONITORING OF IDENTITY	22
TRANSACTIONS MONITORING	22
MONITORING OF THE ACCOUNT ACTIVITIES.....	23
MONITORING OF HIGH-RISK CLIENTS	24
REPORTING ACTIVITIES AND TRANSACTIONS	25
5. EMPLOYEES	26
STAFF RELIABILITY AND PROBITY.....	26
SCREENING	26
PROFESSIONAL SUPPORT AND TRAINING.....	27
AML TRAINING	28
6. RECORD-KEEPING	29
7. RATIFICATION	30
APPENDICES	31
APPENDIX A. OPERATING CONTROL MATRIX (FRAGMENT).....	31
APPENDIX B. SAMPLE OF CUSTOMER TRACK-RECORD	32



ABBREVIATIONS

AML, TF & FP	Anti-money laundering, prevention of the terrorist financing & financing of proliferation
BO	Beneficial Owner
CDD	Customer Due Diligence
CEO	Chief Executive Officer
CGA	Curacao Gaming Authority
CFATF	Caribbean Financial Action Task Force
CFO	Chief Financial Officer
CRA	Customer Risk Assessment
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
KYC	Know your customer
MLRO	Money Laundering Reporting Officer
NOIS	National Ordinance on Identification of clients when Rendering Services
NOPML	National Ordinance Penalization of Money Laundering Regulations
NORUT	the National Ordinance on the Reporting of Unusual Transactions
NRA	National Risk Assessment
PEP	Politically Exposed Person
RBA	Risk Based Approach
SDD	Simplified Due Diligence
SoF	Source of Funds
SoW	Source of Wealth
The Policy	the Policy on Prevention of Money Laundering and Terrorist Financing
UBO	Ultimate Beneficial Owner
URT	Unusual Transaction Report



1. PREAMBLE

THE POLICY

The Policy outlines the general unified standards and procedures of AML, TF & FP which must be adhered to by Losartez B.V. (Hereinafter — «the Company») its directors, officers and employees. The Company is duly licensed and supervised by the Curaçao Gaming Authority (“CGA”), which acts as the competent supervisory authority for the Company’s gaming operations and compliance with applicable AML/CTF regulatory requirements.

The NOIS, NORUT, the Sanction National Ordinance, and the Kingdom Sanction Act all contain provisions requiring service providers to take measures to prevent their services from being used for money laundering, terrorism financing, and the proliferation of weapons. Please also refer to the dedicated Sanction Policy, which forms an integral and enforceable part of the AML framework.

Countries collaborate to combat these issues through the FATF, which was established during the 1989 G-7 Summit in Paris. The Dutch Kingdom is a member of the FATF, while Curaçao is part of the CFATF.

- article 2 paragraph 8 and article 11, paragraph 3, of the NOIS (N.G. 2017 no. 92) and;
- article 22mm, paragraph 3, of the NORUT (N.G. 2017 no.99);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no

54) Among others, current AML policy refers

to:

- The NOIS (N.G. 2017, no. 92);
- The NORUT (N.G. 2017, no. 99);
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the NORUT
- Regulation Indicators Unusual Transactions (N.G. 2015, no. 73);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations’ Security
- Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- National Decree for general measures, of the 10th July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations’ Security
- Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions
- Decree People’s Democratic Republic of Korea 2015) (N.G. 2015 no. 30);
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48).
- Any regulations, policy rules, guidelines, directives, or other regulatory instruments issued by the Curaçao Gaming Authority (“CGA”) or any other competent regulatory or governmental authority in Curaçao, insofar as applicable to the Company’s licensed gaming operations and its AML/CTF/CPF obligations.

For the purposes of this Policy, the above-mentioned laws, national ordinances, decrees, regulations, and supervisory guidance shall collectively be referred to as the “Applicable AML/CTF Regulatory Framework” or the “Regulations”, as appropriate.

DEFINITION OF ML, TF & FP

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 derived from legitimate origins or constitute legitimate assets. Money laundering may generally occur in three phases.

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 traveller'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 AML, TF & FP 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 behaviour to the relevant regulatory or legislative authority.

Terrorist financing may not always involve funds derived from criminal activities; instead, it often seeks to hide the origin or intended use of funds, which could be for illicit purposes. The primary distinction between terrorist financing and money laundering lies in the source of the funds. Unlike traditional criminal organizations, terrorist financiers may rely on legitimate sources of funding. These sources can include charitable donations, foreign government support, business ownership, and personal employment. Despite differing motivations, the methods used to finance terrorism can be similar to those employed by criminals to launder money. Terrorist operations may not require large sums, as funding can be accumulated over time, with transactions that are relatively simple and not immediately suspicious.

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.

JURISDICTION RESTRICTIONS AND TARGETED FINANCIAL SANCTIONS

The Company has developed a dedicated Sanctions Policy, which constitutes an integral part of this Policy and the Company's AML framework. The Company is required to comply with all jurisdictional restrictions and sanctions requirements imposed by the CGA, other competent regulatory or governmental authorities, and the laws of jurisdictions applicable to the Company's operations.

Targeted financial sanctions require countries to freeze funds and assets, ensuring that no funds or assets are made available, directly or indirectly, to designated persons or entities. In Curaçao, all individuals and legal entities must promptly and without prior notice freeze the funds or assets of designated persons and entities. This obligation aligns with United Nations Security Council resolutions and the European Union's Common Foreign and Security Policy. Compliance with UN Security Council sanctions is mandatory under the United Nations Charter, while EU sanctions are binding on Curaçao through the Kingdom Sanctions Act. Mechanisms must be in place to verify the sanction status of withdrawing participants to prevent sanctioned individuals or organizations from accessing funds that should be frozen. The Company does not offer services to residents of, or persons located in, prohibited jurisdictions as follows:



Sanctioned jurisdictions: Countries and territories subject to sanctions or restrictive measures under:
United Nations Security Council resolutions;
European Union restrictive measures applicable through the Kingdom Sanctions Act;
The Sanctions National Ordinance (N.G. 2014, no. 55) and implementing decrees;
OFAC sanctions programs;
Countries on the FATF list of High-Risk Jurisdictions Subject to a Call for Action;
Any local Curaçao sanctions lists published by the CGA or other governmental bodies.

High-risk and monitored jurisdictions: Countries and territories identified as presenting heightened ML/TF risk, including:

Countries on the FATF list of Jurisdictions under Increased Monitoring;
Countries on the CFATF Public Statement;
Countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR);
Countries on the European Commission's list of third countries having strategic deficiencies in their AML/CFT regime;
Countries identified by credible sources as providing funding or support for

The list of prohibited jurisdictions is continuously monitored by the Company's Compliance Officer, and any update triggers an internal compliance review to assess the necessity of mitigation actions. Such review includes identification of any existing players affected by newly prohibited jurisdictions, immediate suspension of affected accounts, assessment of any sanctions freezing obligations, return of non-frozen funds to the original payment source where permitted, and filing of reports with the FIU and/or CGA as required. The Company's technical controls (registration blocks, IP screening, payment instrument restrictions) are updated promptly to reflect any changes to the prohibited jurisdictions list.

The Company maintains a current master list of all prohibited jurisdictions, which is approved by senior management and the Compliance Officer, reviewed at least quarterly (or immediately upon receipt of new regulatory guidance or sanctions designations), integrated into the Company's registration, payment, and monitoring systems, and made available to the CGA upon request.

RELIANCE ON THIRD PARTIES PROVIDERS

The Company may, where appropriate and permissible under applicable laws, rely on third-party providers (such as payment processors, KYC/AML verification vendors, or other regulated entities) to perform certain aspects of customer due diligence and monitoring. Such reliance is only accepted where the provider is subject to equivalent AML/CTF obligations, has been assessed for reliability and competence, and where contractual arrangements are in place to ensure compliance.

Notwithstanding this reliance, the Company retains ultimate responsibility for compliance with all AML/CTF requirements. The Compliance team ensures that third-party providers are monitored on an ongoing basis, with periodic reviews of their performance, data integrity, and adherence to contractual obligations. Any deficiencies identified in third-party processes are addressed immediately, and corrective measures are enforced to safeguard the Company's compliance framework.

Where third-party game providers or gaming-related technology suppliers are integrated into the Company's operations, the Company ensures that such outsourcing arrangements do not impair the effectiveness of its AML/CTF framework or its ability to comply with applicable regulatory obligations.

In this respect, the Company applies appropriate risk-based controls over gaming suppliers and related



systems, including, where applicable:

- conducting due diligence on the provider's licensing status, reputation, integrity standards, and compliance capabilities prior to onboarding;
- ensuring that contractual arrangements require the provider to support the Company's AML/CTF obligations, including cooperation with compliance reviews, audits, and regulatory requests;
- maintaining appropriate access to relevant betting, gameplay and transactional data, including system logs and audit trails, to enable effective monitoring, investigation and escalation of unusual or suspicious wagering activity;
- assessing whether specific game mechanics, betting structures or product features could facilitate rapid fund turnover, collusion, minimal-play laundering, or other activity inconsistent with the legitimate purpose of gaming;
- implementing escalation procedures where anomalies, integrity concerns or suspicious behavioural patterns arise in connection with particular games, platforms or providers, including referral to the MLRO where necessary.

These measures ensure that third-party gaming content and supporting technology operate within the Company's overall compliance environment and do not create vulnerabilities that could be exploited for money laundering, terrorist financing or proliferation financing purposes.

PURPOSE OF THE POLICY

As indicated, the Regulations are applicable for Curaçao Gaming Sector in order to combat ML, TF and FP, and are effective as of 10 April 2025. All online operators are bound to comply with these Regulations in order to ensure that the Company is fully comply with applicable AML, TF & FP and terrorism financing laws and regulations of respective countries and jurisdictions. The Compliance Officer shall serve as the owner of this Policy and is responsible for its maintenance, periodic review, and coordination of any amendments. The Company 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. The Compliance Officer may initiate interim reviews where warranted by material regulatory developments, significant changes to the Company's business model, or other circumstances that may affect the adequacy of this Policy.



2. RISK BASED APPROACH

DEFINITION

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&TF procedures, systems and personnel.

The foundation of the risk-based approach is the risk assessment that the Company must conduct on its own operations. This involves understanding and evaluating the general risks to which the business is exposed, known as the business risk assessment.

The Company has identified the following key ML&TF risks.

1. The risk of accepting the customers whose identities and/or addresses are hidden to conceal the direct relation to ML&TF activities (for example, use of multiple passports to conceal the true 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).

An anti-ML compliance program is an essential component of a Company's compliance regime. The primary goal of every good program is to protect the organization against ML and to ensure that the organization is in full compliance with relevant laws and regulations.

Based on the FATF Recommendations, igaming companies are required to apply a Risk-based Approach to ensure that measures to prevent or mitigate money laundering, financing of terrorism and proliferation of weapons are commensurate with the risks identified.

Applying Risk-based Approach means that the Company:

- Assess the risks that money laundering or terrorist financing may occur within its organization beforehand;
- Design and implement appropriate policies, procedures and controls to manage and mitigate the identified and assessed risks;
- Monitor and improve the effective operation of these policies, procedures and controls;
- Document their risk assessments, including everything that has been done and the reason for this being done.

Risk assessment process for ML&TF 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 ML&TF 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 ML&TF risk. For example, the first deposited amount from a new client is usually accepted at the lowest allowable threshold, thus containing the ML&TF 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.

Given that risks are dynamic, the Company subscribes to continuously monitor the effectiveness of these policies, procedures, and controls, making necessary adjustments as needed. The risk assessment must also be made available to the CGA upon request.

BUSINESS, CUSTOMER & SECTOR RISK ASSESSMENT

The higher the risk, the more measures the Company has to take to mitigate the risk. Where the risks are higher enhanced measures must be taken. Where the risks are lower, they may take simplified measures, provided that this is consistent with the country's assessment of its money laundering/financing of terrorism risks. Following risk segments have to be considering during the operation.

BUSINESS RISK ASSESSMENT

The Company carries a business risk assessment to identify the ML/TF risks it is exposed to and ensure that the policies, controls and procedures adopted are adequate to prevent and mitigate those risks. The risk assessment addresses the ways in which the products and services could be used to launder money, finance terrorism and finance proliferation and the extent of the risk that this will happen. Special consideration is given to the type of customers, products and services offered, delivery channels and geographical risk factors. The Company includes the outcomes and recommendations of the NRA in its business risk assessment, which allows to set a risk appetite. The effectiveness of the implementation of these measures has to be monitored and improved where necessary.

The Company subscribes to revise the business risk assessment whenever there are changes to the environment, such as introduction of new payment methods, new markets, new games or regulatory changes. In the absence of changes, the Company will assess its business risk at least once a year, to evaluate whether any changes thereto are necessary. In order to work risk-based, it is important that the Company continuously follow the latest reporting regarding money laundering and terrorist financing.

This risk assessment has to be documented, approved by the Board of directors of the Company and made available to the CGA upon request. The Company maintains a standalone Business Risk Assessment document, which sets out in detail the methodology, risk factors, and analysis underpinning the Company's enterprise-level ML/TF risk assessment. The Compliance Officer is responsible for maintaining the Business Risk Assessment and shall ensure it is reviewed and updated at least annually, or more frequently where material changes to the business, regulatory environment, or risk landscape warrant. Amendments to supporting methodologies and analysis may be made by the Compliance Officer without requiring Board approval, provided that any material change to the overall risk appetite or conclusions is submitted to the Board for approval.

CUSTOMER RISK ASSESSMENT

Each player presents unique risks to the Company. As a result, a player-specific risk assessment is necessary for the Company to identify potential risks associated with establishing a business relationship or conducting a one-time transaction with a player, referred to as the CRA. This assessment allows the Company to create a risk profile for the customer and categorize the money laundering or terrorist financing (ML/TF) risk posed by the player as low, medium, or high.

The customer specific risk assessment is carried out either prior to the carrying out of an occasional transaction, or during establishing a business relationship. The initial customer specific risk assessment can



be revised at a later stage of the business relationship, which might result in customer's risk rating adjustment.

There are a number 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 ML&TF 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 ML&TF 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 ML&TF 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 Company's relationship with a customer builds up thus allowing for equally commensurate increase in the volumes of business conducted.

Based on the dimensions described above, a specific ML&TF risk is classified as low, medium and high; depending on classification, different actions are called for from the Compliance Officer and other employees involved in ML&TF controls. Typical actions for high-risk detection situations are increase in the time lag for withdrawals and acceptance of the customer funds and enhanced verification of the customer.

On the basis of the CRA, the proper level of CDD is applied. The Company maintains a standalone Customer Risk Rating Matrix, which sets out the specific risk factors, weightings, scoring methodology, and thresholds used to assign customers to low, medium, or high risk categories. The Compliance Officer is responsible for maintaining and updating the Customer Risk Rating Matrix as an operational document, and may amend its contents as necessary to reflect changes in risk indicators, payment methods, jurisdictions, or regulatory guidance, without requiring Board approval. The Customer Risk Rating Matrix is treated as a confidential operational tool and is not routinely disclosed to third parties. All other measures stated above are documented and approved by the Board of directors.

SECTOR RELATED RISK ASSESSMENT

The Company operation covers a vast set of countries, some of which might possess 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 impact the Company's business.

This means that the Company employs a policy of high alertness when entering a new market, managing 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 is country-based and country specific in nature.

There are four sector related risk areas that the business has to cover, as follows:

1. Customer risk

It arises from maintaining relations with a given person. The assessment of the risk posed by a natural person is generally based on the person's economic activity and/or SoW. Categories of customers whose activities may indicate a higher risk include:

- Customers who have multiple sources of income;
- Customers with irregular income streams;
- PEPs;
- High spenders (money can be derived from illegal activities)
- Disproportionate spenders (inconsistent with customer's known source of income/assets);
- Casual customers like locals/tourists, especially when spending pattern changes;
- Improper use of third parties, criminals use third parties to gamble to break up large amount of cash, to buy chips or to cash out on behalf of others to avoid CDD measures;



- Multiple accounts to hinder Company's tracking of their gambling activities;
- Unknown customers (redeeming large amounts of chips);
- Junkets (monitor player activity and issues and collect credit).

The Company must set a value which represents the upper value of a typical player's transactions. A player having a single source of regular income will pose a lesser risk of ML/TF than a player who has multiple sources of income or irregular income streams.

2. Geographical risk

The geographical risk is the risk posed to the Company by the geographical location of the player and the SoW of the business relationship. The nationality, residence, and place of birth of the player have to be taken into account as these might be indicative of a heightened geographical risk. The Company adheres to the framework of prohibited jurisdictions and targeted financial sanctions as described in the Preamble of this Policy and the dedicated Sanctions Policy. The Company maintains a list of countries that are considered high risk and those that are considered low risk.

The following controls are applied to enforce geographic restrictions:

- Country of residence declaration: All prospective players must declare their country of residence during identification procedures. The system automatically blocks account creation and access where any indication of a prohibited jurisdiction is detected.
- Identity document verification: During the CDD process, the player's identity documents are reviewed to confirm country of residence and nationality. Where documents indicate residence in or nationality of a prohibited jurisdiction, the account is suspended pending further review.
- Payment method screening: The Company screens the country of issuance of payment instruments (e.g., credit cards, bank accounts, e-wallets) used for deposits. Payment instruments issued in prohibited jurisdictions are declined.

Geographic restrictions are enforced on an ongoing basis throughout the customer relationship:

- Continuous IP monitoring: The Company monitors player IP addresses during login and gameplay sessions. Players accessing the platform from IP addresses associated with prohibited jurisdictions are subject to immediate session termination, account suspension pending investigation, and a request for explanation and/or updated proof of residence.
- Proxy detection: The Company employs technical measures to detect the use of proxy servers, or other tools that may be used to mask a player's true location. Detected use of such tools results in account review and potential suspension.
- Periodic re-verification: During routine CDD refresh (e.g., document expiry, threshold triggers), the Company re-verifies the player's country of residence. Changes in residence to a prohibited jurisdiction result in account termination.
- Sanctions list rescreening: All active players are rescreened against updated sanctions lists upon publication of new designations. Players identified as residents of newly sanctioned jurisdictions, or as designated persons, are subject to immediate account freezing and reporting to the FIU as required.
- Player self-declaration updates: Players are required under the terms and conditions to notify the Company of any change in residence. Failure to do so constitutes a breach of terms and may result in account termination.

3. Product, service and transaction risk.

Specific payment methods, which are considered to present a higher risk of ML/FT, are treated as high risk factors. These include:

Proceeds of crime. Risk that money transferred is derived from illegal activities such as check fraud, credit/debit card fraud, narcotics trafficking and theft from employer;

Anonymous payment methods such as pre-paid cards and virtual assets;

Use of gaming accounts. This should only be done for gambling purposes and not to deposit and withdraw without gambling or minimal play;

Types of specific games (e.g., roulette, craps → even bets);

The use by customer of accounts held or cards issued in the name of third parties;

Types of financial services (credit/marker, currency exchange, check cashing);

Multiple accounts or wallets (the Company may own and control multiple web sites);

Changes to financial institution accounts to fund player's account;

Identity fraud. Details of financial institution accounts stolen and used on web sites. Also stolen identities used to successfully open financial institutions accounts, and such accounts used on web sites;

Using cash to fund a pre-paid card poses similar risks as cash;

Electronic wallets (e- wallets). Not all e-wallets are licensed in reputable countries, and a number of e-wallets accept cash as deposits. Also, e-wallets which only accept money from financial institution accounts; the financial institution issued statements may only record the payment to the e-wallet, not the transaction to the Company. This may be useful for dishonest customers who wish to disguise their gambling.

4. Distribution channels risk

The channels through which the Company establishes a business relationship or through which transactions are carried out may also have an impact on the risk profile of a business relationship or a transaction:

- Channels that favour anonymity increase the risk of ML/FT if no measures are taken to address the risk;
- While situations where interaction with the customer takes place on a non-face-to-face basis no longer led to the relationship being considered as automatically high risk, interacting in this manner is still to be considered as a high-risk factor for risk assessment purposes unless the Company adopts technological measures and controls to address the heightened risk of identity fraud or impersonation present in these situations;
- Where there is the involvement of a third party in the interactions between the customer and the Company, there is also an increase of risk. This is especially the case where these third parties are not themselves subject to any form of AML/CFT obligations.

PRODUCT AND BETTING ACTIVITY RISK ASSESSMENT

In addition to general customer, geographic and payment-related risk factors, the Company recognizes that online gaming and sports betting services present specific inherent vulnerabilities to money laundering, terrorist financing and proliferation financing due to the nature of gaming activity and the speed of remote transactions.

Accordingly, the Company incorporates gaming-specific risk indicators into its Risk-Based Approach, ensuring that AML/CTF controls are tailored to the particular mechanics of its products, betting markets and player behaviour.

The Company assesses, monitors and mitigates the ML/TF risks arising from, inter alia:

- Game mechanics and product design, including games or betting types that may facilitate rapid turnover, low-risk wagering, or limited economic rationale beyond fund movement;
- Wagering and staking patterns, including activity that is inconsistent with recreational play, such as repetitive low-margin betting, minimal-risk bets, or staking strategies indicative of fund placement or layering;
- Low-play or no-play activity, where deposits are followed by limited gaming engagement and rapid

- withdrawal requests, suggesting potential misuse of the gaming account as a transactional conduit;
- Player behavioural anomalies, including unusual frequency, velocity, or structuring of bets, use of multiple events or obscure markets, or activity inconsistent with the player's established risk profile;
- Potential collusion or third-party misuse, including indicators of chip-dumping, coordinated betting against the same counterparties, or other patterns suggesting that accounts may be used to transfer value between players;
- Bonus and promotional abuse, where incentives or loyalty mechanisms are exploited to disguise the origin or legitimacy of funds.

The outcome of this gaming-specific risk assessment is reflected in the Company's customer risk profile, determination of appropriate due diligence measures, and the application of proportionate monitoring and control mechanisms as further described in this Policy and in the Operating Control Matrix.

To mitigate the risks arising from online gaming products and wagering activity, the Company applies a combination of automated and manual control measures, proportionate to the customer and transactional risk profile. Such measures may include, inter alia:

- Behavioural flagging and alert generation, where player activity triggers risk alerts based on abnormal wagering velocity, repetitive low-risk bets, minimal-play patterns, or unusual deposit-bet-withdrawal cycles;
- Restrictions on peer-to-peer or third-party value transfers, including prohibitions on any gaming-related transactions that may enable indirect movement of funds between players outside the legitimate purpose of wagering;
- Enhanced review of withdrawals following limited gaming activity, where withdrawal requests are escalated for compliance assessment if inconsistent with the expected nature of play or the player's established profile;
- Controls against collusion and coordinated betting, including monitoring for chip-dumping typologies, repeated play against the same counterparties, or patterns suggesting that accounts are being used to transfer value rather than to gamble;
- Game and market integrity oversight, including heightened scrutiny of betting on obscure events, suspicious leagues, or markets vulnerable to manipulation or fixed-match risk;
- Application of transactional thresholds, delays or account limitations, where appropriate, to prevent rapid turnover or layering through gaming accounts;
- Escalation and case management procedures, whereby unusual or suspicious gaming behaviour is promptly reviewed by the relevant operational teams and escalated to the Compliance Officer for determination of whether reporting obligations to the FIU Curaçao are triggered.

These gaming-specific controls are applied in conjunction with the Company's broader customer due diligence, risk scoring, and transaction monitoring framework, ensuring that the gaming platform is not misused as a mechanism for laundering proceeds of crime or financing illicit activity.

VIRTUAL ASSETS AND CRYPTOCURRENCY RISK MANAGEMENT

The Operator may accept deposits and process withdrawals using virtual assets, including cryptocurrencies. Virtual asset transactions are recognised as presenting a higher inherent risk of money laundering and terrorist financing due to their pseudonymous nature and transaction speed.

1. Wallet screening and blockchain analytics

Where appropriate and proportionate to the assessed risk, the Operator may make use of blockchain analytics or wallet screening tools to support transaction monitoring and risk assessment. Such tools are used as a supplementary risk-assessment measure and do not replace the Operator's obligation to apply professional judgement and a holistic assessment of the customer relationship. Transactions involving third-party wallets,

mixing services, privacy-enhancing technologies, or other obfuscation techniques may trigger enhanced due diligence or further review.

2. Reliance on VASPs

Where cryptocurrency transactions involve Virtual Asset Service Providers (VASPs), the Operator applies reasonable, risk-based measures to assess the VASP's credibility and regulatory status, where such information is available. Findings arising from cryptocurrency transaction monitoring, wallet screening, or VASP assessment are evaluated in conjunction with Source of Funds and Source of Wealth information and the customer's overall risk profile. Where cryptocurrency transactions give rise to reasonable grounds to suspect money laundering or terrorist financing, the Operator shall report the transaction without delay to the Financial Intelligence Unit Curaçao, in accordance with the National Ordinance on the Reporting of Unusual Transactions.

All cryptocurrency deposits and withdrawals are subject to ongoing monitoring in accordance with the risk-based approach required under applicable anti-money laundering legislation.

3. Governance and Board-level Oversight of Virtual Asset Risks

The Board of Directors retains oversight responsibility for the risks associated with the acceptance and use of virtual assets, including cryptocurrencies, within the Operator's business model.

In relation to virtual asset activities, the Board of Directors shall, at a minimum:

- approve the Operator's approach to managing money laundering and terrorist financing risks arising from cryptocurrency deposits and withdrawals;
- receive periodic reporting on material virtual asset-related AML risks, including significant findings from transaction monitoring, wallet screening, or reliance on Virtual Asset Service Providers; and
- ensure that appropriate controls, resources, and systems are maintained to mitigate risks associated with virtual asset transactions.

4. AML Reporting on Virtual Asset Risks to Senior Management and the Board

Day-to-day monitoring of virtual asset transactions may be delegated to the Compliance Officer and relevant operational teams; however, material issues, elevated risk exposures, or significant incidents relating to cryptocurrency activity shall be escalated to senior management and, where appropriate, to the Board of Directors without undue delay.

Information on cryptocurrency-related AML risks shall be reported to senior management and the Board of Directors on a periodic basis, and at a minimum annually, as part of the overall AML and risk reporting framework. Where the Operator's exposure to virtual asset transactions is material, such reporting shall be provided at least quarterly to senior management.

In addition to periodic reporting, material cryptocurrency-related AML issues shall be escalated to senior management and, where appropriate, to the Board of Directors without undue delay

OTHER RISKS

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:

1. Potential complicity of employees;
2. Use of false or stolen identity documents by players;
3. Concealment of the identity of the BO;

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 Company to identify the SoF;
9. Remote gambling used as a front for cash deposits, which are then transferred to bank accounts, with apparent winnings from gambling as the SoF;
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 BO's SoW or SoF 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 ML&TF 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 scepticism among employees are the best general preventive measures that could help timely identification recognition of suspicious transactions in terms of ML&TF risks. The management believe that fostering the general alertness, risk awareness and the spirit of constructive scepticism among employees is the best general preventive measure that could prevent ML&TF risks from materializing.

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

- a) are complex transactions;
- b) are 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 different risk categories. For each client, the Company will evaluate the risk factors to establish the degree of

risk, which will be established as a result 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.

TEHCNOLOGICAL DEVELOPMENTS RISK ASSESSMENT

The Company has appropriate procedures and controls for preventing the misuse of technological developments for the purpose of money laundering or the financing of terrorism. It monitors and assess the money laundering or terrorist financing risks that may arise whenever:

- A new product is developed;
- A new business practice emerges;
- A new delivery mechanism becomes available;
- A new or developing technology is used for both new and pre-existing products.

A risk assessment takes place prior to the launch of the new products, business practices, delivery mechanism or the use of new or developing technologies. This is done to determine whether the innovation creates a weakness that can be misused by money launderers or those seeking to finance terrorism.

INTERNAL CONTROLS & AUDIT FUNCTION

The Company internal controls are a set of policies and procedures aimed at securing the efficient and compliant business and provision of the safe and fair gambling environment for the customers. Overall logic of the internal controls at the Company is described by Operating Control Matrix (presented in Appendix A). The Matrix is a practical guidance on various controls mandatory for execution in the course of the daily business of the Company. The matrix is updated on an annual basis to reflect the changing business requirements and regulatory changes in the markets in which the Company operates. These functions may be performed by an independent internal audit team (those members cannot be part of operations or compliance teams) or an outside independent provider.

The AML compliance program is monitored and evaluated at least annually by an outside independent party. The people performing the audit are in no way involved with the Company's AML compliance staff and are sufficiently qualified to ensure reliability of the delivered results. The audit covers information including:

- An evaluation of the Company's AML & CTF policy;
- Customer's file review;
- Compliance management;
- Performance of transaction testing;
- Assessment of training adequacy;
- Assessment of compliance with applicable laws and regulations;
- Evaluation of the system's ability to identify unusual activity;
- Interviews with employees who handle transactions and with their supervisors;
- A sampling of unusual transactions on and beyond the threshold(s) followed by a review of compliance with the internal and external policies and reporting requirements; and
- An assessment of the adequacy of the record retention system.

The assessment will also include an analysis of whether the Company was responsive to earlier audit findings. All the results are documented with the deficiencies reported to the designated Compliance Officer, with a request to take prompt corrective actions by a certain deadline.

The Board of Directors shall, on an annual basis, formally certify that:

- the Company's AML&TF policies, procedures, and internal controls have been reviewed and remain adequate and effective;
- the Company has allocated sufficient resources, including personnel, technology, and training, to meet its



AML&TF obligations;

- the findings and recommendations of internal and external AML&TF audits have been reviewed and appropriately addressed;
- the Company's Business Risk Assessment has been reviewed and updated as necessary; and
- the MLRO has reported on the Company's AML&TF compliance status, including any material deficiencies or regulatory developments.

Such certification shall be documented in writing, retained in accordance with the Company's record-keeping obligations, and made available to the CGA upon request.

AML&TF DESIGNATED OFFICER

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

General duties of the AML&TF Compliance Officer include monitoring of the Company's compliance with the AML&TF obligations, assessment of the business risks both internal and external, oversight of the AML&TF related communication and training for employees, and reporting of the findings and critical issues of the AML&TF systems and procedures to the managers and executives of the Company. The AML&TF Compliance Monitoring Officer/MLRO ensures that the Company keeps and maintains all required AML&TF records and that Suspicious Activity Reports are filed with FIU Curacao when required and appropriate. The Compliance Officer's obligations with respect to goAML portal registration, access management, and reporting procedures are set out in the goAML Portal Reporting Procedures and Timelines chapter of this Policy. The AML&TF Compliance Officer is vested with full responsibility and authority to enforce the Company's AML&TF Policy and working procedures. Responsibilities of AML&TF Compliance Officer includes:

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

DEPUTY MLRO AND SUCCESSION

The Company may designate a Deputy Money Laundering Reporting Officer (Deputy MLRO) who would assume the responsibilities of the MLRO in the event of the MLRO's absence, incapacity, or vacancy. Where a Deputy MLRO is appointed, such person should:

- possess sufficient seniority, knowledge, and authority to act in the MLRO's stead;
- maintain current knowledge of the Company's AML&TF policies, procedures, and systems;
- maintain goAML portal registration and access credentials in accordance with the goAML Portal Reporting Procedures and Timelines chapter of this Policy; and receive the same AML&TF training as the MLRO.



In the event of a permanent vacancy in the MLRO position and where a Deputy MLRO has been designated, such Deputy MLRO could serve in an acting capacity until a replacement is appointed. Alternatively, the Company may make alternative arrangements to ensure continuity of AML&TF compliance functions during any temporary absence or vacancy of the MLRO. The Board of Directors should be notified promptly of any change in the MLRO or Deputy MLRO arrangements.

A handwritten signature in blue ink, consisting of a stylized 'W' or similar character, located in the bottom right corner of the page.

3. CUSTOMER DUE DILIGENCE

INTRODUCTION

The Company is prohibited from keeping anonymous accounts or accounts in obviously fictitious names. It must identify the player and ask for the player's name and other relevant information to determine the purpose and nature of the business relationship. Without sufficient knowledge, the Company may not establish or maintain a business relationship or carry out occasional transactions. A sound CDD program is the best way to prevent AML, TF & FP.

The customer's risk profile is essential to apply a certain level of CDD commensurate to the identified ML/TF risk. The purpose of collecting information is to assess the risk that may be associated with the player and to build a customer profile to assess how the player is going to act within the framework of the business relationship. Such an assessment is necessary in order to detect deviations from the expected behaviour, which are reported to the FIU (more on chapter 4).

The obligation to undertake CDD measures when:

- When players engage in financial transactions equal to or above EUR 2,000;
- carrying out occasional transactions above the monetary equivalent of EUR 2,000;
- there is a suspicion of money laundering or terrorist financing; or
- there are doubts about the veracity or adequacy of previously obtained customer identification data.

Note: a transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount in excess of the monetary equivalent of EUR 2,000.

For transaction above the monetary equivalent of EUR 2,000, CDD measures are applied 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.

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.

THE CDD MEASURES

The CDD measures are as follows:

- Identifying the player and verifying that customer's identity using reliable, independent source documents, data or information;
- Identifying the BO, and taking reasonable measures to verify the identity of the BO, such that the Company is satisfied that it knows who the BO is. For legal persons and legal arrangements this should include understanding the ownership and control structure of the customer;
- Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;
- Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Company's knowledge of the player, its business and risk profile, including, where necessary, the SoF.

The Company, its directors, officers and employees are prohibited to disclose the fact that an UTR is being reported to the FIU. A risk exists that players could be unintentionally tipped off when the Company is seeking to perform its CDD obligations in these circumstances. Therefore, if the suspicion arises those transactions

relate to ML or TF, the risk of tipping-off should be accounted when performing the CDD process. If there are reasonably believes that performing the CDD process will tip-off the player, there is the option of not to pursue the process and file an UTR to the FIU.

IDENTIFICATION AND VERIFICATION OF THE PLAYER

Identification and verification of the player refers to the collection of personal details of the player to establish the identity of the player. Verification on the other hand consists in confirming the personal details collected for identification purposes using reliable, independent source documents, data or information. The personal information required and extent of verification to be carried out, will vary depending on risk.

When identifying the player, at a minimum the following information is collected:

- full name;
- permanent residential address;
- date of birth;
- place of birth;
- nationality; and
- identity number.

However, in low-risk scenarios identification can be limited to full name, permanent residential address and date of birth. On the other hand, in high-risk situations, additional personal can be collected as necessary to mitigate the higher risk of ML/FT.

As soon as identification data of player is captured, the screening of those shall be performed against PEP status, sanctions, criminal status, adverse media or other factors that might impact the risk level associated with player. The screening is to be performed in cooperation with reputable and reliable provider who is capable to maintain complete, comprehensive and up to date database and ensure that the screening outcome is reliable for risk profile assessment.

CRA is done to have sufficient information available to detect unusual activity in the course of the business relationship. A provisional risk rating is assigned based on the initially collected information and is revised once questions are answered or additional information received. On the basis of the CRA, the proper level of CDD can be applied as stipulated by the CAP.

Verification of an identity refers to actions taken to verify that a person exists and is who he claims to be. This is done by checking reliable, independent (of the person whose identity is being verified) sources.

Verification of identity is carried out by making reference to an unexpired government-issued document containing photographic evidence of the customer's identity (e.g., passport, identity card). Where such a document does not allow verification of the player's residential address, other documents are requested, like a bank statement, utility bill¹, letter from a public authority or rental agreement, which should not be more than six months old to verify the residential address. The client can be contacted by letter, e-mail or telephone to verify the information supplied. It can also send a verification code to the e-mail address to verify that the address is current and genuine. Verification can also be done by checking social media, telephone directories, companies' registries or media and news sources. Biometric checks can also be used to confirm that the individual providing the document is the one described therein. The Company also cross references the information with geo-location information, IP address data, funding method data etc.

Verification is carried out to determine that the player is who he declared himself to be. What is important is that documents are clear, legible and of good quality. Verification of evidence of identity implies a check whether the document presented is legitimate and that it has not been stolen from the true owner. Extra care is taken

¹ For phone bills, only fixed line telephone bills are accepted as proof of address.

with regard to verifying the authenticity of foreign documentation, particularly where the type of document is unfamiliar.



When there is not sufficient comfort that the Company knows its player, it is expected that additional measures are to be taken. Some of these measures include requesting additional identification documents, asking the player to provide a photo of himself holding the ID, requiring a first payment through an account held in a reputable jurisdiction, using systems which generate codes for transmission to customers through a verified mobile phone and requiring it to be returned.

TIMING OF CDD MEASURES

Verification of identity is conducted when engaging in financial transactions equal to or in excess of EUR 2,000. However, a minimum level of CDD measures is required prior to reaching the threshold. Thus, simultaneously with the opening of an account, the customer is identified by collecting the minimum personal details. The threshold is calculated on a daily considering all deposits and withdrawals made by the player since the establishment of the business relationship, including any peer-to-peer transfers.

In carrying out the CDD measures, customers are allowed to continue using their gaming account while the Company obtains any necessary information from the customer concerned. However, if the EUR 2,000 threshold is reached because of a deposit of the player, he cannot further deposit funds into the account or withdraw funds from the account. He still will be able to play, using the funds already in his account. However, if the EUR 2,000 threshold is reached because the customer wants to withdraw his money, a complete freezing of the account will occur and the customer would not be able to play.

Besides that, if the requested information and documentation is not received within 30 days from the moment the EUR 2,000 threshold was reached, the Company will terminate the relationship with the player and its Compliance Officer will report the transaction to the FIU, only if a presumption of ML & TF exists. *If presumption of money laundering or terrorist financing exists, internal procedures should indicate whether the funds are blocked or not. Consideration should be given to the fact that by blocking the account, the customer may be tipped off.*

If no presumption of ML & TF, the funds will be transferred to the same bank account or wallet it was deposited from.

UNDERAGE GAMING PREVENTION AND AGE VERIFICATION

In accordance with the Company's dedicated Responsible Gaming Policy, the Company is committed to preventing underage individuals from accessing its gaming services. Pursuant to applicable laws and CGA licensing requirements, only individuals who have attained the age of eighteen (18) years or the minimum legal gambling age in their jurisdiction of residence (whichever is higher) are permitted to register, deposit, or engage in gaming activity on the Company's platform.

Timing of Age Verification

Age verification is performed at multiple stages of the customer lifecycle to prevent underage access:

- Pre-registration: At the point of account creation, all prospective players must confirm they are at least eighteen (18) years of age to register an account. The system automatically rejects registration attempts where the declared date of birth indicates the individual is below the minimum age threshold.
- Pre-deposit / pre-play: Before a player is permitted to make their first deposit, the player is required to provide the full identification data required for CDD purposes (i.e., full name, permanent residential address, date of birth, place of birth, nationality, and identity number). At this stage, the information is checked for sufficiency and validity, and screening is performed to identify high-risk factors. Screening also validates the date of birth through open sources whereby such information is available.
- Threshold-triggered verification: Players are required to complete full identity verification before the EUR 2,000 CDD threshold is reached. If the data provided at the identification stage is not confirmed upon verification, the account is immediately blocked and escalated to the Compliance Officer for review.

to determine whether the event demonstrates any AML/TF-related risks. If, upon verification, it is



discovered that the player is below the legal age, the dedicated procedure set forth in the Company's Responsible Gaming Policy shall be followed.

If underage gaming is detected at any of the stages above, the following mitigation procedures are followed (where applicable):

- If an account was created, it shall be immediately terminated.
- All winnings, if any, shall be voided and forfeited.
- Deposits, if any, shall be returned to the original payment source.
- The incident is documented, reported to the Compliance Officer (and Responsible Gaming Officer, if applicable), and escalated to senior management.
- Where required by applicable law or CGA directive, the matter shall be reported to the regulator.

Methods of Age Verification

The Company may employ the following methods to verify a player's age:

- Document-based verification: Review of a government-issued identity document containing the player's photograph and date of birth (e.g., passport, national ID card, driver's license). Documents must be valid (unexpired) and legible.
- Electronic verification: Where available, automated verification against authoritative databases (e.g., government registries, credit reference agencies) that confirm the player's identity and age.
- Third-party verification services: Use of reputable KYC/age verification vendors capable of cross-referencing player-provided data against reliable independent sources.

Where automated verification is inconclusive or returns a negative result, the account is immediately suspended and manual review by the Anti-Fraud Department is required before the account may be reactivated.

ENHANCED DUE DILLIGENCE

Whenever an occasional transaction presents a high risk of ML/TF, the EDD measures must be applied. 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.

EDD measures should be consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual. EDD has to be conducted where the risks of money laundering or terrorist financing are higher. This concerns for example:

- Residents of higher risk geographic areas;
- Sanctions, PEP, criminal status or adverse media was detected upon screening ;
- Products or transactions that might favour anonymity;
- New products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.

The applied measures must be consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Examples of EDD measures include:

- Obtaining additional information on the customer, like occupation, previous address and information available through public databases, internet, etc.;
- Obtaining additional information on the intended nature of the business relationship;
- Obtaining a clean criminal record;
- Obtaining information on the SoF or SoW of the player. Examples of SoF include personal savings, employment, pension releases, share sales and dividends, property sales, gambling winnings, inheritances and gifts and compensation from legal rulings;
- Obtaining information on the reasons for intended or performed transactions;

- Obtaining the approval of senior management to commence or continue the business relationship;
- Conducting enhanced monitoring of the business relationship;
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

The Operator applies a risk-based approach to the collection of SOF and SOW information. SOF and/or SOW verification is required where a customer is assessed as presenting a higher risk of money laundering or terrorist financing, including but not limited to situations where transaction patterns, customer behavior, or customer profile are inconsistent with information previously obtained, or where Enhanced Due Diligence is required under applicable law.

In situations presenting a higher risk of ML/TF, SoF information has to be requested from time to time even though there may not be any change in pattern or activity conducted by the customer.

SIMPLIFIED DUE DILLIGENCE

Where the risks of money laundering or terrorist financing are lower, the Company can conduct SDD, which should take into account the nature of the lower risk. Examples of possible measures:

- Not collecting specific information. If the risk assessment undertaken indicates a low risk of money laundering or terrorist financing then it is only necessary for the Company to obtain the player's identity. In this case the Company may limit identification to the first three personal.
- Verifying the identity of the customer and the BO after the establishment of the business relationship;
- The extent of verification may also vary depending on the risk posed by the particular business relationship. In a low-risk situation, the Company can also use alternative reputable information sources, even where these do not contain photographic evidence of the player's identity (e.g., birth certificates, bank statements etc.);
- The extent of personal details verified can also vary. In low-risk situations, the Company has to verify the basic identification details, while the verification of any other personal details is upon the Company, as long as it has sufficient comfort that it knows who its customer is;
- Reducing the frequency of customer identification updates;
- Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.

SDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

POLITICALLY AND SANCTIONS EXPOSED PERSONS

All players are screened to establish their PEP status and against applicable sanctions lists. Sanctions screening is performed at account registration (prior to account activation), upon any material change to customer identification data, when CDD refresh or EDD is triggered, and on an ongoing basis against updated sanctions designations. The Company utilises automated screening tools provided by reputable third-party vendors capable of real-time or near-real-time screening against current sanctions lists. The frequency and depth of rescreening may be calibrated on a risk-sensitive basis, with higher-risk customers subject to more frequent review. With respect to transactions or business relationships with PEPs, in addition to the KYC measures:

- the Company has in place appropriate risk management systems to determine whether the customer is a PEP;
- apply the following measures in cases of setting relationships with PEPs:
- obtain senior management approval for establishing or continuing business relationships with such

persons; - take adequate measures to establish the SoW and SoF that are involved in business relationships or transactions with such persons;

- conduct enhanced, ongoing monitoring of those business relationships.

Before establishing of 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). In addition, the Company will screen against Curaçao's local list of designated persons and organizations, once and if this list will be published by the authority.

- Sanctions screening is conducted with the assistance of a reputable third-party screening solution provider. The Company ensures that the selected provider maintains comprehensive, up-to-date sanctions databases, provides timely updates following new designations, and offers reliable matching algorithms with configurable sensitivity. The Compliance Officer shall periodically review the provider's performance, data coverage, and update frequency to ensure continued adequacy. The screening solution checks published lists of known or suspected terrorists or other sanctioned persons or companies, including: UN Sanctions List;
 - EU Sanctions List;
 - Persons List Specially Designated Nationals and Blocked Persons List (SDN) Human Readable Lists | Office of Foreign Assets Control;
 - Sanctions that may be announced by Curacao Gaming Authority or other governmental bodies in Curacao;
 - Other related lists
- Where a potential sanctions match is identified, the Compliance Officer or designated staff shall promptly assess whether the match is a true positive or a false positive. False positives shall be documented, including the basis for the determination, and the customer record updated accordingly. Where the assessment is inconclusive, the matter shall be escalated to the MLRO within twenty-four (24) hours for determination. In case of a confirmed true positive match against a sanctions list, the following actions shall be taken without delay: An account of sanctioned person or organization shall be immediately frozen without delay and without prior notice as to suspend the possibility to withdraw the funds from an account,
- A report must be filed with the FIU,
- Any further actions shall be verified through appropriate legislation, in particular Process for the freezing of resources (Proces bevroezing van middelen) for the implementation of sanctions imposed by international organizations published in the National Gazette on September 16, 2016 and Procedures for releasing of the resources when implementing sanctions of international organizations (Procedure for the releasing of resources) issued by a Central Bank of Curacao as on August 26, 2016.

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 Company, in which the client is involved. The business relationship between the client and the Company is likely to be contracted when the client registers 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 CDD 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&TF. The Company only accepts individuals whose personal data, disposition and further behaviour patterns specifically indicate intention to lawfully and fairly use 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.

The Company collects, if necessary, information and documentation to establish a customer's SoW as well as the expected level of activity. SoW consists of determining the activities which generate the customer's net worth

and whether this justifies the projected and actual level of account activity. As to the extent of the information that the Company collects, it is essential that this reflects the level of ML/FT risk identified through the CRA.

Where the risk is not high, a declaration from the customer with some details (e.g., nature of employment/business, usual annual salary etc.) is sufficient. Social media can also be used as a source of information.

However, where the risk of ML/FT is higher or there are doubts as to the veracity of the information collected, the information obtained would need to be substantiated by independent and reliable information and documentation. In developing a customer risk profile, the Company may also consider using statistical data to develop behavioural models against which to eventually gauge a customer's activity rather than collect SoW information. Where the Company opts to adopt this approach, it can use data collected from the Central Statistics Department such as average national income, average disposable income etc. These indicators should allow the Company to determine the average wagering power of players from a given jurisdiction.

The Company can also use data collected over time to create the profile of an average player. The Company is using this only if the customer-base is wide enough to allow the creation of an average profile. For a limited customer-base, the data is obtained from other players with a similar business model. The use of statistical data is incompatible with high-risk situations as the transactional pattern will fall outside the average behavioural model. In such circumstances, the Company will use SoW information.

CONFIRMATION OF UBO OF THE FUNDS

The ultimate purpose of procedures for monitoring AML-TF 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. Establishment of the identity of the UBO of the funds is thus the key purpose of the AML-TF controls at the Company. Operating Control Matrix sets up a number of barriers to prevent the suspect individuals from access to 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.

The Company is required to identify and verify the identity of the BO by making sure that customers are registering an account to play and transact on their behalf. This is mentioned on the website's terms and conditions that a registering player must explicitly accept, together with a declaration on the registration page. The Company will not merely rely on said declaration and will monitor for possible instances where the player is actually playing on behalf of third parties.

IDENTIFICATION AND VERIFICATION SYSTEMS

The Company's identification and verification systems are predominantly computer-based and include various data-bases and cross-checking software. The products of third-party providers, credit-card databases and other sources are utilized in order to control the customer identification and fund-origination risks. The Company's accounting system traces the account movements by individual IP address of the players. List of IP addresses is stored and can be viewed for each game account; all IP addresses are also stored in the logs of the program (including archived). The system has a viewing facility for analysis of a list of players and the



number of movements at the specified IP address. Recording of IP addresses allows to track down fraudsters whose activities are connected with gaining access to other customers' player account or gaining possession of their funds.

Operating Control Matrix (Appendix B) describes in more details the key procedures applied at the Company to safeguard the integrity of the customer background checks and to arrange for proper customer identification. In

some cases, such as country of residency, age and single-account tests, the controls are automatic (no human involvement). In other cases, e.g., funds ownership and changes in customer information, the Company's officers are personally involved and are required to make professional judgments. The combination of automatic and human-driven controls is a key operating feature of the KYC controls in the Company.

Embargo requirements for ML&TF controls specifically concern two country groups:

- the US List of State Sponsors of Terrorism². Currently the list includes Cuba, Iran, Sudan and Syria.
- the countries and territories with prohibitive and internationally promulgated territorial gambling regulations. Currently the list includes the USA and its dependencies, Israel, France, UK and outlying territories, Italy, Spain, Denmark, the Netherlands and Estonia.

Requests from potential customers from the aforementioned countries and territories (residential addresses and IP addresses) are denied. Furthermore, the names of such customers are retained on record, blacklisted and are routinely screened in any future customer requests. The mechanisms, practices and measures of CDD is outlined in a separate document describing the KYC procedures, (please refer to the dedicated KYC Policy, which forms an integral and enforceable part of the AML framework).

² <http://www.state.gov/j/ct/rls/crt/2012/209985.htm>



4. MONITORING

ONGOING MONITORING OF IDENTITY

In conducting ongoing due diligence on the business relationship, the Company holds accurate and up to date identification data of its customers. Since identity may change due to circumstances, the information must be detected and re-evidenced. The Company requests evidence of identity periodically to detect any changes, refresh the data on key events (i.e., change of payment instrument) or tracks expiry dates on evidence of identity and refreshing it as it expires. The Company determines on a risk-sensitive basis whether changes are substantial as to require re-assessment of customer risk of the business relationship.

Where ongoing monitoring identifies indicators listed under the SOF/SOW escalation criteria, the case must be escalated for Enhanced Due Diligence.

TRANSACTIONS MONITORING

Monitoring of monetary transactions is a constituent part of the monitoring of the account activities and is described in detail in the Operating Control Matrix (please refer to Company's Operating Control Matrix, which forms an integral and enforceable part of the AML framework). Main purpose of transaction monitoring with respect to ML&TF threats is to identify and to prevent the suspicious transactions from taking place at the business facilities. Various safeguards and awareness triggers are employed in transactions monitoring e.g., absolute monetary limits; single-player-single-account, single-session and single-currency rules; obscure event bets (described in Operating Control Matrix).

Assignment of status (and colour grades for visual recognition) to the players according to the types of games and gaming behaviour:

- No status: players who have not triggered suspicions with any departments of the Company. Usually applied to new customers, which have not finished verification procedure yet. Limits could be set according to a governmental database of self-limited individuals from specific countries.
- Monitored: players who have gone through full verification (provided the passport data, etc.). The gaming activity of customers in this group was analysed by the Anti-Fraud Department employees, no suspicious actions were detected at the moment.
- Arbitrage: players with the history of placing sure bets
- Scammers
- Foreigners: players whose country of residence is outside of the Company's core region of operations.
- Suspicious: gaming accounts placed under close monitoring by Payment and Factoring & Monitoring Departments
- Potential VIP players
- Existing VIP players. A group of players, which constantly place bets with amounts over 100 EUR or equivalent in other currencies. Their gaming activity is not limited and they have higher priority in processing transactions.

if the player has a "good" category, it doesn't mean that he drops out of control. Payment and Factoring & Monitoring Departments carry out continuous monitoring of all players and transactions. Employees of the Company seeks to identify the following indications of the potential ML&TF 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.

Changes in registered players' information are monitored by Anti-Fraud Department; consistency and significance of changes are analysed daily; game session patterns are matched against the historic average profile (its IP addresses, his types of games and style of bets, Payment Systems that he uses etc.) for a given game to ensure that, in each particular moment, they resemble the historic gambling trends for the customer. Significant deviations during game sessions are documented, analysed and reported.

If any unusual behaviour is identified by the employees of the Department, they make short time block of the activity on the customer's account in order to check whether the customer performs actions by himself and make investigation on player's activity. As for the internal controls, Anti-fraud department on a daily basis generate Manual adjustment report and review any manual changes that were done to the client's account.

Transaction monitoring is executed to prevent involvement of the Company with ML/TF and to safeguard the reputation of the Company. While in conducting ongoing scrutiny of transactions there are transactions that are not consistent with what it is expected from the customer, the Company establishes the source of the funds used for that transaction. The Company must obtain sufficient information and documentation with regard to the transaction to determine the reason for this deviation. If needed, the risk profile of the customer may have to be revised. After receiving this information, the Company decides whether the transaction is an unusual and needs to be reported to the FIU.

The level of on-going monitoring depends on the risk profile of the customer, but even in low-risk situations there is a degree of oversight to ensure that the business relationship is still considered as a low risk one.

The Company conducts ongoing due diligence on the business relationship and scrutinize the transactions undertaken throughout the course of that relationship to ensure that they are consistent with the Company's knowledge of the customer, the customer's business and risk profile.

PLAYER FUNDS AND PAYMENT FLOW OVERSIGHT

The Company maintains robust controls over player funds to prevent misuse of gaming accounts for money laundering, terrorist financing, or other illicit purposes. These controls address the segregation, monitoring, and reconciliation of player funds across all payment channels.

Player funds are held separately from the Company's operational funds at all times. The Company maintains dedicated accounts for player balances, which are:

- Clearly identified and ring-fenced from corporate operating accounts;
- Subject to daily reconciliation to ensure that aggregate player balances match funds held in segregated accounts;
- Monitored for unusual fluctuations that may indicate fraudulent activity, system errors, or potential ML/TF concerns;
- Protected from use for any purpose other than player withdrawals, gaming activity, or regulatory-mandated actions (e.g., freezing pursuant to sanctions obligations).

The Finance Department is responsible for the constant monitoring of segregated account balances on a daily basis and investigates any material discrepancies immediately.

Reconciliation Between Player Wallets, Payment Agents, and Operational Accounts

The Company performs regular reconciliation across all payment touchpoints to maintain full visibility over the flow of player funds. Reconciliation procedures include:

- Daily reconciliation of individual player wallet balances against the Company's internal ledger;



- Daily reconciliation of funds received from and disbursed to third-party payment agents, payment processors, and e-wallet providers against internal transaction records;
- Weekly reconciliation of aggregate player liabilities against funds held in segregated player accounts and amounts in transit with payment agents;
- Monthly reconciliation reports reviewed and signed off by the Finance department officer, with any unresolved discrepancies escalated to senior management.

All reconciliation records are retained for a minimum of five (5) years in accordance with the Company's record-keeping obligations. Discrepancies identified during reconciliation are logged, investigated, and, where they give rise to suspicion of ML/TF, reported to the Compliance Officer for assessment and potential filing of an Unusual Transaction Report (UTR) with the FIU.

Controls to Detect Misuse of Player Accounts for Non-Gaming Purposes

The Company actively monitors for indicators that a player account is being used as a conduit for funds transfer rather than for legitimate gaming activity. The following controls are in place:

- Deposit-to-play ratio monitoring: Accounts where deposits significantly exceed wagering activity are flagged for review. Players who deposit funds and subsequently request withdrawals with minimal or no gaming activity are subject to enhanced scrutiny and potential account suspension pending investigation.
- Withdrawal pattern analysis: Requests to withdraw funds to accounts or wallets different from the original funding source, or to multiple destinations, trigger enhanced verification and MLRO review.
- Velocity controls: Limits are placed on the frequency and volume of deposits and withdrawals within defined time periods. Transactions exceeding these thresholds require manual approval and may trigger CDD refresh or EDD measures.
- Third-party payment detection: The Company prohibits the use of third-party payment instruments (i.e., credit cards, bank accounts, or e-wallets not registered in the player's name). Attempted use of third-party instruments results in transaction rejection and account review.
- Peer-to-peer transfer monitoring: Where peer-to-peer transfers between player accounts are permitted, such transfers are subject to transaction limits, are logged, and are monitored for patterns indicative of chip dumping, collusion, or value transfer unrelated to gaming.
- Dormant account reactivation: Accounts that have been inactive for extended periods and are subsequently reactivated with significant deposit or withdrawal activity are flagged for MLRO review prior to processing transactions.

Where any of the above controls identify activity inconsistent with legitimate gaming purposes, the Company may:

- Suspend the player's ability to deposit, withdraw, or transact pending investigation;
- Request additional CDD/EDD documentation, including SOF and SOW;
- Terminate the business relationship if satisfactory explanations or documentation are not provided within thirty (30) days;
- File a UTR with the FIU where there is cause to presume the activity is related to ML/TF.

All actions taken pursuant to these controls are documented in the player's account record and retained in accordance with the Company's record-keeping policy.

MONITORING OF THE ACCOUNT ACTIVITIES

This component is central to the Company's AML&TF 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 Compliance Officer. This enforcement is conducted daily and

supported by various thresholds set up to flag the potential problems. Operating Control Matrix describes the controlling processes in detail (Appendix A).

Overall, monitoring of account activities consists of:

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

date

Critical controlling measures with respect to ML&TF

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 ML&TF threats.

MONITORING OF HIGH-RISK CLIENTS

Suspicious players and scammers have the highest risk range of all players. There are several categories of such kind of players and the measures for their detection:

"Review"- this group includes players whose gaming activity is unusual. These accounts are limited by 5-10 EUR or its equivalent in other currencies bet amount or even blocked-in order to prevent fraud. For the "Review" the account will be unblocked only when Anti-fraud or Payment or other departments who detected the trigger would confirm that the customer has passed all the required procedure.

"Betting arbitrage" - is an example of arbitrage arising on betting markets due to either bookmakers' differing opinions on event outcomes or errors. When conditions allow, by placing one bet per each outcome with different betting companies, the bettor can make a profit regardless of the outcome. Mathematically, arbitrage occurs when there are a set of odds, which represent all mutually exclusive outcomes that cover all state space possibilities (i.e., all outcomes) of an event, whose implied probabilities add up to less than 1.

"Bonus hunting (also known as bonus bagging)" is a type of advantage gambling where turning a profit from sportsbook bonus situations is mathematically possible.

"Late Betting"- players that place bets on the matches, which are finished already, but not included to the system, result. Also are detected by gaming patterns, by analysing time of bets and real time of events happened. Depending on player's average bet amount the 1-20 EUR or its equivalent in other currencies limit in equivalent could be implemented.

"SFM (Suspicion Fixed Matches)" when player that often bets on events or leagues that are considered highly corrupt and with a high risk of negotiated matches.

"PEP" - Means a natural person who is or who has been entrusted with a prominent public function in the Republic or another country, a close family member of that persons as well as a person known to be a closely associated with such person. Transactions of PEPs continuously monitored, especially to ensure that the threshold has not been exceeded and that the amounts played correlate with the income profile of the PEP

received during the EDD procedure.

Adverse media publications, publicly available registers etc.

Payment systems database – reconciliation to the records of the customers. Anti-fraud and Payment departments often refer to the data provided by the Payment systems in order to reconcile information provided by the customer in his registration form with the information recorded in Payment System database. In the black-lists employees who perform controls can find list of persons, which were blocked according to the certain reasons.

And finally, Payment Systems send automatic or manual notifications, if they detect any suspicious transaction. All these notifications are checked and assessed by the Responsible employees.

After suspending the account, a notification appears on the customer's page and the Support Team requires information and/or documents in order to check the suspicious action. Also, additional information may be requested from affiliated who are processing deposits and withdrawals from the gaming accounts, in order to obtain information about the origin of the funds.

The customer still has the possibility to enter his personal account during the investigation process but the funds will remain frozen and all transactions blocked until the investigation is completed.

All the investigation steps recorded in the system. If it completed successfully, the responsible employee will unblock the account and the customer can manage his funds again. If there were no response to the notification or the customer provides not enough data to complete the investigation - the account will remain blocked until the requested documents received.

"Problematic Gamblers"- we characterize the players whose behaviour is excessive and/or aggressive and in general problematic like harassing the support team staff or whose actions could be classified as compulsive gambling. There are 3 ways of identifying players who display problematic gambling behaviour and the respective following steps for each type of it:

I. The customer informs the Support team by himself about his gambling problem through e-mail or chat or telephone. The request can include limits of bets that should be set to the customer OR temporary blocking of the account. After the Anti-fraud department execute the request, the customer notified about the changes done to his account via e-mail.

II. Mathematical review. One of the triggers that monitored by the department is the problematic gambling trigger. It includes the following algorithms: if a gamer has losses, which were increased 10 times during a period of more than 3 months (90 days) the gamer is identified as a problematic one OR if a gamer doubled his losses each month during the last 12 months he is identified as a problematic gambling customer. According to these analyses, the Support department initiates the communication with the customer, where they describe the situation, give links to gambling addiction help websites and propose measures to the customer like self-limitation with the most comfortable and suitable conditions.

III. Support team review. While communicating with the customers, the Support department identifies the problem gambling customers if their chats or calls are harassing to the Support team or other customers or compulsive gambling. One of the main triggers of the compulsive gambling is the constant request of the credit to be issued by the website. (no one can issue any credits to customers).

CONSEQUENCES AND ESCALATION FOLLOWING SOF / SOW ASSESSMENT

Where the assessment of SoF and/or SoW information identifies an increased risk of money laundering or terrorist financing, the Operator shall apply enhanced ongoing monitoring measures proportionate to the identified risk, as:

- Increased frequency of transaction reviews;
- Lower internal alert thresholds;
- Manual review of withdrawals prior to execution.

Where SoF and/or SoW information cannot be satisfactorily obtained, is inconsistent, or raises unresolved



concerns, the Operator may apply appropriate risk-mitigation measures, which may include temporary account restrictions or suspension, in accordance with a risk-based approach.

Such measures are applied solely to prevent misuse of the gaming platform for money laundering or terrorist financing and shall not be used to delay or avoid legitimate withdrawals.

Where the outcome of a SoF and/or SoW assessment gives rise to reasonable grounds to suspect money laundering or terrorist financing, the related transaction(s) shall be reported without delay to the FIU Curaçao, in accordance with the National Ordinance on the Reporting of Unusual Transactions.

RECONCILIATION OF SOF / SOW WITH EXPECTED PLAYER ACTIVITY

The Operator reconciles SoF and/or SoW information against the customer's expected player activity and assigned risk profile to assess whether the customer's actual transactions and gambling behavior are reasonable, plausible, and consistent with the information obtained.

Where the reconciliation confirms consistency between SoF and/or SoW, and observed activity, the business relationship may continue subject to standard or enhanced monitoring, as applicable. Where inconsistencies, unexplained discrepancies, or implausible activity are identified, the Operator shall reassess the customer's risk profile and apply appropriate enhanced due diligence or risk-mitigation measures. Material discrepancies identified during reconciliation are escalated and may result in enhanced monitoring, account restrictions, or reporting of unusual transactions, where applicable.

REPORTING 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. Concurrent analysis is conducted on each such activity or transaction in accordance with the Operating Control Matrix. The officers responsible for respective areas of transaction monitoring report the suspicious activities to the Compliance Officer 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 Compliance Office even when their immediate superior is in disagreement with them. The Compliance Office must determine if the information available can be considered as sufficient for Unusual Transaction Report (UTR) to be made to the FIU. All unusual transactions are subject to be reported to the FIU in accordance with the procedures, timelines, and documentation requirements set out in the goAML Portal Reporting Procedures and Timelines chapter of this Policy. In accordance with Article 10 of NORUT the following transactions are deemed as unusual and subject to be reported:

- a. Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;
- b. Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- c. Transactions in the amount of Naf. 5,000 or more, regardless whether the transaction is made in cash, by check or other form of payment, or through electronic or other non- physical means.

This includes but is not limited to:

1. A cashless transaction in the amount of NAf. 5,000 or more.
2. A cashless transaction is a transfer from a bank account of the casino to a local or international bank account, at the request of the client.
3. Accepting or releasing a deposit in the amount of NAf. 5,000 or more at the request of the client;
4. Sale to a customer of chips in the amount of NAf. 5,000 or more. "Chips" include but is not limited to tokens and credits.
5. A cash out in the amount of NAf. 5,000 or more.

With regards to the above, it shall be noted that a transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount of the monetary equivalent of NAf. 5,000 or more and is considered per gaming (calendar) day.

- d. Presumed money laundering transactions or terrorist financing: transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

If internally reported transactions are not reported to the FIU by the Company, the reasons therefore are subject to be adequately documented and signed off by the Compliance Officer and stored in companies records in accordance with the requirements.

goAML PORTAL REPORTING PROCEDURES AND TIMELINES

The Company is required to submit all Unusual Transaction Reports (UTRs) and other regulatory reports to the Financial Intelligence Unit Curaçao (FIU) exclusively via the goAML reporting portal, unless an alternative submission method is expressly authorised by the FIU. The following procedures and timelines govern the Company's use of the goAML portal and apply to all compliance personnel involved in the detection, escalation, and reporting of suspicious or unusual activity.

REGISTRATION AND ACCESS MANAGEMENT

The Compliance Officer shall ensure that the Company maintains an active and valid registration on the goAML portal at all times. The following requirements apply to access management:

The MLRO shall be the primary registered user on the goAML portal and shall hold active access credentials at all times. Where a Deputy MLRO has been designated, such person shall also be registered on the portal with independent access credentials, enabling uninterrupted reporting capability in the absence or incapacity of the MLRO.

The Compliance Officer may designate additional compliance staff as authorised goAML portal users where operationally necessary. All designated users must be formally approved by the MLRO, and a current list of authorised users shall be maintained and reviewed at least annually.

All access credentials for the goAML portal must be treated as strictly confidential. Credentials must not be shared between users. Each authorised user is responsible for the security of their own login credentials. Access must be revoked immediately upon the departure or change of role of any authorised user.

In the event that the goAML portal is temporarily unavailable, or access credentials are compromised or lost, the MLRO shall initiate the technical contingency procedure described below. The Company shall document all access issues and the steps taken to restore portal access without delay.

REPORTING TIMELINES

The Company applies the following mandatory timelines for the submission of reports via the goAML portal:

Unusual Transaction Reports (UTRs): All UTRs shall be submitted without delay and, in any event, no later than three (3) business days from the date on which the MLRO makes the determination that a report is



required. For the purposes of this Policy, “without delay” means as soon as reasonably practicable following the MLRO’s determination that a UTR is warranted, and in no case shall administrative or operational convenience justify deferral beyond the three (3) business day maximum.

Sanctions-related reports: Where a transaction or account is identified as involving a designated person or entity subject to targeted financial sanctions, a report shall be submitted to the FIU immediately and no later than twenty-four (24) hours after detection. Simultaneous account freezing obligations apply in accordance with the Sanctions Policy.

Threshold-based transaction reports: Transactions meeting or exceeding the NAF. 5,000 reporting threshold as set out under Article 10 of NORUT shall be submitted via the goAML portal within five (5) business days of the relevant transaction or the last transaction in a series that cumulatively meets the threshold.

Presumed money laundering or terrorist financing transactions: Reports relating to transactions where there are reasonable grounds to presume a link to ML or TF shall be submitted as soon as possible and no later than twenty-four (24) hours following the MLRO’s determination.

REPORTING PROCEDURES

The following step-by-step procedure governs the preparation and submission of reports through the goAML portal:

Step 1 - Internal detection and escalation: Any employee, officer, or automated monitoring system that identifies a potentially suspicious, unusual, or threshold-triggering transaction or activity shall escalate the matter to the Compliance Officer or MLRO immediately, in accordance with the internal reporting procedures set out in this Policy. Escalation shall be made in writing and shall include a description of the activity, the relevant account or transaction details, and any supporting documentation or risk indicators identified.

Step 2 - MLRO review and determination: Upon receipt of an internal escalation, the MLRO shall review the matter and make a determination as to whether a report to the FIU is warranted. Such determination shall be made within forty-eight (48) hours of receipt of the escalation, unless exceptional circumstances require a longer review period, in which case the reasons for delay shall be documented. The MLRO’s determination, whether to file or not to file, shall be recorded in writing and retained as part of the Company’s internal SAR/UTR register.

Step 3 - Preparation of the report: Where the MLRO determines that a report is required, the Compliance Officer or designated compliance staff shall prepare the report using the goAML portal’s prescribed format. The report shall include all mandatory fields as required by the FIU, together with all relevant supporting documentation, including but not limited to account information, transaction records, CDD documentation, and a clear narrative description of the suspicious or unusual activity and the grounds for reporting.

Step 4 - Quality review: Prior to submission, the completed report shall be reviewed by the MLRO for accuracy, completeness, and consistency with the available evidence. No report shall be submitted without the MLRO’s written approval.

Step 5 - Submission via goAML portal: The approved report shall be submitted through the goAML portal by an authorised user. The submitting user shall verify that the submission has been successfully received by the portal and that a goAML reference number has been generated.

Step 6 - Confirmation and reference number retention: Upon successful submission, the goAML reference number and submission confirmation shall be retained and cross-referenced to the relevant entry in the Company’s internal SAR/UTR register. Submission confirmations shall be stored securely in the Company’s compliance records system.

Step 7 - Internal record: A complete record of each report filed, including the internal escalation, the MLRO’s determination, the submitted report, the goAML reference number, and any subsequent correspondence or



feedback received from the FIU, shall be entered into the Company's SAR/UTR register and retained in accordance with the record-keeping obligations set out in this Policy.

DOCUMENTATION AND RECORD-KEEPING

All goAML submission confirmations, including portal-generated receipts, reference numbers, and any acknowledgements or feedback received from the FIU, shall be retained in the Company's compliance records system.

The Company shall maintain a formal internal SAR/UTR register in accordance with the provisions of this Policy. Each register entry shall be cross-referenced to the corresponding goAML reference number where a report has been filed externally. Where the MLRO determines not to file a report, the reasons for that determination shall be documented and recorded in the register.

All records relating to goAML submissions, internal determinations, and supporting documentation shall be retained for a minimum period of five (5) years from the date of the report or the date of the determination not to report, in accordance with applicable record-keeping requirements.

TECHNICAL CONTINGENCY

In the event that the goAML portal is temporarily unavailable due to technical issues, system maintenance, or any other cause, the following contingency procedures apply:

The MLRO shall immediately document the nature and timing of the technical issue, including all attempts made to access the portal. The MLRO shall contact the FIU directly to notify them of the technical difficulty and to obtain guidance on an alternative submission method, which may include submission by secure email or other means authorised by the FIU.

Any report that cannot be submitted via the goAML portal due to technical unavailability shall be prepared in the prescribed format and submitted via the FIU-approved alternative method as soon as practicable. Upon restoration of portal access, the relevant report shall be re-submitted or cross-referenced via the portal as directed by the FIU, and a record of the alternative submission shall be retained.

All technical contingency actions, including the nature of the issue, the steps taken, the method of alternative submission, and the outcome, shall be fully documented and retained as part of the Company's compliance records.

QUALITY ASSURANCE

The MLRO shall conduct a periodic review of the Company's goAML reporting practices, including an assessment of the timeliness and completeness of reports submitted, the accuracy of goAML portal registrations and access credentials, the adequacy of the internal escalation and determination procedures, and compliance with the reporting timelines set out in this Policy. Such review shall be conducted at minimum on a quarterly basis.

The Company's goAML reporting procedures and timelines shall form a mandatory component of the scope of the annual independent AML audit carried out in accordance with this Policy. The audit shall include a sample review of submitted UTRs, internal determinations not to file, reporting timeliness against the deadlines set out herein, and the accuracy and completeness of the SAR/UTR register. Findings arising from the quality assurance review and the annual audit shall be reported to senior management and, where material, to the Board of Directors, with corrective action plans implemented without undue delay.

SAR/UTR REGISTER MAINTENANCE

The Company shall establish and maintain a formal register of all Suspicious Activity Reports (SARs) and Unusual Transaction Reports (UTRs), whether filed externally with the FIU or retained internally. The register shall include, at a minimum:

- the date of detection and date of filing (or decision not to file);
- the identity of the player or transaction party involved;
- a summary of the suspicious activity or unusual transaction;
- the goAML reference number (for externally filed reports);
- the outcome or status of the report (e.g., pending, filed, closed, feedback received from FIU); and
- any follow-up actions taken.

The register shall be maintained by the Compliance Officer, kept confidential, and accessible only to authorized personnel on a need-to-know basis. The register shall be reviewed periodically by the MLRO to identify trends, patterns, or systemic issues, and a summary shall be included in the annual AML&TF compliance report to the Board of Directors.

All register entries and supporting documentation shall be retained for a minimum of five (5) years from the date of the report, in accordance with the Company's record-keeping obligations.



5. EMPLOYEES

STAFF RELIABILITY AND PROBITY

The Company represents 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 are of paramount importance to an extent unseen in other businesses.

The Management of the Company 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.

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.

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.

AML TRAINING

- The Compliance Officer is responsible for the conduct of the introductory AML&TF training course for every new employee. Such training shall be completed within a reasonable period following commencement of employment, taking into account the employee's role and access to customer-facing or compliance-sensitive functions. The Compliance Officer shall also arrange for periodic refresher training for all relevant personnel, at intervals determined appropriate by the Compliance Officer but at minimum on an annual basis. Enhanced or specialised AML&TF training may be provided to employees in higher-risk functions, such as those involved in customer onboarding, transaction monitoring, or compliance oversight, where the Compliance Officer determines such training would be beneficial. Training content shall be delivered 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&TF investigations.

The Compliance Officer 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.

A handwritten signature in blue ink, located in the bottom right corner of the page. The signature is stylized and appears to be a single letter 'A' or a similar character.

6. RECORD-KEEPING

The Company is keeping, for at least five years, all necessary records on transactions (both domestic and international), to comply with information requests from the competent authorities. These records permit reconstruction of individual transactions (including the amounts and types of currency involved) so as to provide, if necessary, evidence for prosecution of criminal activity. From the collected information, the following is being kept:

1. 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 (Appendix B contains a sample of the customer account history):
2. Primary customer data (required at the registration stage) and scanned documents. The fullness of the data required in each particular case is driven by the risk triggers described in Section 3 of this policy 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.
3. Comments by the employees of the respective departments concerning each player account. There are fields designated to comments in the program for four departments: Anti-fraud, Payments, VIP Players and Support. Each department provides comments (notes) in their respective fields only and strictly in accordance with their official duties. For example, the VIP Players Department usually provides ranking information of VIP players (ranked by stars: from a "small" VIP player to the largest according to graduation, etc.).

When the comments lose relevance with the passage of time, head of the appropriate department may remove a comment however the log will be kept on record indefinitely.

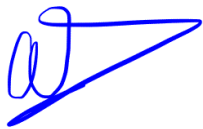
4. System also keeps records regarding profitability of each gaming account for the entire period of its existence – also utilized as an ML&TF risk trigger.
5. All suspicious activities and transactions are recognized and recorded in the system. Concurrent analysis is conducted on each such activity or transaction in accordance with the Operating Control Matrix. Upon receipt of the Report on suspicious activities and transactions, Compliance Officer decides as to the further course of actions concerning possible reporting of the transactions to authorities and licensing authority.
6. All transactions history of a player including amendments, additions and deletions to the transactions are kept for records for 5 years' period. For CDD 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.
7. The system provides technical facilities for sending the messages to clients; such messages are stored in a special Message Box in the context of each player account, as well as in the logs of the system. Disputes with the player arising in the gaming context are solved operationally by communicating with the customers via Skype, email, chat, or phone. The records of disputes are stored in the system.



7. RATIFICATION

The Policy will be valid for a period up to its annual or required reviewing. This Policy has been duly executed this day of 01/03/2026.

Director eMagnus Curacao B.V.



4/6/2026



APPENDICES

APPENDIX A. OPERATING CONTROL MATRIX (FRAGMENT)

Number	Subareas	Control	Control type (prevention/detection)	Procedures description	When/ how often is performed/ trigger
1	Customers acceptance	Host country is monitored (prohibited: USA, Israel, France, Estonia, UK and outlying territories, Italy, Spain, Denmark, the Netherlands, Mohawk Territory of Kahnawae. list updates periodically)	prevention	System doesn't allow registration of the players from the prohibited countries	100% coverage
2	Customers acceptance	Age of the players is monitored	prevention	System doesn't allow registration of the players under 18 years	100% coverage
3	Customers acceptance	PEPs identification (KYC procedure)	detection	all the players are checked within PEPs list	100% coverage
4	Customers acceptance (1st deposit stage)	Only 1 account is allowed for 1 player	prevention	Table of first deposits is daily reviewed within the system - IP addresses are checked through "Search IP" button in the programme - deposits done through 1 wallet	100% coverage
5	Customers acceptance (1st deposit stage)	Full verification for risky players and full verification of the players where the country requires it (Belorussia)	prevention	Additional checks are performed for risky players: - passport copies - photo-passport copies - password sending to the registered address	Special criteria (risk country, risk currency, risk amount)
6	Customers acceptance (1st deposit stage)	Black-lists	prevention	all the players are automatically checked within the Black-lists in each Payment system	100% coverage
7	Customers acceptance (1st deposit stage)	PEP-lists check by PSPs	detection	all the players are automatically checked within the PEP-lists in each Payment system	100% coverage
8	Activation of account	Activation of the player can be done only after his e-mail check (it should be real)	prevention	Automatically generated link is sent to the registered e-mail of the player. The account will not be activated, till the link is followed	100% coverage

Responsible department	Who is doing?	To whom is reported?	Reports, back-ups, further actions
Automatic control	Automatic control	Automatic control	Account is not opened
Automatic control	Automatic control	Automatic control	Account is not opened
Automatic control	Automatic control	Head of Anti-fraud Department	Restrictions to the account undertaken, request for additional documents sent to the player
Factoring and monitoring department	4-5 persons depending on the playing activity	The account is either blocked or agreed with the Head of the Department for blocking	Operational control, history of each player with comments can be reviewed in the system.
Factoring and monitoring department	4-5 persons depending on the playing activity	Operational review is done by the Head of the Department	Operational control, history of each player can be reviewed in the system
Automatic control	Automatic control	Automatic control	Account is blocked, notification sent to the player
Automatic control	Automatic control	Head of Payments Department	Restrictions to the account undertaken, request for additional documents sent to the player
Automatic control	Automatic control	Automatic control	Automatic control

W

APPENDIX B. SAMPLE OF CUSTOMER TRACK-RECORD

3440GtPremium0.15REGISTRATION: 124

Brand Time:
User Time:

PLAYER INFOSPORT LIMITSKYCFIN HISTORYTRX HISTORYBET HISTORYCASINO HISTORYMANUAL TRX

Account notes

GeneralPaymentsRisk

Player account

Trusted groupUntrusted FD

Verified

Test account

Player settings

WD restrictedDeposit restricted

Autopayments restrictedLogin restricted

Bets no allowed

Forbid Eva

Forbid Virtual Sports

Forbid Tv Games

Forbid Live Casino

Forbid Slots

Forbid Instant Games

Forbid Bingo

Player WMIN

Personal data - G e ***

Last name

First nameC e

Middle nameEnter middle name

Date of birth095

CPF10

Residence address

Country

Player financial accounts

Other Balances

bonus balance

bonus eva

cash deposit

locked crm

locked eva

tax deposit

Cash Balances

Statistic

sport turnover

profit sport

bonus sport

bonus sport deposit

bonus sport retract

locked sport

profit eva

profitability sport

Pending Balances

Payment accounts

Payment methodAccount numberDateStatus

No data

Registration data

Registration IP-address1704

Restriction settings

Access to withdrawals. X

Player Context

Brand

W