

Anti-money laundering (AML) and Counter terrorist financing policy

SORT SERVICES B.V.

Version:	1
Date of version:	11.01.2025
Created by:	Internal Compliance Committee
Confidentiality level	Internal

1. INTRODUCTION

Pursuant to the Code of Criminal Law (Penal Code) (N.G. 2011, no. 48), money laundering is a criminal offence in Curaçao.

Further main national regulations relating to money laundering and terrorist financing are the following:

- a. The National Ordinance on Money Laundering (P.B. 1993, no. 52);
- b. The National Ordinance on the Reporting of Unusual Transactions (N.G. 1996, no. 21) as lastly amended by N.G.2024,no.41(N.G.2017,no.92)(NORUT) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;
- c. The National Ordinance on Identification of Clients when Rendering Services (N.G. 1996, no. 23) as lastly amended by N.G. 2024 no.41 (N.G. 2017, no. 99) (NOIS) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;
- d. The National Decree containing general measures on the execution of articles 9, paragraph 2, and 9a, paragraph 2, of the National Ordinance on Identification of Clients when rendering Services. (National Decree containing general measures on Penalties and Administrative Fines for Service Providers) (N.G. 2010, no. 70);
- e. Sanctions national decree Al-Qaida c.s., the Taliban of Afghanistan c.s. Osama bin Laden c.s., and terrorist to be designated locally (N.G. 2010, no. 93); and
- f. National Ordinance on the Obligation to report Cross-border Money Transportation N.G. 2002, no. 74) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations.
- g. National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- h. Kingdom Sanction Act (N.G. 2016, no. 54);

These laws and decrees serve as the basis for the procedures maintained by the financial sector of Curaçao to detect and deter industry related risks for money laundering, the financing of terrorism or other criminal activities.

International regulations

As a member of the Financial Action Task Force (www.fatf-gafi.org) and of the Caribbean Financial Action Task Force (www.cfatf-gafic.org), Curaçao is meeting international standards by regularly implementing these standards in its national legislation.

On an international level, the FATF plays an important role in the combating of ML and the TF and proliferation of weapons of mass destruction.

The FATF monitors the progress of its members in implementing necessary measures, reviews ML and TF techniques and countermeasures, and promotes the adoption and implementation of appropriate measures globally.

In performing these activities, the FATF collaborates with other international bodies involved in combating money laundering and the financing of terrorism. In total 34 countries are direct members of the FATF and through regional organizations over 180 countries are connected to the FATF.

Subsequently the present policy is a combination of the FATF and local AML/CFT rules and regulations. This ensures a solid, internationally accepted basis regarding AML/CFT. In case local laws and regulations require additional compliance duties, the Company is free to develop additional procedures to comply with local regulations.

The Anti-Money Laundering Policy provides the guidelines that should be followed throughout the Company to assist in the detection and/or prevention of money-laundering and terrorist financing activities in accordance with the Law.

The aim of this manual is to provide the guidelines that should be followed throughout the Company for the detection and/or prevention of money-laundering activities and terrorist financing. All Company staff should execute their duties as per the guidelines set out in this Policy and the relevant Company Operations Manuals.

Money laundering / Terrorist Financing is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities (e.g. illegal drugs dealing, tax evasion etc.) thereby avoiding prosecution, conviction and confiscation of the criminal funds. The ultimate aim of this process is to convert such criminal proceeds into “clean” money. The risks to the gambling sector primarily involve being used to facilitate this process, whether knowingly or unwittingly.

1.1 DEFINITION OF MONEY LAUNDERING

Money laundering is defined very widely and includes all forms of handling or possessing criminal property, including possessing the proceeds of one’s own crime, and facilitating any handling or possession of criminal property. Criminal property may take any form, including money, securities, tangible property and intangible property.

Illegal profits can be generated for example through drug trafficking, illegal arms sales, smuggling, insider trading, embezzlement, bribery and internet fraud schemes.

Businesses and individuals need to be alert of the risk of customers, their counterparties and others laundering money in any of its possible forms. The business or its customer does not have to be a party to money laundering for a reporting obligation to arise.

Money laundering is not only about cash transactions. Money laundering can be achieved through virtually every medium and licensed gambling operator or business.

For the purpose of this Policy, money laundering is also taken to encompass activities related to terrorist financing, including handling or possessing funds to be used for terrorist purposes as well proceeds from terrorism.

1.2. DEFINITION OF TERRORISM AND TERRORISM FINANCING

Terrorism is defined as the use or threat of action designed to influence government, or to intimidate any section of the public, or to advance a political, religious or ideological cause where the action would involve violence, threats to health and safety, damage to property or disruption of electronic systems.

Terrorism financing is an offence by any means, directly or indirectly, unlawfully and wilfully, which provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in whole or in part, in order to carry out an act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.

1.3 PREVENTION OF MONEY LAUNDERING AND TERRORISM FINANCING

The Company is a licensed gambling operator, which is obliged by the national legislation and the union law of the EU to actively implement strict measures to prevent money laundering and terrorist financing (preventive measures).

In order to properly apply preventive measures, the Company:

- developed and maintained a risk-based approach to money laundering and terrorist financing risk assessment and management;
- established an appropriate personnel structure, involved employees and managers at all levels in the implementation of preventive measures, created conditions for the improvement of employees' knowledge and skills and requires high competence of employees in the implementation of preventive measures;
- apply appropriate customer identification procedures and enhanced monitoring for higher risk customers (eg. politically exposed persons);

- apply risk-based ongoing customer monitoring systems and procedures;
- executes international financial sanctions, implements restrictive measures and does not enter into business relations with persons subject to sanctions or restrictive measures, and terminates them immediately if such relations have been initiated;
- established procedures for notifying the relevant law enforcement authorities of suspected dangerous or illegal activities;
- manages and stores all information related to the application of preventive measures.

The Company seeks to provide its services to honest, lawful and transparent customers using the Company's services, therefore, in order to reduce operational risks, does not enter into business relationships, and if such relationships are initiated and the following circumstances become clear, immediately terminates the relationship with the customer if they intend to use or use the Company's services in such a way that it is reasonable to suspect that the services provided by the Company are used for money laundering, terrorist financing, tax evasion, fraud or other criminal and illegal activities.

The services provided by the Company are focused on the provision of gambling for entertainment purposes to persons residing in the European Union/ European Economic Area. Therefore, the Company pays special attention to customers who are not residents of the country or the European Union/ European Economic Area and use the Company's services outside the country and starts and continues business relations with such customers in exceptional cases, fully convinced of the customer's transparency and purposes of using the Company's services.

1.4 RESPONSIBILITIES

All employees of the Company must follow this Policy and be acquainted with the legal acts regulating the prevention of money laundering and terrorist financing, participate in training organized by the Company on this topic.

The employee appointed by the Company, responsible for organizing the implementation of money laundering and terrorist financing prevention measures and cooperating with the Curacao Gaming Control Board (the Commission), is the Company's money laundering reporting (the Responsible Employee). Compliance Officer, the key individual responsible for the prevention of money laundering and the

financing of terrorism, has overall responsibility for ongoing regulatory compliance and anti-money laundering procedures.

Money Laundering Compliance Officer (MLCO) will be fully engaged in defining and managing the processes needed to prevent money laundering and other fraudulent activity based on the following principles:

- The Company assumes that most customers are not money launderers. However, it identifies players since it requires the applicable regulations, using a risk-based approach.
- The Company monitors all transactions and activity.
- The Company continuously monitors its customers as well as risks and processes.
- The Company will ensure that all relevant employees are trained on AML and CTF policies and procedures and emphasize alerting these risks. Relevant employees will be required to pass competency tests on this topic at least once annually.

The Company ensures that all confidential information received for the purpose of money laundering and terrorist financing is adequately protected. The information is disclosed only to those employees of the Company whose direct functions require this information. Confidential information shall be disclosed to third parties only in the cases and on the grounds provided for in the legal acts. The Company's Compliance Officer is responsible for the data protection.

The Company regularly evaluates the effectiveness of its internal control systems, reviews and updates its assessment of the money laundering and terrorist financing risks associated with its operations, taking into account customer behaviour and the monetary operations they perform (*modus operandi*). If necessary, the Company takes measures to improve the effectiveness of internal control systems, regularly reviews and updates this Description.

2. PERSONS PARTICIPATING IN THE INTERNAL CONTROL SYSTEM AND THEIR FUNCTIONS

All employees of the Company who communicate with customers, check customer registrations, monitor customer actions and monetary transactions, approve payments and accept payments, must know how to identify suspicious customer actions and monetary transactions, what actions must be taken to implement money laundering and terrorist financing prevention. The Company regularly provides training to employees to ensure proper performance of their duties in the field of money laundering and terrorist financing prevention.

It is the responsibility of all Company employees to read and understand the Company's Anti-Money Laundering and Terrorist Financing Policy. Each employee receives a copy of the Policy and must read and understand its contents, the responsibilities and procedures outlined in it.

The Company's internal control system for the prevention of money laundering and terrorist financing (the control system) includes all employees of the Company (including its managers and members of the Board), however, depending on the duties and competencies assigned, the control system participants have different roles and responsibilities.

It is the duty and responsibility of the Head/Officer of the relevant Division to exercise the duties within their area of responsibility as itemized in this Policy, and be in line with the Policies of the Company, the Law, and any directives relevant to their area of responsibility.

The participants of the control system in the Company and their levels in the system are:

- Decision-making level:
 - CEO (General manager)
 - MLCO, Head of Risk and Payments
- Operational level:
 - Risk and payments specialists
 - Compliance officers
- Auxiliary level:
 - Chief financial officer
 - Head of Legal

Each level of the control system is responsible for the implementation of certain tasks assigned to that level:

- Decision-making level is responsible for monitoring the effectiveness of the control system, its continuous improvement, and individual and complex decision-making.
- Operational level is responsible for monitoring customer activities and operations and applying the established preventive measures, reporting to decision-making level employees.

- Auxiliary level is responsible for assistance to the operational and decision-making levels in providing the necessary data for preventive measures and decision-making.

When implementing preventive measures, the levels of the control system interact according to the following communication scheme:

- Employees of operational and auxiliary levels are directly subordinate to and accountable to the General Manager of the Company.
- The Money Laundering Compliance Officer monitors the preventive measures implemented by the operational level employees, reports on their implementation to the General Director of the Company and the responsible member of the Board, as well as provides recommendations on the application of preventive measures to the operational level employees and the General Director of the Company.
- The responsible member of the Board, based on the reports submitted by the Money Laundering Compliance Officer, makes decisions on the improvement of preventive measures and gives instructions on the efficiency of operations to the General Director of the Company.
- Decision-making level employees jointly collegially, at least once a year, assess the situation of application of preventive measures and prevention of money laundering and terrorist financing in the Company and the procedures specified in this Description, and decide on improvement of preventive measures or control system. Decisions are made with relevant documents.

3. ETHICS STANDARDS AND MANAGEMENT OF CONFLICTS OF INTEREST

In performing their work functions, the Company's employees must follow the values established by the Company, be honest, intolerant of violations of the law, objective in making decisions and avoid conflicts of interest.

For the purposes of this Description, a conflict of interest is understood as a situation when an employee of the Company, while performing their duties or performing an order, must make a decision, participate in its acceptance or execute an order that is related to their and (or) their relatives' private interests.

Employees of the Company must avoid conflicts of interest, in particular (but not limited to) by taking preventive measures against their relatives or acquaintances, such

as controlling the gambling of such persons, addressing suspicious monetary transactions for the Commission, etc.

An employee of the Company who is involved in a potential conflict of interest situation must immediately inform their immediate manager and refrain from making any decisions that may be considered a violation of a conflict of interest. In this case, the manager of the absent employee decides who to instruct in this situation or makes the decision themselves.

4. CUSTOMER IDENTIFICATION AND DUE DILIGENCE PROCEDURES

The law requires that the company maintains certain identification procedures to verify its customers' identity. Customer due diligence (CDD) is required under applicable law when the company is establishing a business relationship with a customer, where it or any member of staff suspects money laundering or terrorist financing or where the veracity or adequacy of documents and client's information previously obtained for CDD purposes is doubted.

The purpose of the CDD is to confirm the identity of the client. For the client's identity to be confirmed, independent and reliable information is required.

The Company must also apply customer due diligence measures:

- at other appropriate times to existing customers on a risk-based approach;
- when Company becomes aware that the circumstances of an existing customer relevant to its risk assessment for that customer have changed.

In determining when it is appropriate to take customer due diligence measures in relation to existing customers, the Company must take into account, the following:

- any indication that the identity of the customer has changed;
- any transactions which are not reasonably consistent with the relevant person's knowledge of the customer;
- any change in the purpose or intended nature of the relevant person's relationship with the customer;
- any other matter which might affect the relevant person's assessment of the money laundering or terrorist financing risk in relation to the customer.

The Company must conduct regular customer and transaction due diligence and must undertake a prescribed ongoing due diligence process to monitor its account, service or relationship with each of its customers to identify, mitigate and manage the risk it may reasonably face with its customer that might involve money laundering, financing of

terrorism or other serious offences. In addition, the Company must record its findings in writing.

4.1 KNOW YOUR CLIENT PRINCIPLE (KYC)

“Know Your Client” (KYC) processes are intended to enable a company to form a reasonable belief that it knows the true identity of each customer before the client enters into a business relationship with the Company.

The need to effectively KYC is at the very heart of an efficient anti-money laundering management system. KYC due diligence is a continuous process and not only limited to clients seeking to open new accounts. While client identification procedures are aimed at establishing clients’ identity, the Company is also required to decide whether the clients’ risk-profile necessitates enhanced due diligence procedures.

The resources used to undertake effective customer due diligence are not prescribed. Various sources may be used to enhance a business’ knowledge of its client, including direct discussion with the client, information (e.g. websites, brochures, reports etc) prepared by the client and review of public domain information.

4.2 CUSTOMER DUE DILIGENCE MEASURES

A clear customers’ acceptance policy is developed and established, which is completely in line with the legislation. The customers’ acceptance policy is prepared after detailed assessment of the risks faced by the Company from its customers and/or their transactions and/or their countries of origin or operations.

The Company applies general customer due diligence (CDD) measures to the customers at the registration stage. The purpose of the CDD is to confirm the identity of the customer and process consists of:

- Identification: Every potential customer of the company must complete the account opening procedure, accept business terms and conditions and confirmed that they are not under 18 years old, the Company will perform an Anti-Money Laundering (AML) check to ensure compliance with regulatory requirements and mitigate potential risks.

The Company uses a designated KYC software tool to perform AML checks, including Politically Exposed Persons (PEPs) and sanctions screening, as well as adverse media checks. These processes are critical for ensuring compliance with regulatory obligations and mitigating risks associated with money laundering, terrorist financing, and other financial crimes.

- Politically Exposed Persons (PEPs) are defined as:

- individuals who are or have been entrusted with prominent public functions by a country, such as heads of state or of government, senior politicians at national level, senior government, judicial, military or political party officials at national level, and senior executives of state-owned corporations of national significance;

- individuals who are or have been entrusted with a prominent function by an intergovernmental organisation or international sports federations, such as secretaries general, directors, deputy directors and members of the board or individuals who have been entrusted with equivalent functions.

The family members and close associates of politically exposed persons are individuals who are closely connected to persons from above either through their family or for social or professional reasons.

Politically exposed persons are no longer regarded as being politically exposed when 12 months have elapsed since they relinquished their position.

Business relationships with politically exposed persons and their family members or close associates are deemed in every case to be business relationships with a higher risk.

Business relationships with politically exposed persons and politically exposed persons in international organisations and their family members or close associates are deemed when combined with one or more further risk criteria to be business relationships with a higher risk.

- Sanctions Screening: The Company screens all customers against PEP lists, terrorist lists, global sanctions lists as well as any other blacklists and watchlists that might be relevant of the respective level of AML due diligence.
- Adverse media checks are conducted to identify negative information linking the customer to financial crimes, fraud, or reputational risks.
- Verification: The process of confirming a customer's claimed identity by obtaining and validating documentation or information from reliable and independent sources that substantiate the authenticity and accuracy of the identity provided. Customer Due Diligence (CDD) is applied based on the assessed risk level. Higher risk customers undergo more stringent checks.

- Identity Documents: Collect and validate a government-issued photo ID (e.g., passport, national ID, or driver's license) with a signature, matching the provided name, not expiring within three months, and confirming the individual is 18 or older.
- Liveness Check: To further ensure the authenticity of the customer's identity, a liveness check must be conducted using biometric methods, such as a selfie with liveness detection.
- Address Verification: The customer is required to provide a valid proof of address document that matches the name on their ID. The submitted document must confirm their current residential address as provided during registration.
- Acceptable Documents: The main requirements for documents provided by the customer are that they must be valid, not expired, clear, legible, and of good quality.
- Threshold approach: The Company applies Customer Due Diligence (CDD) measures to any transaction amounting to EUR 2,000, whether executed as a single operation or through multiple operations that appear to be linked. A "transaction" includes the wagering of a stake, such as the deposit of funds required to participate in remote gambling, as well as the collection of winnings. This collection encompasses the withdrawal of funds deposited to participate in remote gambling or winnings resulting from the staking of such funds. Transactions are considered linked when they form part of the overall activity conducted by a customer during a single session on the operator's gambling facilities. However, this example is not exhaustive, and the Company assesses other circumstances in which transactions may be linked using a risk-based approach.

4.3 ONGOING MONITORING

The company must conduct ongoing monitoring of a business relationship, including:

- scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the relevant person's knowledge of the customer, the customer's risk profile;
- undertaking reviews of existing records and keeping the documents or information obtained for the purpose of applying customer due diligence measures up-to-date.

4.4 CLIENT CATEGORIZATION AND RISK ASSESSMENT

The Company undertakes reasonable steps to identify, assess, and manage the risks of money laundering (ML) and terrorist financing (TF) that may arise within its business activities.

To achieve this, the Company conducts a comprehensive risk assessment of all its operations, which serves to identify emerging risks of ML/TF and prioritize areas requiring enhanced attention and resources. The risk assessment guides the implementation of appropriate preventive measures.

The Company establishes and maintains robust policies, controls, and procedures to effectively mitigate and manage ML/TF risks identified through its risk assessments. These policies, controls, and procedures are subject to regular review and updates, particularly in response to significant changes in the Company's operations, regulatory framework, or business environment.

The Company's MLCO (Money Laundering Compliance Officer), Head of Risk, and Payments Team are jointly responsible for performing, reviewing, and updating the risk assessment process. Each risk assessment is documented and reviewed by the Company's management.

Following the completion of a risk assessment, the Responsible Employee must present the results of the ML/TF risk assessment to the Company's management bodies. If existing risk management measures are deemed insufficient, the MLCO prepares a revised risk management plan, which is subject to approval by the General Director.

Customers are categorized as High-Risk, Normal-Risk, or Low-Risk based on a detailed analysis of multiple factors, including but not limited to:

- The customer's background.
- The type and nature of the customer's business activities.
- The customer's country of origin or residence.
- The services applied for by the customer.
- The anticipated volume and nature of transactions.
- The expected source and origin of funds.

The Company employs a Risk Assessment Table to calculate the average risk classification for each customer. The risk factor scores are summed, and the total determines the customer's categorization as High-Risk, Normal-Risk, or Low-Risk.

The results of the customer risk assessment are documented in a “Client Risk Assessment” form, which is stored securely in the customer’s file. This ensures traceability and compliance with regulatory requirements.

Customers identified as Politically Exposed Persons (PEPs), as well as those associated with high-risk countries or jurisdictions, are automatically categorized as High-Risk. Additional Enhanced Due Diligence (EDD) measures are applied to these customers to mitigate potential ML/TF risks effectively.

4.5 ENHANCED DUE DILIGENCE

The Company applies enhanced customer due diligence measures (EDD) and enhanced ongoing monitoring, in addition to the required CDD measures, to manage and mitigate the money laundering or terrorist financing risks.

The Company is applying EDD measures in the following cases:

- in any case, identified by the Company or in the information provided by the authorities to the Company as one where there is a high risk of money laundering or terrorist financing;
- If the Company has determined that a customer or potential customer is a person, or a family member or close associate of Person connected to Sporting Events, who has close connection to a sport event, team, sporting association or organization. For avoidance of doubt, a “person having a close connection to a sport or sporting event” includes an individual who (having regard to information that is public or readily available) owns, plays with, coaches, trains or manages a sporting team, or who has a senior role with the governing body of a sport.
- If the Company has doubts as to whether the information collected regarding the identity of the customer is correct or not (or no longer) accurate;
- if the Company has determined that a customer or potential customer is a PEP, or a family member or known close associate of a PEP.
- in any case where the Company discovers that a customer has provided false or stolen identification documentation or information and the Company proposes to continue to deal with the customer;
- in any case where a transaction is complex or unusually large, or there is an unusual pattern of transactions, or the transaction or transactions have no apparent economic or legal purpose,

- if the payment of a customer's winnings is made to a different payment account of the customer than to the account from which the customer makes the wagers,
- in any other case which, by its nature, can present a higher risk of money laundering or terrorist financing, including.

For customers deemed high-risk or when elevated risks are identified, the following EDD measures are undertaken, as applicable:

- undertaking Re-verification of identity (repeated CDD).
- Establishing how the customer acquired his wealth to be satisfied that it is legitimate:
 - Salary or business income (e.g., payslips, employer letters, audited accounts, or tax declarations for self-employed individuals).
 - Sale of financial instruments (e.g., certified sale contracts or investment statements)
 - Property sales (e.g., certified sale contracts or solicitor/estate agent letters).
 - Inheritance (e.g., certified copy of the will indicating the value of inheritance).
 - Sale of a company (e.g., certified contracts, media reports, or accountant/solicitor letters).
- Determining the source of the customer's funds to ensure they do not originate from criminal activities.
- Ensure that deposits originate from payment methods and do not allow anonymity by requesting copies of bank statements or account statements.
- Undertaking increased continuous monitoring of the business relationship.
- The suspicious transaction must be investigated, and the business relationship underlying the transaction shall be monitored to assess the risk of money laundering and terrorist financing.

Given that the Company's relationships with customers is remote, the Company carries out enhanced continuous monitoring of customer actions and monetary transactions. Monitoring is carried out in accordance with the established risk assessment and criteria for identifying suspicious customer actions and transactions. Evaluations are performed taking into account the information available to the Company about the client and the actions performed by the client; monitor whether the client's actions and monetary transactions are specific to him, whether they are in line with the client's financial capabilities, or whether there are any suspicions that the client may be involved in fraud, money laundering or terrorist financing. Particular attention is paid to:

- Transactions that are not specific to the customer, such as unusually increased transaction amounts, transactions without a clear economic purpose;
- Transactions which give rise to suspicion that they may be carried out by another person.

Suspicious customer behaviour can be identified by the following criteria:

- The client avoids providing information about himself (document confirming the place of residence, information about the source of funds used for the Company's services or other information requested by the Company);
- It is difficult or impossible to contact the client, no one answers the provided phone number or it is permanently switched off, the client does not answer by contacting the e- mail address, his place of residence and contact information often changes;
- The client decides to close the account by requesting additional documents/information on the origin of his funds, address of residence or other requested information;
- The client refuses to provide information about the origin of his funds, address of residence or other requested information.

Suspicious customer monetary transactions can be identified by the following criteria:

- The nature of the monetary transactions performed by the customer raises the suspicion that the aim is to avoid the inclusion of monetary transactions in the

journal maintained by the company when the amount of contributions or payouts exceeds EUR 500;

- The customer only replenishes the account (replenishes it many times with small amounts or one or more larger amounts), but does not place any bets, or makes only a few bets with very small amounts and then payouts a large amount;
- Customer contributions exceed known customer capabilities;
- Significant discrepancy between the customer's cash transaction history and the gambling history - the customer's account contains a large amount of money, but no bets are made (or almost not made);
- A sudden change in the customer's history of contributions, payouts and/or bets.

In the context of enhanced monitoring of customer actions and monetary transactions, the Company may additionally request the following documents:

- A bank statement showing the monetary transactions performed in connection with the customer's gambling account;
- A screenshot showing the details of the owner of the e-wallet used by the customer to top up the gaming account;
- A document confirming the source of funds used for the Company's services (always requested from politically exposed persons with whom the Company decides to continue relations).

Undertaking the EDD on transactions, the Company's fundamental aim is to ensure the transparency of payment flows. Accordingly, the origin and destination of the money used in a transaction shall be traceable back in each case to an account.

5. ACCOUNT CLOSURE PROCEDURE

The Company may decide to close a customer's account for various reasons, including but not limited to:

- Fraud: Engaging in fraudulent activities on the platform.

- Cheating: Utilizing unfair practices or methods to gain an advantage.
- Bonus Abuse: Exploiting promotional offers in a way that breaches their intended purpose.
- Allowing Third-Party Use: Permitting another person to use the account, contrary to terms and conditions.
- Underage Gambling: Evidence that the customer is below the legal age for gambling.
- Problem Gambling: Demonstrating signs of gambling addiction or harm.
- Abusive Behaviour: Being abusive or threatening towards Company staff.
- Commercial Concerns: Situations where the customer's activities present a risk to the Company's operations or reputation.
- CDD Failure: Failure to comply with Customer Due Diligence (CDD) requirements.
- Terms and Conditions Breach: Violations of the Company's agreed terms and conditions.

If there is suspicion or knowledge that the customer is involved in money laundering (ML) or terrorist financing (TF), the Company is legally obligated to terminate the business relationship unless appropriate consent has been obtained from the relevant authorities. Even with such consent, it may remain precautionary to close the account.

Due to tipping-off provisions under applicable AML/CFT legislation, the Company must ensure that the account closure is handled with discretion, and the customer cannot be informed that the closure is due to ML/TF concerns.

The Money Laundering Compliance Officer (MLCO) must evaluate whether a Suspicious Activity Report (SAR) has been submitted in connection with the customer's behaviour. If a SAR was filed, the MLCO must determine whether appropriate consent was sought to continue or terminate the business relationship.

Additionally, if the Company is unable to complete or apply the required CDD measures when the CDD threshold is reached, transactions with the customer must cease, and

the business relationship must be terminated. This ensures compliance with legal and regulatory obligations to mitigate risks of financial crime.

6. DEPOSIT AND WITHDRAWAL MANAGEMENT PROCEDURES

Player account balance. Each player has a wallet with funds from which bets are deducted, and winnings added. The player can top up the funds in his account by depositing through the cashier on the site and then use these funds to place bets. Bets are deducted from his account balance, and winnings are added to the account balance. The player can withdraw withdrawals of available funds in the player's balance. The Company does not offer credit to players. A player may not transfer funds to another player.

Payment methods. Payments shall only be accepted and made from accounts held with licensed financial institutions or through licensed payment providers. No cash deposits/withdrawals will be effected between the Company and its players.

Player deposits. After registering, a player may then deposit funds into their account through the cashier on the site. In order to facilitate these deposits, the company has integrated a number of gateways. All gateways are PCI DSS compliant, and the company does not hold any credit card data itself. The company submits the transaction to the PSP and then waits for approval from the card acquirer/e-wallet. On approval, the deposit status is updated, and the funds added to the player's balance.

Player withdrawals. A player with an available balance will be able to request a withdrawal of the funds via the cashier on the site. The player will enter the amount they wish to withdraw and select their preferred payout method. The withdrawal amount is then deducted from the player's balance.

In remitting funds to the player, we will, where possible, remit the funds directly into the account where the funds originated from. Provided that where this is not possible, we will remit the funds to the player in line with the requirements under AML legislation.

When the customer orders any amount of payout, the specialists of the Company's payment department check:

- Customer's contribution, bet and payout history;
- Documents provided by the client and available data about the client.

Payouts are made only after they have been approved, when it is determined that there is no fraud or other suspicious signs in the client's actions.

7. SUSPICIOUS TRANSACTION REPORTING

The MLRO will consider each report and determine whether it gives grounds for knowledge or suspicion. If they do, then a Suspicion Transaction Report 'STR' should be submitted to the Curacao Gaming Control Board (the Commission).

A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report the activity then arises. Likewise, if concern escalates following further enquiries, it is reasonable to conclude that the transaction is suspicious and will need to be reported to the Commission.

The MLCO assesses all the circumstances and the customer or others more questions if needed. The choice depends on what is already known about the customer and the transaction and how easy it is to make further enquiries.

Every employee of the Company must report to the MLCO if:

- If it is known or suspected that any amount is derived directly or indirectly from or participating in a criminal offense, and if it is known or suspected that the money is intended to support one, several terrorists or a terrorist organization, no later than one working day from the occurrence of such knowledge or suspicion, the Commission shall be notified. If it is established that a customer performs a suspicious monetary transaction, regardless of the amount of the monetary transaction, that transaction shall be suspended (unless it is objectively impossible due to the method or other circumstances) and the transaction shall be reported no later than within 24 business hours for Commission. Such transactions must be objectively identified in the light of the client's activities, which by their nature may involve money laundering and (or) terrorist financing, the identification of the client and the ongoing monitoring of the client's actions;
- Upon receipt of information that the client intends or attempts to perform a suspicious monetary transaction, Commission is informed immediately.
- If it is established that a customer performs a suspicious monetary transaction, regardless of the amount of the monetary transaction, that transaction shall be suspended (unless it is objectively impossible due to the method or other circumstances) and the transaction shall be reported no later than within 24 business hours for Commission. Such transactions must be objectively

identified in the light of the client's activities, which by their nature may involve money laundering and (or) terrorist financing, the identification of the client and the ongoing monitoring of the client's actions.

All employees have a duty to report suspicious transactions. If an employee has any suspicion about a customer's behaviour or transaction, it must be reported to the Compliance Officer immediately. All employees are expected to report suspicious transactions to the Compliance Officer. For this purpose, employees use approved Internal Suspicious Activity Report Form.

The employee should still submit the report, even if their superiors are not in agreement. It will then be up to the MLCO to determine if the information available can be considered as sufficient for a STR to be made to the Commission.

The following information is included to an Internal SAR:

- The customers details
- The member of staff's statement about what gave them cause to make the report
- All relevant documentation and information

The MLCO will:

- acknowledge receipt of the report and review and investigate further as required
- make an assessment based upon all the information and decide whether the matter needs to be reported to law enforcement
- if it does, submit a STR to the Commission
- make a record and inform General management about the decision taken.

Once the MLCO has received an Internal SAR, she/he will decide if a STR should be submitted to the Commission.

When making this decision, the MLCO should consider that AML legislation is intended to address and attack serious crime which usually either involves amounts that are not minimal or circumstances that show an intent to circumvent and abuse the safeguards in place to deter the use of the financial system for criminal purposes.

For example, identity fraud and chargebacks may give rise to ML, but a licensee will only be subject to reporting obligations if they result in funds derived from these activities being deposited with or held by the licensee.

However, the Company won't report single instances involving small amounts but should consider whether it can detect a more significant pattern or scheme.

The MLCO considers whether an internal report gives rise to a suspicion of ML by taking into account all relevant information, including assessing whether there are common denominators between e.g., repeated suspicious behaviour, instances of chargebacks or identity fraud. For example, these may consist of common or related persons, common IP addresses etc.

When deciding whether to submit a Suspicious Activity Report (SAR), the MLCO must carefully consider and address several key questions to ensure a thorough and informed decision-making process. The MLCO should determine who is involved in the suspected activity and how they are connected to the potential criminal or terrorist property. It is essential to identify what the criminal or terrorist property entails, its estimated value, and where it is located. The timeline of events must also be assessed, including when the suspicious circumstances arose and any plans or indications of when they might occur in the future. Additionally, the MLCO should evaluate how these circumstances came about and articulate the specific reasons for their suspicion or knowledge of the activity in question. These considerations form the foundation of the MLCO's analysis and support the rationale behind submitting or withholding the SAR.

8. OTHER POSSIBLE RED FLAGS INDICATORS

Red flags are not intended to automatically result in the filing of a Suspicious Activity Report (SAR) with the Commission. Instead, they serve as indicators that should prompt the Company to question the customer's behaviour. If there is no reasonable explanation for the identified red flags, an internal report must be submitted to the AML Officer.

The following is a list of possible red flags which should be considered:

- The customer does not cooperate during the Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD) process.
- The customer attempts to register more than one account on a site.
- The customer makes small wagers despite depositing significant amounts, followed by a withdrawal request far exceeding any winnings.
- The customer makes frequent deposits and withdrawal requests without a reasonable explanation.

- There are noticeable changes in the customer's gaming patterns, such as transactions significantly larger in volume compared to their usual activity.
- The customer inquires about transferring funds between accounts within the same gaming group.
- The customer carries out transactions that appear disproportionate to their known wealth, income, or financial situation.
- The customer seeks to transfer funds to a bank account held in the name of a third party.
- The customer requests a withdrawal to an account that was not used for depositing funds.
- The customer opens an account, registers multiple cards, and transfers funds between them.
- The customer deposits large sums, places minimal bets, and then withdraws all funds.
- The customer deposits large amounts and repeatedly loses significant amounts as if the losses have no impact or consequence.

9. REPORTING PROCEDURE

The Company is required to submit a Suspicious Activity Report (SAR) to the Commission without undue delay if there are indications that:

- The Company knows, suspects, or has reasonable grounds to know or suspect money laundering and/or terrorist financing.
- An asset related to a business relationship or transaction originates from a criminal offense that constitutes a predicate offense to money laundering.
- A business case, transaction, or asset is connected to terrorist financing.

When determining whether it is necessary to submit a SAR, the Company considers the following factors, including but not limited to:

- The purpose and nature of the transaction.
- Any peculiarities in the customer's behaviour or profile.

- The financial and business background of the customer.
- The origin of the assets contributed or intended to be contributed.

Tipping-Off. It is an offense to inform anyone that a SAR has been submitted or is being considered for submission if doing so could prejudice an ongoing investigation. While internal discussions about the customer may occur within the Company, under no circumstances can the customer or their associates be informed that they may be under investigation.

This means that no one working for the Company:

- May inform the customer that a transaction is being delayed because a report is awaiting confirmation or consent from the Commission.
- May disclose to the customer that law enforcement is conducting an investigation.

9. INTERNAL CONTROL

The Company has a number of internal controls and general procedures which will be used on a day- to-day basis in respect of managing and running the daily operations of the business for the purpose of money laundering and terrorist financing prevention.

Employees background check

Prior to engaging employees, the Company will carry out relevant integrity checks, in-line with their position, responsibilities and access levels. The Company will not employ any persons who are not deemed to be fit and proper.

Once a person is employed, screening shall still be carried out on an ongoing basis as required. All Company's employees must guarantee that they observe the provisions of applicable legislation and the associated due diligence obligations, report facts relevant to money laundering, and do not themselves participate actively or passively in dubious transactions.

For this purpose, senior management will regularly carry out checks on employees or whenever the Company feels the need to perform such inspections. In particular, such inspections shall be carried out when suspicion arises concerning the behaviour of specific employees. The Company may carry out these checks through surprise spot checks or other procedures that will enable such personnel to verify whether employees comply with the policies and procedures.

The frequency and extent of screening that shall be carried out shall be proportionate to the risk level posed by the employee. The risk level will be determined case by case depending on employee's position (e.g., head of dept, senior, mid), the scope of duties and obligations, etc.

The Company will check all the employees at least once a year. The Company will use an employee performance sheet for this purpose.

The Company keeps all the documents and data collected or obtained within the scope of the due diligence, including:

- all data and information used to identify and verify customers (including type and number of the document, issuing authority, etc.)
- all records (receipts) relating to transactions, i.e., winnings paid out or refunds to customer accounts,
- all documents and records used for the preparation of the risk analysis, the risk analysis itself, including the results of the risk assessment, as well as the documentation on the appropriateness of the measures taken based on these results,
- the results of internal investigations, communication with the Commission and regulators,
- documents collected within the scope of business partners due diligence
- documents collected from the employees within the scope of the due diligence
- documents regarding AML trainings (training materials, examination results, etc.)

The Company also keeps all documents created and processed in connection with a suspicion of money laundering or terrorist financing, including:

- all related internal and external correspondence,
- file and interview notes,
- the results of internal investigations and the measures taken, that can explain why the money laundering officer concluded and initiated the actions taken.

The retention period is five years and starts with the end of the calendar year in which the business relationship ends and in all other cases with the end of the calendar year in which the respective information was ascertained. Applicable legislation may provide for a more extended retention period.

The Company destroys all the documents and data collected after retention period expiration unless other recordkeeping or retention obligations apply, but not later than after 5 years.

10. TRAINING

The Company will give training to all staff directly or indirectly through a service provider upon joining the Company and after that annually.

Relevant training materials will be prepared for all teams based on the company policies which have been compiled according to the applicable legislation requirements and guidelines.

Training will be conducted as follows:

- Training material based on the finalised and approved policies the Company has, in the form of documents and presentations.
- Training will be provided to existing management and staff in a class setting or online.
- Training will also be included in the induction of all new staff.
- Training will be followed up with a questionnaire to test everyone's understanding.
- Should the Company find that some issues are not clear we will repeat the training focusing on the issues that were not understood.
- Regular refresher training will be given, which will include any updates and will focus on any shortfalls that arose during the previous period.
- Any update in policy will be communicated in a group email and through ad- hoc training, and added to periodic training updates and material.

Staff training will focus on ensuring awareness of:

- all applicable legislation.

- the provisions of the money laundering and terrorist financing requirements
- staff personal obligations under the money laundering and terrorist financing requirements.
- applicable internal reporting procedures.
- Company's policies and procedures to prevent money laundering and the financing of terrorism.
- Company's identification and verification procedures, record-keeping, and other procedures to prevent money laundering and the financing of terrorism.
- recognition and handling of suspicious transactions.
- Staff personal liability for failure to report information or suspicions under the money laundering and terrorist financing requirements and the Company's internal procedures;
- New developments, including information on current techniques, methods, and trends in money laundering and the financing of terrorism.
- The money laundering and terrorist financing risks faced by the Company.

Induction training sessions will be conducted for all employees and will include fraud prevention, detection and ancillary matters, as required by their role. Refresher training will also be provided, both on a regular basis and as needed, so as to keep employees up to date and informed of the Company's policies and procedures and any changes or improvements made.

The MLRO keeps records of training delivered, showing what training has been provided, when and by whom, and the next training date. In case of any changes to the Company's policies and procedures or applicable legislation, all staff will get the relevant training.

Staff training will focus on ensuring awareness of:

- all applicable legislation,

- the provisions of the money laundering and terrorist financing requirements,
- staff personal obligations under the money laundering and terrorist financing requirements,
- applicable internal reporting procedures,
- Company's policies and procedures to prevent money laundering and the financing of terrorism,
- Company's identification and verification procedures, record-keeping, and other procedures to prevent money laundering and the financing of terrorism,
- recognition and handling of suspicious transactions,
- Staff personal liability for failure to report information or suspicions under the money laundering and terrorist financing requirements and the Company's internal procedures; and
- New developments, including information on current techniques, methods, and trends in money laundering and the financing of terrorism.
- The money laundering and terrorist financing risks faced by the Company
- Data protection regulations.

Induction training sessions will be conducted for all employees and will include fraud prevention, detection and ancillary matters, as required by their role. Refresher training will also be provided, both on a regular basis and as needed, so as to keep employees up to date and informed of the Company's policies and procedures and any changes or improvements made.

The MLCO keeps records of training delivered, showing what training has been provided, when and by whom, and the next training date. In case of any changes to the Company's policies and procedures or applicable legislation, all staff will get the relevant training.

Date: 02.05.2025

Approved by Virae Management B.V.

V. Demir

Veysel Demier, Managing Director

CERTIFICATE *of* SIGNATURE

REF. NUMBER

QRF6Q-5FLU8-VUAXV-VLTP8

DOCUMENT COMPLETED BY ALL PARTIES ON

02 MAY 2025 13:32:28 UTC

SIGNER

VIRAE MANAGEMENT B.V.

EMAIL

INFO@VIRAEMANAGEMENT.COM

TIMESTAMP

SENT

02 MAY 2025 13:32:27 UTC

SIGNED

02 MAY 2025 13:32:28 UTC

SIGNATURE

V. Demir

IP ADDRESS

161.22.55.35

