

Sort Services B.V.

**ANTI-MONEY LAUNDERING (AML) AND COUNTER TERRORIST
FINANCING POLICY**

Version:	3
Date of version:	20.11.2025
Created by:	Internal Compliance Committee
Confidentiality level	Internal

Change history

Version	Date	Author	Comment
1.0	10.01.2020	Internal Compliance Committee	
2.0	15.02.2024	Internal Compliance Committee	Amended
3.0	19.11.2025	Internal Compliance Committee	Amended

Table of Contents

1. AML/CFT Policy	7
2.Scope.....	8
3. Regulatory Framework.....	8
4. International regulations	9
5. Procedures	9
6. Risk Management.....	9
6.1 Risk assessment	9
6.3 Account Holder Risk	10
6.4 Product/Service/Transaction Risk	10
6.5 Interface risk.....	11
6.6 Geographical Risk	11
6.7 Risk Classification	12
7. Ethics Standards and Management of Conflicts of Interest.....	12
8. Know Your Customer Procedure.....	13
8.1 Standard Customer Due Diligence	13
8.2 Enhanced Due Dilligence	15
9. POLITICALLY EXPOSED PERSONS AND SANCTIONS SCREENING.....	19
10. Ongoing Monitoring	20
11. Unusual activities.....	21
12.Account Closure Procedure.....	22
13.Money Laundering Reporting Officer (MLRO).....	23
14.DEPOSIT AND WITHDRAWAL MANAGEMENT PROCEDURES	23
14.1 Player account balance	23
14.2 Payment methods.....	23
14.3 Player deposits.....	23
14.4 Player withdrawals.....	24
14.5 Cash Transactions	24

14.6 Transactions using Cryptocurrency	27
15. SUSPICIOUS TRANSACTION REPORTING	28
16. OTHER POSSIBLE RED FLAGS INDICATORS	30
17. REPORTING PROCEDURE.....	31
18. INTERNAL CONTROL.....	32
18.1 Employees background check.....	32
19 Training	34

Definitions and Abbreviations

Account Holder	An individual who has a Player Account on the Website.
AML	Anti Money Laundering. All efforts focused on the prevention of money laundering, the direct or indirect participation in any transaction that seeks to conceal or disguise the nature or origin of funds derived from illegal activities.
Combatting terrorist financing (CFT)	Combating the Financing of Terrorism. All efforts focused on the prevention of providing funds at the disposal of terrorists to be used for committing terrorist attacks.
Combatting proliferation of weapons of mass destruction (CPWMD)	Efforts focused on combatting the sale, transfer and export of nuclear, chemical or biological weapons and their means of delivery and related materials.
Cash transaction	The deposit and withdraw of fiat money into and out of a Player Account.
Cryptocurrency	Distributed, open-source, mathematically based peer-to-peer virtual currencies that have no central administering authority, and no central monitoring or oversight. Examples include Bitcoin, Ethereum, Litecoin and Dogecoin.
Cryptocurrency transaction	The deposit and withdraw of cryptocurrencies into and out of a Player Account held by a Player.
The Company	Sort Services B.V., a limited liability company duly organized under Curaçao law registered with the Chamber of Commerce and Industry in Curaçao under number 164182.
Employee	Any person working for the Company.
FATF	Financial Action Task Force (www.fatf-gafi.org)
FIU	Financial Intelligence Unit of Curaçao. Pursuant to FATF Recommendation no. 26, countries must establish a Financial Intelligence Unit (FIU) that serves as a national center for the receiving (and, as permitted, requesting), analysis and

	dissemination of suspicious transaction reports (STR) and other information regarding potential money laundering or terrorist financing.
KYC	Know Your Client, the mandatory process of identifying and verifying the client's identity when opening a Player Account and periodically over time.
License Holder	Sort Services B.V. a limited liability company duly organized under Curaçao law, registered with the Chamber of Commerce and Industry in Curaçao under number 164182
ML	Money Laundering: a process through which criminals conceal, or attempt to conceal, the origin of the proceeds of their illegal activities and disguise, or attempt to disguise, such proceeds to make them appear to be legitimate.
MLRO	Money Laundering Reporting Officer
Player	Individual who has registered with the Company for the purpose of making use of the Services offered on the Website and for which a Player Account has been opened providing him/her with a unique code.
Player Account	An account granted to an individual after registration on the Website. The Player Account is created and issued by the Company and is required for wagering with real money. Only one Player Account is permitted per person, per IP address, per family and per Shared Environment.
PEP	Politically Exposed Persons
Prohibited Jurisdictions	Jurisdictions prohibited under the Curaçao license conditions (Aruba, Belgium, Bonaire, Curacao, France, Netherlands, Saba, Statia, Sint Maarten, USA) as well as jurisdictions restricted by decision of the Company's managing director (amongst others Belgium and Singapore) and the Master License Holder (amongst others UK, Australia and Spain) when and where still applicable.

Shared Environment	An environment that has a common internet connection which includes but is not limited to airplanes, households, universities, libraries, cyber cafes, coffee shops and offices. Only one Player Account is permitted per Shared Environment.
Service	the gaming and betting offers provided by the internet gateway operated by the Company to the Account Holder, through the Website.
Terms and Conditions	The terms and conditions for the use of the Services, as published on the Website.
TF	Terrorist Financing: the process of making funds or other assets available to terrorist groups or individual terrorists to support them, even indirectly, in carrying out terrorist activities.
Trusted Third Party (TTP)	payment service provider with a physical presence, registered and approved by the Company to receive cash deposit by a Player or providing the cash withdrawn by the Player
Ultimate beneficial owner (UBO)	Natural persons who are the ultimate beneficiary who are the owner or having control of the Company due to having direct or indirect retention of 25% or more of stocks, or a comparable interest, or having 25% or more of the voting rights or a comparable position or hold 25 percent or more of the ownership interest in that company, including holding bearer shares or other assets
Website:	the online gaming platform offering online gaming services operated by the Company.

1. AML/CFT Policy

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 (hereinafter - preventive measures).

Money Laundering, Terrorism Financing and proliferation of weapons of mass destruction are some of the ever-growing threats for national and international economies throughout the world, forcing all vulnerable sectors to have measures in place for the prevention of their misuse for these purposes. Individuals involved in ML and/or TF continually attempt to exploit services and products to conceal their unlawful activities and proceeds' true nature. Illicit efforts by such individuals must be recognized and thwarted by all feasible means. AML policies incorporate regulations and laws for limiting financial criminals from concealing funds collected through illicit sources.

ML in the online gaming industry manifests itself in two opposing forms:

- a. the use of criminal funds to fund gambling activities; and
- b. the exchange of criminally acquired funds for legitimate money.

In both cases, authorities fear that those phenomena damage sports, the online gaming industry, and society as a whole. Therefore ML, when not eliminated, can have far-reaching implications.

TF may not involve the proceeds of criminal conduct but rather an attempt to conceal the origin or intended use of the funds, which will later be used for unlawful purposes. Terrorists regularly adapt how and where they raise and move funds and other assets in order to circumvent safeguards that jurisdictions have put in place to detect and disrupt this activity. Identifying, assessing and understanding TF risks is an essential part of dismantling and disrupting terrorist networks, as well as the effective implementation of the risk-based approach of CFT measures. PFWMD may involve the sale, transfer, export, of weapons of Mass destruction, like nuclear weapons and atomic weapons. Such proliferation must be countered as well due to it posing a signification threat to international peace and security, as identity by relevant United Nations Security Council Resolutions (UNSCRs). Therefore, the CP measures involve identifying and assessing the risks of potential breaches or evasion of the targeted financial sanctions to proliferation financing and taking appropriate mitigating measures with the level of risks identified.

The Company takes AML/CFT/CPF seriously and has policies in place to ensure compliance with the regulations in the jurisdictions where we operate. The Company's procedures and internal controls are designed to ensure compliance with all applicable national and international regulations and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in applicable law and changes in our business.

2.Scope

This Policy applies to all persons working for the Company or on the Company's behalf in any capacity, including Employees, directors, officers, agency workers, seconded workers, volunteers, interns, agents, contractors, external contractors, third-party representatives and business partners, sponsors, or any other person associated with the Company that falls within the scope of the Company's AML Policies.

This Policy defines procedures that will assist all persons working for the Company to comply with its legal obligations. Failure of an Employee to comply with the procedures defined within this Policy may lead to disciplinary action.

3. Regulatory Framework

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:

[L]
[SEP]

- 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; [L]
[SEP]
- 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; [L]
[SEP]
- 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 [L]
[SEP]Penalties and Administrative Fines for Service Providers) (N.G. 2010, no. 70); [L]
[SEP]
- 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.

4. 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.

5. Procedures

In an effort to be compliant with the applicable rules, regulations and international standards, the Company has procedures in place to which it attains itself when providing Services to Account Holders. These procedures cover the following standards:

- Risk management
- Know Your Customer Procedure
- Monitoring of Account Holder activities
- Reporting of unusual transactions
- Recordkeeping

6. Risk Management

6.1 Risk assessment

The possibility of online gaming being used by criminals to assist ML and/or TF poses many risks for the Company, such as criminal and regulatory sanctions and/or reputational damage for the Company and/or its Employees. For this purpose, the Company must carefully identify its risks and manage them accordingly.

The Company takes the following steps to manage its risks appropriately:

- i. identifying the ML and TF risks relevant to the Company.
- ii. assessing the level of risk;
- iii. understanding the impact of the risk;

- iv. designing and implementing appropriate policies, procedures and controls to manage and mitigate these risks;
- v. monitoring and improving the effective operation of these controls and identifying any weaknesses; and
- vi. recording what has been done and why.

In view of the above, the Company must conduct a risk assessment to analyse the risks faced by the Company and ensure that the identified risks are properly mitigated and resources adequately invested.

The risk assessment must identify and analyse the risks related to the following four key risk sources stemming from inherent vulnerabilities in the online gaming sector:

- i. Account Holders
- ii. Product / service / transactions
- iii. Interface
- iv. Geography

The Company must review its risk management processes on an on-going basis to ensure that it remains abreast of new risks. As a minimum, the risk assessment must be reviewed annually, or more frequently in the case of any important changes to products or technology, payment methods, customer type and other material changes.

The risk assessment will also analyse the policies, procedures and systems of the Company in order to ensure that the identified risks are properly mitigated through the adoption of robust policies and procedures. The results of the risk assessment will serve as the foundation to determine the Company's risk appetite. The following risk areas should be considered by the Company for the purpose of the risk assessment:

6.3 Account Holder Risk

The risk of ML/FT may vary in accordance with the type of Account Holder. The assessment of the risk posed by a natural person is generally based on the person's economic activity and/or source of wealth. An Account Holder having a single source of regular income will pose a lesser risk of ML/FT than a Account Holder who has multiple sources of income or irregular income streams.

6.4 Product/Service/Transaction Risk

Some products/services/transactions are inherently riskier than others and are therefore more attractive to criminals. These include products/services/transactions which are identified as being more vulnerable to criminal exploitation such as gaming products or services that allow the Account Holder to influence the outcome of a game, be it on his own or in collusion with others. The use of specific funding methods should also be treated as high risk factors. This includes cash and other similar or anonymous payment methods that may not leave or disrupt the audit trail and allow the Account Holder to operate with a degree of or complete anonymity such as pre-paid cards or virtual currencies. The exceptional use by an Account Holder of Player Accounts held or cards issued in the name of third parties is also to be regarded as a high-risk factor. Conversely, where an Account

Holder transfers funds from a bank account or a card linked to a bank account held in his name with an institution established in a reputable jurisdiction, the risk of ML decreases.

6.5 Interface risk

Channels through which a business relationship is established and/or through which transactions are carried out may also have a bearing 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 same. While situations where interaction with the Account Holder takes place on a non-face to face basis will no longer lead 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.

GAME TYPES					
	Low	Low-Medium	Medium	Medium-High	High
Fixed odds games without hedging (ex: slots, lotteries, bingo)	X				
Fixed odds games where hedging is possible (blackjack, baccarat, roulette)			X		
Sportsbetting			X		
P2P games (ex: poker, betting exchange)					X

FUNDING METHODS					
	Low	Low-Medium	Medium	Medium-High	High
Bank transfers (EEA or equivalent safeguards)	X				
Debit/credit cards issued by banks (EEA or equivalent safeguards)	X				
Debit/credit cards issued by other licensed financial institutions		X			
EEA-licensed payment service providers			X		
Non-EEA licensed PSP				X	
EEA-licensed PSP that can be funded with cash or quasi-cash				X	
Prepaid cards/vouchers					X
Cash					X

6.6 Geographical Risk

The geographical risk is the risk posed to the licensee by the geographical location of the business/economic activity and the source of wealth/funds of the business relationship. The nationality, residence and place of birth of a Account Holder have to be taken into account as these might be indicative of a heightened geographical risk. Countries that have a weak AML/CFT system, countries known to suffer from a significant level of corruption, countries subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction as well as countries which are known to have terrorist organizations operating within are to be considered as high risk. The opposite is also true and may therefore be considered as presenting a medium or low risk of ML/FT.

In order to identify and manage potential hazards, the high-risk territories are the next:

- i. Prohibited Jurisdictions: these jurisdictions are prohibited under the Curaçao license conditions and/ or pursuant to a resolution of the Company's managing director;
- ii. jurisdictions which are identified by FATF as high-risk jurisdictions subject to a call for action;
- iii. jurisdictions under increased monitoring by FATF;
- iv. countries which are identified by the European Union as high-risk countries;
- v. countries which are identified by the United States as state sponsors of terrorism.

6.7 Risk Classification

Upon registration, the Company makes a risk classification for each Account Holder.

The Company maintains the following risk classification:

- Low risk
- Medium risk
- High risk

The level of due diligence that should be performed on the Account Holder is determined based on the risk classification above.

Type of Account Holder	Monitoring frequency
Account Holders who are under active investigation or suspected in ML/TF or other fraudulent activity and their accounts are not limited for deposit or logins	Daily
PEPs, which are deemed to present a high risk	Daily
High-Risk Account Holders, High-Rollers, PEPs with lower relative risk and active Account Holders from high-risk jurisdictions	Weekly (or upon a material change)
Medium Risk Account Holders	Every six months (or upon a material change)
Low Risk Account Holders	Annually (or upon a material change)

7. 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 his duties or performing an order, must make a

decision, participate in its acceptance or execute an order that is related to his and (or) his 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 FIU, etc.

An employee of the Company who is involved in a potential conflict of interest situation must immediately inform his 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 himself.

8. Know Your Customer Procedure

An individual cannot make use of the Services unless that individual is over eighteen (18) years of age or any legal age at which gambling or gaming activities are permitted under the law or jurisdiction applicable to his person and has successfully registered for a Player Account. To register for a Player Account, an applicant must register personally and provide the following information:

- a. First and last name;
- b. Date of birth;
- c. Gender;
- d. ID card number;
- e. Full residential address;
- f. Telephone number;
- g. Valid email address and
- h. Username and a password.

The name on the account must match the true, legal name and identity of the individual. The username, password and other personal information related to the account must be kept secret and confidential and may not be used by any third party. In case of a suspected violation, an Account Holder must request new log-in credentials.

8.1 Standard Customer Due Diligence

The Company applies general (standard) customer due diligence (hereinafter – CDD) measures to the customers at the registration stage. The CDD process consists of:

identification – establishing identity by collecting information from the customer.

verification – proving a customer is who they claim to be by obtaining and validating documents or information which supports this claim of identity, which come from a reliable and independent source.

According to the above requirements, The Company collects the following information for identification and verification to prevent money laundering and terrorist financing: (a) first name(s); (b) last name(s); (c) date of birth; address (street, no., ZIP code, city); (d) phone number.

Standard Due Diligence is conducted in the following cases:

anytime during the Player onboarding;

upon a request for withdrawal; and

anytime at the discretion of the Company. When a transaction or incidental transaction of Nafl 4000,-(€ 2000,-) or more takes place.

All applicants are required to submit proof of identity, proof of address and payment ID at moment of deposit of funds or where applicable at any given time requested by the Company. Account holders are required to submit satisfactory documentation to proof the identity and residential address including but not limited to copies of:

valid passport;

identify card;

driving license; and/or

recent utility bill not older than three months.

Depending on the method used for the verification of the authenticity of the documentation, the documents are not required to be certified prior to the provision thereof. Further specifications in relation to the method of verification are to be detailed in separate complementary instruments to this document.

In case the Company discovers that a transaction in the course of the business relationship of an amount of Nafl 4000,- (€ 2000,-) or more takes place, then the Company must perform verification of the Account holder's identity prior to accepting more transactions of the Account holder taking place.

“Transaction” consists of the wagering of a stake, including:

- the deposit of funds required to take part in remote gambling
- the collection of winnings, including
 - the withdrawal of funds deposited to take part in remote gambling or
 - winnings arising from the staking of such funds

The transactions are considered linked if they are part of the overall activity undertaken by a customer during a single period of being logged on to the operator's gambling facilities. However, this example is not exhaustive, and the Company considers other circumstances in which transactions are linked using a risk-based approach.

The Company has geo-blocking measures in place that restrict residents of Prohibited Jurisdictions access to the Website.

The Company will proceed to review the information provided within a reasonable time and will contact the applicant and request further information in case the documentation provided is found to be unsatisfactory. A document may be considered unsatisfactory if it is not in English, is suspected to be fraudulent, is suspected to be obtained from a third party to perform illegal operations over the Internet, or for any other reason subject to the discretion of the Company. The applicant may be required to provide further information or information in the internationally accepted format, including but not limited to requesting official translation of legal documents with appropriate seals. If the applicant does not succeed in providing sufficient information, refuses to do so or provides documentation not meeting the criteria (e.g. forged, altered, failing security checks), the Company may immediately proceed to permanently close the Player Account without the refund of the deposited amount.

8.2 Enhanced Due Dilligence

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

EDD is applied 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 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.

In cases where there is a higher risk, establishment of the business relationship or continuation of the business relationship (if the higher risk only arose later or was only recognised later) only with the consent of the MLRO.

If a customer has been deemed to be a high-risk or becomes one at any stage, the Company undertakes the EDD, comprising of (depending on the case):

- undertaking Re-verification of identity (repeated CDD).
- Establishing how the customer acquired his wealth to be satisfied that it is legitimate:
 - salary income or company profit (Payslip / employer letter / audited accounts/ tax declaration if self-employed) ○ sale or liquidation of financial instruments (Certified shares/investments sale contracts or statements/ accountant letter)
 - sale of property (Certified copy of the contract of sale or letter from a solicitor or estate agent) ○ inheritance (Certified copy of will including the value of heritage)
 - sale of the company (Certified contracts, media articles, certified letter from accountant or solicitor).
- Establishing the source of the customer's funds to be satisfied that they do not constitute the proceeds from crime.

- Checking verifying the disclosed details against certain (public or private) databases (e.g. sanction lists)
- 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 behavior 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).
- Requesting credit report

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.

** The Source of Funds refers to the origin of the particular funds being used to deposit on the Company's website. This is not simply verifying which bank or financial institution the customer may have received the funds from. The information obtained should be substantive, relevant and establish the fund's origin and the method/circumstances under which the funds were acquired.*

*** The Source of Wealth refers to the origin of the entire body of wealth (i.e. total assets) of the client. The information that the Company obtains should indicate the volume of wealth the client would reasonably be expected to have and provide a picture of how it was acquired.*

The Company reserves the right to restrict the Account Holder from withdrawing funds from the account and/or prevent access to all or certain parts of the services. Failure to pass the checks may result in permanent closure of the Player Account and suspension of any of the outstanding balance.

9. POLITICALLY EXPOSED PERSONS AND SANCTIONS SCREENING

The Company uses KYC software tool to check all new customers at the registration stage against the PEP and Sanctions databases. The Company also regularly check the whole customer database every six months to ensure existing customers have not changed status.

Screening for PEP status has to be carried out regularly but it is important that this is done within thirty days of the threshold being met. Any new or existing customer found on the Sanctions database, or a PEP or relative of such will have their account rejected or closed.

In case of identifying a PEP, responsible staff will send a report to Compliance Officer who in turn will send a report to the senior management.

The Compliance Officer will investigate each case to identify positive or false-positive PEP alert. The Company has a right to request additional documents from the customer for this purpose within the investigation.

If the PEP alert is true-positive, the responsible AML Officer will reject registration or close the account and informed the senior management about the decision taken. Should an Account Holder who had not been identified as a PEP at on-boarding stage result to have become one, the Employee is required to carry out or implement the measures described above, failing which it would have to terminate the business relationship with the said Account Holder.

Politically Exposed Person means any person who has been entrusted with a high- ranking prominent public function at the international, European, or national level or who is or has been entrusted with a public position of comparable political importance below the national level. In particular, politically exposed persons are:

- heads of state, heads of government, ministers, members of the European Commission, deputy ministers and assistant ministers,
- members of parliament and members of similar legislative organs,
- members of the governing bodies of political parties,
- members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are usually not subject to further appeal,
- members of the boards of courts of audit,
- members of the boards of central banks,

- ambassadors, chargés d'affaires and defence attachés,
- members of the administrative, management or supervisory bodies of state- owned enterprises,
- directors, deputy directors, members of the board or other managers with a comparable function in an international or European intergovernmental organisation.

Family member of PEP means a close relative, in particular:

- the spouse or civil partner,
- a child and the child's spouse or civil partner and
- both parents.

FATF blacklisted/grey-listed countries are blocked on the company's sites, and individuals from these countries are not able to register or login from these countries. The list of FATF blacklist/grey-listed countries may be found here - [https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc\(fatf_releasedate\)](https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)).

Information required to determine whether a Account Holder (or its beneficial owner) is a PEP can be obtained either from the Account Holder himself (e.g. by completing a standardized self-declaration as to his status and, to the extent which may be applicable, that of his beneficial owner) or by using reliable electronic databases to screen their Account Holder database. However, where the Employee relies on the Account Holder to disclose and declare whether he is a PEP or otherwise, he is required to (a) provide the Account Holder with guidance as to what is meant by a PEP, including by providing him with a definition of the said term; and (b) confirm on a risk sensitive basis the information so obtained.

10. Ongoing Monitoring

The Company reserves the right to conduct a review at any time to validate the identity, age and/or registration data provided by the Account Holder in order to verify the use by the Customer of the provided services for any breach of the Terms and Conditions and any applicable laws.

The general due diligence duties include the ongoing monitoring of the business relationship. This includes:

- obtaining fresh identification when existing documents have expired. (This can be done on a risk-sensitive basis.)

- questioning the data and information the Company have have whenever inconsistencies are noticed.
- general review and update from time to time, on a risk sensitive basis.
- checking if transactions match with the documents and information available at the Company about the customer and the origin, customer's assets
- updating the respective documents, data, or information at appropriate intervals.

To keep all the customers information up to date, the Company apply CDD procedure every 6 months from the date of the successful complete verification of each customer and on a risk-sensitive basis. During the review the Account Holder may be restricted from withdrawing funds from the Player Account and/ or prevented from accessing certain Services offered on the Website.

The Company takes reasonable steps to prevent activities of money laundering and terrorism financing and constantly monitors all Player activities including financial habits and behavior in order to mitigate industry related risks such as money laundering, terrorism financing and other criminal activities such as fraud.

11. Unusual activities

The Company has systems in place to monitor the activities on the Player Accounts for the presence of any unusual or suspicious. These activities include but are not limited to:

Duplicate or multiple Player Accounts

Any Player Accounts containing the same personal information, IP address or bank account is considered to be a duplicate account. It is not permitted for an Account Holder to have duplicate Player Accounts or manage more than one (1) Player Account when using the Services on the Website including but not limited to the web-based version. If the Company becomes aware, suspects or believes that this might be the case it reserves the right to immediately terminate any and all Player Accounts held and the Player Account balances either deemed as forfeited by the Account Holder in which event the deposit will be subject to further investigation by the Company. Any winnings arising from such behavior will be forfeited.

Collusion

Upon the suspicion of the multiple registration by Account holders acting in collusion or as a syndicate, the setup of fictitious Player Accounts or the use of front men, the Company reserves the right to change or terminate any bonus offer, cancel any winnings and close Player Accounts.

Identity fraud

At the detection of any use of falsified documentation (identity fraud), the Company will proceed to close the Player Account(s). Any winnings arising from such activities shall be confiscated and the amount deposited will be subject to further investigation.

12.Account Closure Procedure

Among the situations described above, There are numerous reasons for why the Company will want to close a customer's account:

- Fraud
- Cheating
- Bonus Abuse
- Allowing a third person to use their account
- Under-aged gambling
- Problem gambler
- Being abusive to staff
- Commercial concerns
- CDD failure
- Terms and Conditions breach

The concern of this Company Policy is the reason that there is a suspicion or knowledge that the customer is involved in ML/FT. By law the Company must end the business relationship with the customer unless we have obtained appropriate consent for it to continue and even then, it is precautionary to close the account. Due to the laws on Tipping Off the Company cannot inform the customer that we have concerns regarding ML/FT, thus account closure must be done sensitively.

The MLRO will need to consider whether if an SAR was submitted as part of the concern about the player's behaviors whether appropriate consent should have been requested. Where the Company is unable to complete or apply the required CDD measures in relation to a particular customer at the point the CDD threshold for transactions is reached and is accordingly required to cease transactions and terminate the business relationship with the customer.

13. Money Laundering Reporting Officer (MLRO)

The Company has designated an MLRO who is in charge of the review of KYC information and the monitoring of Player Account activities and is further assisted by designated personnel. The MLRO is in charge of the following:

- viii. ensure a proper review of the Player Accounts by the personnel in relation to identification and verification of an Account Holder;
- ix. keep a list of registered Account Holders;
- x. monitor the reviews and investigations conducted by the designated personnel performed on the Player Account activities;
- xi. provide initial and ongoing training to all relevant staff ensuring awareness of their personal responsibilities and the procedures in respect of identifying Players, monitoring Player activity, record-keeping and reporting any unusual/suspicious transactions;
- xii. cooperate with all relevant administrative, enforcement and judicial authorities in their endeavor to prevent and detect criminal activity; and
- xiii. ensure that this policy is adhered to, reviewed and maintained regularly.

14. DEPOSIT AND WITHDRAWAL MANAGEMENT PROCEDURES

14.1 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.

14.2 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.

14.3 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. A player may deposit money in his Player Account only in order to play on the Website and use the Services and is not allowed to withdraw without prior wagering activity. Furthermore, the Company will not grant interest on deposits. The Company reserves the right to apply certain restrictions to the payment methods in selected countries and/or for certain Players.

14.4 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.

An Account Holder can only make a withdrawal request once the initial deposit amount is fully used, and specific bonus terms of a bonus must be satisfied before requesting its withdrawal.

No withdrawal will be processed, and funds cannot be withdrawn from the Player's Player Account until: (i) the required verification checks have been satisfactorily completed; (ii) payments have been confirmed; and (iii) the Player has complied with any other withdrawal conditions, specific rules and promotional terms relating to the Player's use of the Website and/or affecting his/her Player Account (for example, any applicable bonus terms), and (iv) wagering activity has been conducted by the Player in the minimum amount of EUR 2000.

Withdrawal requests can only be addressed to the Account Holder registered on the Player Account and only to the account from which deposits were made. The information provided on the withdrawal form must be identical to the personal data held by the Company. Withdrawal requests made to other parties will not be taken into consideration.

14.5 Cash Transactions

Cash transactions can only be made at those locations which are registered with the Company. In order for a company to be registered as a Trusted Third Party the applying company will need to provide the Company with:

- its trade- and official name,
- the Articles of incorporation,
- excerpt from the Chamber of Commerce
- register of shareholders,
- register of directors,
- last financial statements and
- KYC on the owners (shareholders) and directors (PP, proof of registered address, proof of no criminal record).

- Furthermore, the applying company must commit itself to provide the Company with a monthly record of deposited and withdrawn amounts mentioning the corresponding name of the Player, Player Accounts (username), date and time of the transaction and the amount transferred.

The applying company together with its related individuals will be submitted through a thorough background check by the Company. Upon acceptance, the applying company will be registered as a Trusted Third Party, able to receive cash deposits from Account Holders to be deposited on the Player Account and to pay out requested cash withdrawals from the Player Account to the player.

Cash payment restrictions

Although the Trusted Third-Party payment options are convenient and relatively fast for the Player, certain requirements (AML/CFT) need to be in place to ensure that this payment option is not misused. The following restrictions should be noted:

Cash deposit

- Player needs to have registered for a Player Account on the Website and at the TTP;
- Cash payments can only be made in person at designated TTPs;
- Player will need to verify his identity and account information before making transactions;
- For first deposits, a maximum deposit of EUR 2.500 can be made;
- Funds are available in the Player Account instantly;
- A limit for subsequent deposits is in place (up to EUR 10.000).

Cash withdrawal

- Player will need to verify his identity and account information whenever requesting a withdrawal;
- For first withdrawals, a withdrawal limit on the first withdrawal of EUR 2.500 is imposed. A withdrawal limit is in place (up to EUR 10.000) for any subsequent withdrawal;
- Upon the request for withdrawal, the Company will review the Player Account for any irregular activity such as money laundering or suspicious play (e.g. repetitive deposits with little to no wagering followed by a request for withdrawal). If the suspicion is found to be grounded, the Company reserves the right to withhold funds and will proceed to report to the FIU;
- Cash withdrawals will only be paid out to the Player who has identified himself personally through the provision of a valid ID. The TTP will verify the identification information in accordance with its own records.

All further AML & CFT processes applied by the Company are in place. These efforts include but are not limited to:

- The requirement to play through the deposited amount in order to be able to request a withdrawal
- No funds, rewards, credits or bonuses can be transferred nor paid out to third parties

- The monitoring of Player Account activities for irregularities such as:
 - repetitive deposits with little to no wagering, followed by a request for withdrawal
 - the creation of multiple accounts
 - acting in collusion with other Players
 - attempt to commit a fraudulent act
 - Filing reports to the FIU of detected irregularities or suspicions of Money Laundering, Terrorism financing or other fraudulent activities.

Cash Transaction procedures

The following procedures need to be followed by the Player when making a cash deposit or withdrawal.

Deposit

First deposit:

1. Player visits the TTP personally
2. Player provides the cashier at the TTP with the following:
 - a. a valid photo ID,
 - b. Player Account details
 - c. The cash to be deposited onto his Player Account (maximum of EUR 2.500)
3. The cashier proceeds to validate the Player Account information on the Website. Upon successful validation, the cashier proceeds to make the deposit to the Player Account on the Website. The funds will be immediately available in the Player Account.
4. The cashier creates an account at the TTP and registers the deposit mentioning the Name of the Player, the date and time of deposit and the deposited amount.

Subsequent deposits:

1. Player visits the TTP personally
2. Player provides the cashier at the TTP with the following:
 - a. a valid photo ID,
 - b. Player Account details
 - c. The cash to be deposited onto his account (maximum of EUR 10.000)
3. The cashier proceeds to validate the account information on the Website. Upon successful validation, the cashier proceeds to make the deposit to the Player Account on the Website. The funds will be immediately available in the Player Account.
4. The cashier registers the deposit mentioning the Name of the Player, the date and time of deposit and the deposited amount.

Withdrawal

1. Player logs in to the online Player Account and submits the request for withdrawal as per the method indicated on the Website. Player specifically chooses the “Cash at TTP” option,
2. The Website will proceed to conduct its review of the Player Account and will provide the Player with confirmation for the withdrawal request within 24 hours in case no irregularities are found.

3. Cash withdrawals are immediately available at the TTP once the Player receives confirmation from the Website that the funds are available for pickup.
4. For the first withdrawals, a withdrawal limit of EUR 2.500 is imposed. For subsequent withdrawals the limit is set to EUR 10.000 per withdrawal per month (in case Player requests the withdrawal of over EUR 10.000 the Company will reserve the right to payout the requested withdrawal in arrears at the end of each subsequent month).
5. Players must visit the TTP in person. Payouts will only be made to the Player.
6. Player provides the cashier at the TTP with the following:
 - a. a valid photo ID,
 - b. Player Account details
 - c. Withdrawal confirmation as provided on the Website
7. The cashier will verify the ID and the Player Account information
8. Upon successful verification the cashier requests the Player to sign off for receipt of the cash and will provide the Player with the Cash.
9. The cashier registers the cash out mentioning the name of the Player, the date and time of transaction and the amount paid out.

14.6 Transactions using Cryptocurrency

Cryptocurrency transactions are only possible if the initial deposit was made with a crypto currency. Following this transaction all transactions (deposits, wagers and payout) with the Player must be conducted using the same crypto currency as with the first deposit.

The Company will at no time sell/buy/exchange crypto currency with and/or to FIAT currency.

The Company is bound by the following requirements as set by the Master License Holder:

- Collect and verify proof of identity and proof of address as described above in the 'Client Due Diligence' paragraph and to make sure that the Player is over 18 years of age;
- Collection and storage of hardware KYC in all pathways from signup, login, deposits and withdrawals, including but not limited to IP address, mac address and browser information to ensure that all wagering, deposits and withdrawals are to/from the same Player (IP and computer);
- The Company will make available to the Master License holder on demand and provide proof of balance as acceptable by the Master License Holder, to ensure Player's funds have been deposited;
- Provide proof of Solvency to the Master License Holder on a periodic basis (weekly, monthly) to ensure that operator has all funds to cover all bets and jackpots, and that the crypto currency is kept in a separate account.
- The Company will display the rate of exchange from crypto currencies to FIAT currency on the home page of the Website. In no way shall the Company make exchanges between any crypto currency and any FIAT currency.
- The Company must include in their Terms and Conditions and highlight that crypto currency values can change dramatically depending on the market value.

It is important to note that due to the current anti-money-laundering regulations, the Player may deposit money into the Player Account only in order to play and to use the Services. Likewise, the

Player may only withdraw winnings and not the funds deposited into the Player Account. Players who deposit and withdraw without gaming activities will have their funds blocked until further notice. The Company is not a financial institution and does not grant interest on deposits. In any case, the Company reserves the unlimited right to apply certain restrictions to the payment methods in selected countries and/or for certain Players.

Notification of new payment methods will be made on the homepage of the Website and sent by e-mail to the Account Holders as they are added. For each new depositing method, this Manual and the Terms and Conditions on the Website will be updated accordingly.

15. 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 Financial Intelligence Analysis Unit (hereinafter – FIU).

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 FIU of Curacao.

The MLRO 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 MLRO 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 FIU 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 FIU. 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, FIU 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 FIU. 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 behavior 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 MLRO to determine if the information available can be considered as sufficient for a STR to be made to the FIU.

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 MLRO 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 FIU
- make a record and inform General management about the decision taken.

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

When making this decision, the MLRO 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 MLRO 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.

The MLRO, in deciding to submit the SAR or not, should answer the following questions:

Who is involved?

- How are they involved?
- What is the criminal/terrorist property?
- What is the value of the criminal/terrorist property (estimated as necessary)?
- Where is the criminal/terrorist property?
- When did the circumstances arise?
- When are the circumstances planned to happen?
- How did the circumstances arise?
- Why you are suspicious or have knowledge.

16. OTHER POSSIBLE RED FLAGS INDICATORS

Red flags are not intended to automatically result in filing a SAR with the FIU, however are merely indicators that should lead the Company to question the customer's behaviour. If there is no reasonable explanation for the red flags, then an internal report must be by the AML Officer.

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

- Customer does not cooperate in the carrying out of CDD/EDD.
- Customer attempts to register more than one account on a site.
- Customer makes small wagers, even though the amounts deposited are significant, followed by a request to withdraw well in excess of any winnings.

- Customer makes frequent deposits and withdrawal requests without any reasonable explanation.
- Noticeable changes in the gaming patterns of a customer, such as when the customer carries out transactions that are significantly larger in volume when compared to the transactions he normally carries out.
- Customer enquires about the possibility of moving funds between accounts belonging to the same gaming group.
- Customer carries out transactions which seem to be disproportionate when seen in the context of what is known about the Customer's wealth, income or financial situation.
- Customer seeks to transfer funds to a bank account held in the name of a third party.
- Customer requests a withdrawal to an account he never deposited with.
- Customer opening an account and registering several different cards and making transfers between them.
- Customer depositing large sums, then places minimal bets, then withdrawing all their funds.
- Customer depositing large amounts and repeatedly losing large amounts as if the loss is of no consequence.

17. REPORTING PROCEDURE

The Company is obliged to submit a suspicious activity report to the FIU, through the user interfaces on the FIU's website or by mail (if possible), without due delay if there are indications that:

- the Company know, suspect, or has reasonable grounds for knowing or suspecting money laundering and/or terrorist financing,
- an asset related to a business relationship or transaction originates from a criminal offence that could constitute a predicate offence to money laundering,
- a business case, transaction, or asset is related to terrorist financing.

When the Company decides whether it is necessary to submit STR, it takes the following factors into account, including but not limited to:

- the purpose and nature of the transaction,
- peculiarities in the customer,
- the financial and business background of the customer,
- the origin of the assets contributed or to be contributed.

Tipping-off. It is an offence to tell anyone that a STR has been submitted or is being considered to be submitted and that this is likely to prejudice the investigation. This means it is possible to have an internal discussion about the customer, but in no way can the customer or their associates be given any indication that the customer may be under investigation.

This means that no one working for the Company:

- can, at the time, tell a customer that a transaction is being delayed because a report is awaiting confirmation (consent) from the FIU;
- can tell the customer that law enforcement is conducting an investigation.

18. 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.

18.1 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 FIU 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 10 years.

19 Training

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.

The Company's internal control system for the prevention of money laundering and terrorist financing (hereinafter - 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.

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

Decision-making level:

- . CEO (General manager);
- MLRO and Head of Risk and Payments;

Operational level:

- risk and payments specialists;
- AML officers;

Auxiliary level:

- Legal Counsel
- Chief financier and financiers

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 Reporting 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 Reporting 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.

Training for the Company's employees is organized at the frequency indicated in the which covers the following topics:

- legislation related to the prevention of money laundering and terrorist financing, their amendments;
- customer identification methods and requirements;
- identification of suspicious customer actions and monetary transactions, deepening of knowledge in this field;
- verification of customer information;
- monitoring customer actions and operations;
- the procedure and deadlines for submitting information to the FIU;

Storage of information.

This training specified is organized with the following frequency:

- For decision-making level employees - at least 2 times per calendar year;
- For operational level employees - at least 2 times per calendar year;
- For employees of the auxiliary level, intermediaries and third parties to whom the Company has delegated certain functions - at least once per calendar year;
- For employees of all levels - no later than within 20 calendar days from the amendment of the legislation regulating the prevention of money laundering and terrorist financing (if the amendments relate to the functions performed by these employees).

The content of the training specified in the Description 3.7 paragraph must be proportional to the level of the control system and ensure that:

- the employee is aware of the requirements of legal acts that affect (regulate) his functions in the field of preventive measures;
- the employee is aware of good practice in the field of preventive measures taken by him;
- the employee knows the control system implemented in the Company;
- the employee knows his functions, competence limits, information provision rules.

After each training, an employee knowledge test is performed to determine how the employees understood and assimilated the training information (in individual cases, it may be checked how the employees will apply the training knowledge in their activities).

The Company maintains a training log, which indicates the date of training, training topics, names of employees who have completed the training, and other related information. Employees shall confirm their participation in the training by signature or other prescribed means in an electronic system. Data on the organized trainings and the employees who participated in them, the results of the knowledge test, the content of the training material, etc. stored for at least 5 years from the end of the 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 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.

20.Recordkeeping

The Company maintains a record of all relevant documentation on a separate database for at least five years after ending a business relationship. The Company is obliged to retain files in a way that enables

investigating authorities to identify a satisfactory audit trail for individual transactions including the amounts, currencies and type of transactions.

In specific circumstances, if ordered by rule of law and permitted by national law and the relevant authorities, the Company may provide copies of the records maintained.

21. Periodical review of AML/CFT policies

The AML/CFT policies of the Company are subject to a yearly review, comprising of a fair and unbiased appraisal of each of the required elements of this policy. The review includes testing of internal controls and transactional systems and procedures to identify problems and weaknesses. The review may be conducted by an Employee or group of Employees, so long as the reviewer is not the MLRO and does not report directly to the MLRO.

Addendum

Risk score calculation

The purpose of this procedure is to pick up minor incidents of ML/FT behaviour that by themselves may not warrant suspicion but, if combined with other behaviours, can do so. A player will be scored by the internal CMS system according to part of the factors above, and a risk score will be assigned. Each factor will generate a score, and the overall risk score will be a sum of the individual scores. The more negative the score, the higher the risk. Note that these factors, the scores and the thresholds are internal, and will be adjusted as we improve and update the RS Calculation.

Indicator	Description	Score
individual status		
PEP	A customer considered to be PEP	100
Adverse media	A customer was mentioned in negative news or information the company discovered from various sources	50
Sanctions/blacklist	A customer is under international sanctions/blacklists	50
geographical location		
Not at home	A customer whose IP location is different from their registered address	20
High-risk country resident	A customer resides in a High-risk country	30
gambling behaviour		
Large sums no play	A customer depositing large sums, then places minimal stake bets, then withdrawing all their funds	50

Large sums big losses	A customer depositing large amounts and repeatedly losing large amounts as if the loss is of no consequence (EUR 5000 per week)	50
Low odds betting	A customer repeatedly placing short odds (such as red/black on roulette or repetitive betting on favourites) bets	25
Big changes in money	Dramatic changes in terms of volume and size of player deposits or staking activity	20
Several gaming accounts	A customer is trying to register several gaming accounts	30
transactional behaviour		
Smurfing	A customer making multiple deposits or withdrawals of small amounts without no objective reasons	30
Spending above wages	A customers spend is outside of their affordability	20
No withdrawals	Player has never requested a withdrawal	-20
Withdrawal without playing	Money is deposited by a customer or held over a period and withdrawn by the customer without being used for gambling	30
payment methods the player is using		
Card switching	A customer opening an account and registering several different cards and making transfers between them	20
High risk payment methods	A customer uses high-risk payment methods	30
fraud red flags a customer triggered		
VPN	Customer used a VPN	30

Once the score is calculated, a risk level is assigned:

CMM Score	Risk Category

0-20	Low
21 - 40	Medium
41 - and higher	High

Not all factors can be automatically included in the CRA calculation due to technical or practical reasons, but we do monitor for these risks in other ways. For example, we check for VPN usage or multi-accounting at the point of registration, we have a separate alert for players who use cards under a different name, and all withdrawals are checked before approval and payment. The level of customer due diligence (CDD) conducted on a player will depend on the risk score assigned to the player as follows:

	Low	Med	High
Verify ID and address with docs		X	X
Collect additional personal details	X	X	X
Collect Source of Funds/ Wealth info		X	X (with documentation)
Ongoing monitoring	X	X	X (Enhanced)
Additional measures to address any other risk identified			X
Report suspected cases of ML/FT	X	X	X

V. Demir

Virae Management B.V.

Managing Director

20-11-2025

CERTIFICATE *of* SIGNATURE

REF. NUMBER
JS6SE-RPW5X-YHQKZ-WBSM8

DOCUMENT COMPLETED BY ALL PARTIES ON
20 NOV 2025 23:46:49
UTC

SIGNER

VIRAE MANAGEMENT B.V.

EMAIL
INFO@VIRAEMANAGEMENT.COM

TIMESTAMP

SENT
20 NOV 2025 23:46:48

SIGNED
20 NOV 2025 23:46:49

SIGNATURE

V. Demir

IP ADDRESS
161.22.55.35

LOCATION
WILLEMSTAD, CURAÇAO

