Intelligent Innovations N.V.

AML Policy

Version 4.0.

Change history

Date of effectiveness	Version	Author	Summary	Approving Official	Responsible Officer
May 2020		Intelligent Innovations N.V.	Initial version	eMoore N.V.	Compliance function
February 2021		Intelligent Innovations N.V.	Updated version	eMoore N.V.	Compliance function
01.05.2023	1.0	Intelligent Innovations N.V.	New version	eMoore N.V.	Compliance function
03.05.2024	2.0	Intelligent Innovations N.V.	New version	eMoore N.V.	Compliance function
15.01.2025	3.0	Intelligent Innovations N.V.	New version	eMoore N.V.	Compliance function
15.05.2025	4.0	Intelligent Innovations N.V.	Updated version	eMoore N.V.	Compliance Officer

Next Review Date: 15.05.2026

For any questions regarding this policy, please contact:

eMoore N.V.
Legalcompliance Department
Groot Kwartierweg 10, Livestrong Building
Willemstad, Curaçao
Telephone: +599 9 7471401
Email: legalcompliance@the-emgroup.com

Definitions and Abbreviations

Account Holder	An individual who has a Player Account on the Website.
Anti-Money Laundering (“AML”)	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.
Caribbean Financial Action Task Force (“CFATF”)	An organization of states and territories of the Caribbean region that have agreed to implement common countermeasures against money laundering and terrorism financing. (www.cfatf-gafic.org)
Combatting terrorist financing (“CFT”)	All actions focused on detection, prevention, and disrupting the flow of funds to individuals or groups engaged in terrorist activities.
Combatting proliferation of weapons of mass destruction (“CPWMD”)	Efforts aimed at combatting the financing or provision of funds for the sale, transfer, or export of nuclear, chemical or biological weapons, their delivery systems and related materials.
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	Intelligent Innovations N.V., a limited liability company duly organized under the laws of Curaçao with the company number 142065, registered with the Chamber of Commerce and Industry in Curaçao.
Employee	Any person working for the Company.
Financial Action Task Force (“FATF”)	An intergovernmental organization dedicated to developing standards and promoting effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. (www.fatf-gafi.org)
Financial Intelligence Unit (“FIU”)	Pursuant to FATF Recommendation no. 26, countries must establish a Financial Intelligence Unit (FIU) that serves as a national center for the receipt (and, where permitted, the request), analysis and dissemination of suspicious transaction reports (STRs) and other information regarding potential money laundering or terrorist financing.
Know Your Client (“KYC”)	The mandatory process of identifying and verifying the client's identity when opening a Player Account and periodically over time.
Money Laundering (“ML”)	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.

Money Laundering Reporting Officer ("MLRO")	Designated individual in charge of the review of KYC information and the monitoring of Player Account activities. The MLRO might further be assisted by designated personnel.
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.
Politically Exposed Person ("PEP")	A person who holds, or has held, prominent public positions, such as a senior political figure, and those closely associated with them, including immediate family members and close associates. PEPs are classified as a money laundering risk due to the potential exposure to assets acquired through corruption or bribery as a result of their position.
Prohibited Jurisdictions	Jurisdictions prohibited under the Curaçao license conditions by the Curaçao Gaming Authority at a certain moment, jurisdictions restricted by decision of the Company's managing director at a certain moment when and where applicable, and countries listed on the FATF blacklist or subject to financial sanctions imposed by the EU, United Nations, and/or OFAC.
Proliferation Financing ("PF")	The act of providing funds or financial services intended, whether wholly or partially, to support, for the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling, or use of nuclear, chemical or biological weapons and their means of delivery, or related materials (including technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or applicable international obligations.
the Regulator	The Curaçao Gaming Authority (CGA). The regulator for the entire gaming industry operating in and from Curaçao.
Shared Environment	An environment that uses a common internet connection and 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.
Terrorism Financing ("TF")	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.
Website	The online gaming platform offering online gaming services operated by the Company.

1. Overview

1.1. Introduction

Money laundering is the process of concealing, disguising, converting, transferring, or removing criminal property. In other words, it is the process of converting the proceeds of crime into assets with legal origin.

There are three stages of money laundering:

1. **Placement** – placement of funds generated from crime into financial system, either directly or indirectly (blending of funds, invoice fraud, smurfing).

2. **Layering** – the process of separating illicit proceeds from their source by creating complex "layers" of financial transaction designed to disguise the audit trail and provide anonymity (multiple bank transfers, investing in "cash" business).

3. **Integration** – the provision of apparent legitimacy to criminal derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system and appear to be legitimately earned or acquired funds (property dealing).

Terrorist financing is the provision or collection of funds with the intention that they should be used (or in the knowledge that they are to be used) to carry out acts that support terrorists or terrorist organizations or to commit acts on terrorism.

The key differences between ML and TF are:

- For money laundering to occur, the funds involved must be the proceeds of criminal conduct.

- For terrorist financing to occur, the source of funds is irrelevant, i.e., the funds can be from a legitimate or illegitimate source.

However, they both involve money or other forms of value. They both involve the movement of money or value, for example, from one person to another, one account to another, one institution to another, one country to another, one asset class to another. They are both keen to disguise the source and destination of funds.

The detection and deterrence of money laundering (ML) and terrorist financing (TF) are critical to maintaining the integrity and legal compliance of the company's operations. As an online casino operator, the company acknowledges the inherent risks associated with the gaming industry, which can be vulnerable to abuse by individuals seeking to launder illicit funds or finance terrorism. In accordance with applicable national and international

regulations, the company is committed to implementing and maintaining effective policies and procedures designed to detect, prevent, and report suspicious activities related to ML and TF. These measures are fundamental to ensuring that the company operates within the bounds of the law, safeguards its reputation, and protects the interests of its legitimate customers. The company's efforts in combating money laundering and terrorist financing contribute to promoting a secure and transparent gaming environment and are essential to upholding the standards of responsible gaming.

Financing of Proliferation (FP) refers to the act of providing financial resources for the creation, acquisition, ownership, development, export, transportation, brokerage, transfer, storage, or use of nuclear, chemical, or biological weapons, as well as the materials and delivery systems associated with these weapons. This includes any funding that supports the spread and availability of these highly destructive weapons and their related components.

The Company developed internal security measures to prevent money laundering and terrorist financing. The key features of these measures aim to stay aware of high-risk customers and detect suspicious activity, including the predicate offenses to money laundering and terrorist financing.

1.2. Management

Intelligent Innovations N.V., a limited liability company incorporated under the laws of Curaçao, with the company number 142065, having registered office at Groot Kwartierweg 10, Livestrong Building, Curaçao (hereinafter – the Company) appointed a Compliance Officer as part of the art. 5g of the NOIS.

This policy applies to all employees and outsource staff undertaking anti-money laundering, responsible gambling and anti-fraud procedures to the extent connected to their direct responsibilities, including senior management and Compliance officer.

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.

Compliance Officer 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.

Onsite versions of the AML policy can be found on:

https://vulkan.bet/en/aml-policy

https://hotspincasino.com/en/anti-money-laundering

1.3. Legal framework

The Company's Policy and Procedures were created subject to the relevant applicable legislation of the EU and Curaçao, reports of Financial Action Task Force and International standards of money laundering prevention, in particular (but not limited to):

- The Code of Criminal Law (Penal Code) (N.G. 2011, no 48);
- The National Ordinance on Money Laundering (P.B. 1993, no. 52);
- The National Ordinance on Identification of Clients when Rendering Services (NOIS) (N.G. 2017, no. 92), last update August 2024;
- The National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update August 2024;
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- National Decree Penalties and Fines Reporting Unusual Transactions (N.G. 2021, no. 69), as amended by PB 2023, no. 6;
- National Decree supervisor identification when rendering services gaming sector (L.B. 28.01.2019, no. 19/0282);
- National Decree supervision unusual transactions gaming sector (L.B. 28.01.2019, no. 19/0283);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- National Decree for general measures, of the 10th July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094

(2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015, no. 30);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National Ordinance extension of validity sanction decrees (N.G. 2018, no. 34);
- National Decree Prohibition to Import, Export and Transit of Venezuelan Gold (N.G. 2019, no. 82);
- National Ordinance on the Obligation to Report Cross-Border Money Transportation (N.G. 2002, no. 74), as amended by (N.G. 2014, no. 90);
- National Ordinance on Offshore Games of Hazard (PB 1993, no. 63);
- Curacao Gaming Control Board, Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update January 2025.

The Company regularly monitors and reviews amendments to all applicable Decrees and Regulations, ensuring that its policies and procedures are updated to remain in compliance with any changes. In addition to adhering to local regulatory requirements, the Company continuously aligns its practices with relevant international standards, including the recommendations of the Financial Action Task Force (FATF), the Caribbean Financial Action Task Force (CFATF), as well as the guidelines and instructions issued by the European Commission. The Company also ensures compliance with the six European Union Directives related to Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT).

1.4. Risk Classifications

The Company adopts a risk-based approach to effectively prevent and combat money laundering (ML) and terrorist financing (TF). This approach is structured around several key elements, which include the identification, assessment, and mitigation of risks across various areas of the business. Specifically, the Company focuses on the following risk categories:

- **Risk Identification and Assessment:** The Company proactively identifies and assesses the ML and TF risks associated with its customer base, products, services, and geographical operations. This includes evaluating the potential scale and impact of these risks, considering available data and intelligence.
- **Risk Mitigation:** Upon identifying material risks, the Company applies appropriate mitigation strategies to reduce the likelihood and impact of these risks. These measures are continuously reviewed and updated to ensure their effectiveness.
- **Risk Monitoring:** The Company maintains robust monitoring systems to track and update the risk profile over time. This includes ensuring that changes in the business environment, products, services, or regulatory landscape are incorporated into the Company's risk management framework.
- **Documentation and Accountability:** The Company ensures that all risk assessments, strategies, and mitigation measures are properly documented. Policies and

procedures are designed to uphold transparency, and senior management is held accountable for effective risk management.

Furthermore, in the development and implementation of the AML Manual, a thorough risk assessment is conducted covering the following categories:

- **Customer Risk:** The Company assesses specific customer categories and evaluates the associated business relationships to identify any higher potential risk factors related to money laundering or terrorist financing.
- **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.
- **Payment Risk:** The risk associated with different payment methods offered by the Company is carefully reviewed. The Company assesses how the characteristics of these methods may present vulnerabilities to ML/TF threats.
- **Geographical Risk:** The Company evaluates the risks linked to the geographic locations in which it operates. This includes considering the regulatory environment, prevalence of financial crime, and any jurisdiction-specific vulnerabilities.
- **Product Risk:** The Company considers the types of products offered and the extent to which their features might be exploited for illicit activities, such as money laundering or financing terrorism.
- **Service Risk:** The Company assesses risks linked to the delivery channels of its products and services, such as online platforms and mobile applications. Special attention is given to vulnerabilities that may enable money laundering or terrorist financing, ensuring appropriate controls are implemented to mitigate these risks.
- **Employee Risk:** The Company also assesses risks related to its employees and ensures appropriate controls are in place to prevent insider threats or complicity in illicit activities.

Products with the potential for large, rapid, or anonymous transactions, as well as those prone to manipulation, are identified as higher risk and are subject to enhanced controls. Payment methods that involve cash, prepaid cards, or untraceable transfers are classified as high risk, with mitigation measures such as prioritising transfers to banks in reputable jurisdictions. The Company continuously reviews and adjusts its risk mitigation strategies to ensure effective monitoring and compliance with regulations.

To manage gaming type risks, the Company also classifies risks based on the different types

of games offered. Games that facilitate quick, high-value transactions or are more susceptible to result manipulation are categorized as higher risk.

Game Type	Risk Level	Key Risk Factor
Slot Machines	Low	Fixed outcomes, low transaction values
Table Games	Medium	Large bets, frequent transactions
Poker	High	Collusion, anonymity
Sports Betting	Medium	High transaction volume
Peer-to-Peer Games	High	Player interaction, high stakes

1.5. Data processing system

The Company operates its internal data processing system to detect high-risk scenarios, money laundering, and terrorist financing in day-to-day operations.

The Data processing system consist of the following mechanisms:

- identification and verification of all users before the business relationship is established carried out by internal KYC software integrated into the website
- politically exposed person (PeP) and sanction list checks are performed by the relevant software
- transaction monitoring is managed by trained staff using internal transaction monitoring software
- reporting of all suspected money laundering cases to the Compliance Officer and the FIU.

The Company will monitor trends and changes connected to ML/TF and will develop the Data processing system to keep it up to date.

1.6. Staff Training

Upon joining the Company and thereafter annually, all staff (including outsourcing teams) will get training on AML/CFT procedures and associated policies. The training will be supplied by online and face-to-face training providers or by the appropriate Company's specialist. The specific employees are to be trained depending on the individual risk analysis.

2. Customer Acceptance and Registration Policy

2.1. Introduction

Before engaging in any gambling activity, depositing funds, or placing real-money stakes, a customer must complete the account registration process. Customers who do not register an account will not be permitted to gamble or use the Company's services.

The Company's Customer Acceptance and Registration Policy outlines the criteria for accepting or rejecting potential customers, ensuring compliance with all relevant Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) regulations. This policy also defines the registration process, which includes Customer Due Diligence (CDD) procedures, designed to verify the identity of all customers and assess the associated risks.

2.2. Customer Acceptance

In order to deposit and play on a company's site, a customer must first register on the site.

Registration is limited to individuals who are over eighteen years of age.

Customers may only open one account in their name per site. Additional checks are run to block multiple accounts by email address, mobile number, device and certain other combinations of customer data. These checks are done in order to prevent customers opening multiple accounts in order to bypass the AML threshold.

2.3. Restrictions

- Individuals under 18 years of age are not permitted to register on the site.
- Individuals considered to be PEP, under Sanctions or listed in any blacklists, in particular: the Consolidated United Nations Security Council Sanctions List, Consolidated list of persons, groups and entities subject to EU financial sanctions, Office of Foreign Assets Control Sanctions List, Her Majesty's Treasury Sanctions List, the Sanction Decree "Al-Qaida c.s., the Taliban of Afghanistan c.s., ISIL c.s., ANF c.s." (N.G. 2015, no. 29), the Ministerial Regulation "Libya" (N.G. 2015, 28), the Sanction Decree "Islamic Republic Iran 2015" (N.G. 2015, 27);, the Sanction Decree "Democratic People's Republic of Korea 2015" (N.G. 2015, 30), and the Ministerial Regulation "Yemen" (N.G. 2015, 65).
- Existing customers who have an existing exclusion on the site.
- Individuals with fraud red flags.

Each customer is allowed to open only one account in their name per site. The Company reserves the right to close any customer accounts found to be in violation of the policy regarding multiple accounts or collusion.

2.4. Information Entered on Registration

During the registration process, customers must provide complete personal information, which will be used for identity verification and to assess compliance with regulations. The Company may request the following identifying information and contact details:

- First Name and Last Name
- Date of Birth
- Gender
- Address and Country of Residence
- Email Address and Mobile Number
- Username and Password

The customer must enter all mandatory information requested on the registration form on the website, which also contains: passport number, relevant payment information (including credit card number, expiry date), etc. all of which the client warrants to be true and correct.

2.5. Terms Acceptance

During the registration process, the customer must also confirm acceptance of the website's general terms and conditions and its privacy policy.

2.6. Underage Customers

The system does not allow registration of customers who are underage: In order for the registration process to be successful, customers must be at least 18 years old or of legal age in their territory.

2.7. Customer Due Diligence

To complete registration the customer must pass Customer Due Diligence. If the CDD is failed, the registration will be declined.

3. Customer Risk Scoring and Profiling

3.1. Introduction

To effectively manage the risks of money laundering, terrorist financing, and the financing of proliferation, the Company employs a structured, risk-based approach grounded in thorough internal assessments.

This methodology enables the efficient allocation of resources and the implementation of targeted risk mitigation measures. The core principles of our risk-based approach include:

- **Proportionality** – Aligning the scope and intensity of risk management efforts with the level of identified risk.
- **Risk Prioritization** – Concentrating resources on the areas posing the greatest risk to ensure focused and effective mitigation.
- **Continuous Adaptation** – Regularly updating our risk management practices to respond to evolving threats and changes in the risk environment.
- **Operational Integration** – Embedding risk management into everyday business processes to ensure it supports and informs decision-making at all levels.

This framework includes two core components: a Business Risk Assessment (BRA) and a Customer Risk Assessment (CRA). Both assessments are essential for ensuring that the Company remains responsive to evolving threats and aligned with international standards and local expectations. The resulting risk profiles form the basis for applying proportionate preventive measures and are regularly reviewed to account for changes in business activities, regulatory developments, and emerging typologies.

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

- Identifying the ML/TF/FP risks relevant to the Company;
- Assessing the level of risk;
- Understanding the impact of the risk;
- Designing and implementing appropriate policies, procedures and controls to manage and mitigate these risks;
- Monitoring and improving the effective operation of these controls and identifying any weaknesses;
- Recording the risk assessments, including what has been done and why.

3.2. Business Risk Assessment

The Business Risk Assessment (BRA) serves as the foundation of the Company's anti-money laundering (AML) strategy. It reflects an overall understanding of the ML/TF/FP threats the Company may face in the course of its operations. It evaluates the inherent risks related to products and services offered, distribution channels, geographic exposure, transaction flows, customer demographics, and delivery methods. This process helps determine the Company's overall risk appetite and informs the design of appropriate mitigating controls and resource allocation.

The BRA is maintained in a separate document and reviewed regularly to ensure alignment with the Company's operations, market environment, and applicable regulatory requirements.

Responsible department for oversight:

Compliance function

3.3. Customer Risk Assessment

Based on the information supplied at registration (e.g. customer home address, customer location, customer age, whether PEP/sanctions), the Company will make an initial risk assessment of each customer. Customers thus start their gambling history with the Company categorized as either Low, Medium or High risk for ML/FT, which will determine decisions in how they are dealt with. Customer risk assessments are made regularly and when new information comes to light.

A Customer risk assessment is based on:

- Individual status (PEP, under sanctions, adverse media, etc.);
- Geographical location;
- Gambling and transactional behaviour;
- Payment methods the player is using;
- Fraud red flags a customer triggered.

Customers who are considered High Risk will need to undergo EDD.

The Company applies a risk-based approach to assess and monitor the normal and expected transaction volumes and amounts of its customers. This process involves developing a general understanding of typical deposit, withdrawal, and wagering patterns during onboarding and throughout the customer relationship. When transaction activity deviates significantly from established norms, it may indicate unusual or suspicious behaviour. In such cases, the

Company may conduct additional checks or enhanced due diligence (EDD) to ensure that the activity aligns with the customer's profile and to mitigate potential risks associated with money laundering or terrorist financing.

3.3.1. Customer Risk Calculation

The company employs a methodology where **risk score** is calculated by multiplying **likelihood (L)** and **impact (I)**.

Risk likelihood refers to the probability of a specific ML/TF/FP risk occurring during regular operations. This can also be seen as the vulnerability of each identified area and the likelihood of it being targeted by criminals. Consequently, some risks are more probable than others.

Risk impact measures potential damage to the company and industry if the identified ML/TF/PF risks materialize without any specific control measures in place.

Inherent risk is determined by multiplying the likelihood of a threat (rated from 1 for low probability to 5 for high probability) by the potential impact (rated from 1 for negligible impact to 5 for severe impact) should the threat occur.

Residual risk refers to the level of risk that remains after the company has applied its risk mitigation measures and controls. It reflects the effectiveness of existing procedures in reducing the identified inherent risks.

Risk scores are categorized into three levels:

- Low risk (L): 1 to 4
- Medium risk (M): 5 to 11
- High risk (H): 12 to 25

The table below presents the potential risks, their likelihood and possible impact as assessed for a customer, along with the corresponding inherent risk category and the residual risk category, which reflects the remaining risk after controls have been implemented.

Risk no.	Description	Likelihood	Impact	Risk score	Inherent risk	Residual risk (after mitigation)
	individual status					
#01	PEP: A customer is considered to be a PEP, a close family member of a PEP, or a close associate of a PEP. Mitigation methods: PEP checks in CDD and ongoing monitoring; any customer identified as a PEP, relative of a PEP or a close associate of a PEP is assigned a High-risk status and their registration is rejected or account is closed.	4	5	20	**H**	**M**
#02	Adverse Media: A customer was mentioned in negative news or information the company discovered from various sources. Mitigation methods: Adverse media and sanctions list checks during CDD and ongoing monitoring; any customer flagged in adverse media may assigned a High-risk status, and EDD will conducted when applicable.	3	4	12	**H**	**M**
#03	Sanctions: A customer is under international sanctions/blacklists. Mitigation methods: Sanctions list checks within CDD and ongoing monitoring; customers found on sanctions lists are rejected or their accounts are closed.	3	5	15	**H**	**M**
	geographical location					
#04	High-risk countries: A customer is linked to a High-risk jurisdiction. Mitigation methods: Prohibition of registration and usage from high-risk jurisdictions; geo-blocking for high-risk countries via IP addresses and CDD at the registration stage.	4	4	16	**H**	**M**
#05	Not at home: A customer's IP location is different from their registered address. Mitigation methods: Use of internal systems to detect mismatched IP addresses; apply additional scrutiny and take action if discrepancies are detected.	3	4	12	**M**	**M**
	gambling behaviour					
#06	Large sums no play: Suspicious gambling behaviour (large deposits, minimal bets, quick withdrawals). Mitigation methods: Continuous monitoring of customer transactions; review suspicious accounts and apply further CDD/EDD checks when needed.	4	4	16	**H**	**H**
#07	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). Mitigation methods: Ongoing monitoring of customer gambling behaviour; apply further CDD or EDD for customers with large, repeated losses.	3	4	12	**M**	**M**
#08	Big changes in amounts: Dramatic changes in terms of volume and size of player deposits or staking activity.	3	3	9	**M**	**M**

	Mitigation methods: Real-time detection of unusual deposit amounts or changes in staking activity; apply EDD and request sources of funds (SOF) for those who reach financial thresholds or whose behaviours escalate their risk rating.					
#09	Low odds betting: A customer repeatedly placing short odds bets (such as red/black on roulette or repetitive betting on favourites). Mitigation methods: Continuous monitoring for low odds betting patterns; flagging suspicious accounts and applying KYC, CDD, or EDD when needed.	4	3	12	**H**	**M**
	transactional behaviour					
#10	Spending above income: A customer's spend is above their affordability. Mitigation methods: Monitor customers for sudden, large increases in behaviour; apply CDD/EDD checks on customers whose spending exceeds financial thresholds.	3	4	12	**H**	**M**
#11	No withdrawal requests: Player has never requested a withdrawal. Mitigation methods: Flag accounts with no withdrawal requests as higher risk for further investigation; conduct a review to ensure the casino is not being used to facilitate illicit financial activity.	3	3	9	**M**	**L**
#12	Deposits held: Money is deposited by a customer or held over a period and withdrawn by the customer without being used for gambling. Mitigation methods: Apply Terms and Conditions regarding dormant accounts, and monthly fees for inactivity; notify customers about potential account closure and request withdrawal of funds.	4	5	20	**H**	**M**
#13	Smurfing: A customer making multiple deposits or withdrawals of small amounts without objective reasons. Mitigation methods: Monitor transaction patterns for signs of smurfing; apply EDD for clients exhibiting smurfing behaviour and request Source of Funds.	5	5	25	**H**	**H**
#14	Frequent chargebacks/disputed transactions. Mitigation methods: Monitor chargeback patterns and apply EDD for players with frequent chargebacks; investigate the reasons for chargebacks, verify the Source of Funds when necessary, and track discrepancies.	3	4	12	**H**	**M**
	payment methods the player is using					
#15	Multiple linked accounts: A customer opening an account and registering several different cards and making transfers between them. Mitigation methods: Enforce a closed-loop policy where winnings are returned to the original payment method; monitor for attempts to use multiple payment methods to bypass controls, and verify account ownership.	3	5	15	**H**	**M**
#16	High-risk methods: A customer uses high-risk payment methods, including cash, cryptocurrency, prepaid/gift cards. Mitigation methods: Restrict high-risk payment methods like prepaid cards or gift cards; implement EDD when customers use high-risk methods.	4	5	20	**H**	**M**

fraud red flags						
#17	VPN: Usage of a VPN/proxy. Mitigation methods: Implement VPN/proxy detection tools and flag suspicious activity at registration; monitor accounts for VPN/proxy usage and conduct checks where necessary.	4	3	12	**H**	**M**
#18	Multiple accounts: A customer is trying to register several gaming accounts. Mitigation methods: Implement document verification during registration; use IP address and device fingerprinting to prevent multiple accounts by the same person, as customers are allowed to open no more than one account in their name per site.	5	3	15	**H**	**M**
#19	Suspicious verification: Anonymous or incomplete customer KYC. Mitigation methods: Require complete KYC documentation for all users during registration; flag incomplete or suspicious KYC data and apply EDD when necessary.	4	4	16	**H**	**L**
#20	Inconsistent user behaviour suggesting account takeover. Mitigation methods: Implement an internal system constantly monitoring behavioural changes to detect unusual activity; apply step-up authentication when suspicious activity is detected; implement additional KYC/CDD/EDD measures whenever necessary.	3	5	15	**H**	**M**

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.

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.

3.3.2. Individual status

PEP

Politically Exposed Person (PEP) 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.

Any new or existing customer that is found to be a PEP, a relative of a PEP or a close associate of a PEP will have their account rejected or closed.

Sanctions list

Governments and international authorities publish sanctions lists to combat persons engaged in illegal activities. Sanction lists include sanctioned people, organisations, or governments. Companies, individuals, organisations, or governments are on these lists as they may pose a high risk.

Individuals and entities on this list are subject to financial restrictions prohibiting counter-terrorism regimes and money laundering worldwide.

Any new or existing customer that is found on the Sanctions database will have their account rejected or closed.

Adverse media

Adverse Media or negative news is any bad and negative information about the customer or business discovered in various sources. This information can also expose someone to being involved in a crime.

Any new or existing customer mentioned in adverse media will be a subject for EDD. The Company may close the account or reject the registration depending on EDD results.

3.3.3. Geographical location

If the Company finds that the customer resides in a High-risk county, this fact may be a subject for EDD.

High-risk countries are jurisdictions with serious strategic deficiencies to counter money laundering, terrorist financing, and proliferation financing. The Company defines the High-risk countries based on the FATF regulations, which can be found on the following website:

https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate).

The Company has implemented a geo-blocking tool to limit access to our services from players located in certain geographic locations. A list of prohibited countries can be found in Appendix 1.

3.3.4. Gambling and transactional behaviour

Each player's behaviour is constantly monitored. The Company both looks for behaviours that are considered markers of harm for problem gambling and behaviours that indicate money laundering.

Behaviours, if noticed, are allocated scores that combines with other scored ML/FT red flags.

If any examples of overt ML/FT behaviour are observed, then an EDD must be undertaken immediately of the customer and, if necessary, the SAR process implemented.

3.3.5. Payment Methods

Payment methods that allow us to trace the origin of the funds (such as the bank account) and to pay back to the source of the funds are considered low risk.

Payment methods that are funded by cash, and don't allow us to trace the source of the funds or to back to source are considered high risk.

Payment Method	**Risk Rating**
Bank transfers (Klarna, Trustly, Rapid, ApplePay), debit cards issued by banks	Low
EEA licensed e-wallets (Skrill, Neteller, Paysafecard)	Medium
Prepaid cards and vouchers	High

Manipulations with payment methods (e.g. deposits using one method, withdrawals using another) also considered as a high risk by the Company.

Cash and cryptocurrency transactions may pose a higher risk due to the challenges in tracing the source of funds and verifying their legitimacy. As these methods can be used to obscure the origin of funds or the identity of the parties involved, the Company may implement stronger checks and enhanced due diligence (EDD) procedures when such payment methods are used by customers.

3.3.6. Fraud red flags

The Company has implemented an internal anti-fraud risk management system to prevent bot attacks, fraudulent traffic, synthetic identities, account takeovers, identity thefts, credit card and CNP fraud, proxy users, multi-accounting, collusion etc. Some of the fraud red flags may also be connected to money laundering.

If the Company becomes aware a player triggered a fraud red flag, the player may be a subject for EDD.

3.4. Customer Due Diligence level

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

The frequency of customer checks is determined based on the customer's risk classification, which is assigned according to factors such as their location, transaction patterns, and sources of funds. High-risk customers, such as those from high-risk jurisdictions or with suspicious activity, will undergo more frequent reviews and monitoring. Medium-risk customers will be subject to periodic checks, while low-risk customers may have checks conducted at longer intervals. The Company ensures that these frequency requirements are aligned with regulatory expectations and are adjusted whenever there are significant changes in a customer's risk profile.

3.5. Additional Details & Source of Funds/Wealth

A daily report will be sent to the Compliance Officer. The report will include any player who is newly classified as medium or high risk, or who has moved from medium to high.

The responsible AML manager will then:

1. Review all accounts in the report, including:
    a. Checking what information the Company already have on them
    b. Open source internet checks

    c. Checking if they are in any way suspicious
2. The AML manager will then take appropriate action:
    a. Block account if needed
    b. Apply appropriate Due Diligence measures
    c. Review the responses and the information provided by the player
    d. Take appropriate action
3. If the player does not reply within 14 days, or the response is unsatisfactory, the account will be blocked. If docs are provided later, the AML manager should consider if the delay itself was suspicious, and act accordingly.

Accounts that have been assigned as medium or high risk will require AML approval before any withdrawal request can be processed.

All decisions taken by the AML manage must be documented.

3.6. On-Going Monitoring

The AML team will conduct on-going monitoring on accounts, on a risk sensitive basis. This includes:

- Obtain fresh identification when existing documents have expired.
- Question the data and information about a player whenever inconsistencies are noticed.
- And in general review and update from time to time, on a risk sensitive basis.

3.7. Withdrawals

When the AML Team review a withdrawal request, they will also look at the player's risk level:

- If the player has been classified as medium or high risk, the Verification Team will review the players documentation, and ensure that all the documents are still valid.
- If any documents have expired, new documents will be requested.

Therefore, any withdrawal request by a player who is flagged as medium or high risk, or any withdrawal request that has been otherwise flagged as high risk, will require approval by the AML team before being approved and processed.

4. Customer Due Diligence

4.1. Introduction

The Company distinguishes between general (standard), simplified and enhanced customer due diligence.

The customer is obliged to cooperate concerning the fulfillment of the due diligence obligations. If the Company cannot undertake the due diligence, the business relationship won't be established or continued, and no transaction will be carried out. In addition, the Company examines whether it is necessary to submit SAR.

4.2. 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.
- Identifying the beneficial owner and taking reasonable steps to verify their identity to ensure the casino has a clear understanding of who the beneficial owner is. For legal entities and arrangements, this process should include gaining insight into the ownership and control structure of the customer.
- Understanding and, where necessary, gathering information about the purpose and intended nature of the business relationship.

According to the above requirements, The Company collects the following information for identification and verification to prevent money laundering and terrorist financing:

a) Last name(s)

b) first name(s)

c) date of birth

d) address (street, no., ZIP code, city)

4.3. Documents acceptance

For ID, the Company require a government-issued document containing photographic evidence of the customer's identity. The following documents may be accepted for the verification purpose:

- current signed passport
- driving license
- identity card
- travel document or passport;
- another document to be designated by the Minister

For POA verification the Company accepts:

- Utility bill for a service installed at the residence issued in the last 3 months.
- Correspondence or any other government-issued document from a central or local government authority, department or agency issued in the last 3 months.
- Lease agreement (Does not have to be issued in the last 3 months but must be currently valid.)

The main requirements to the documents provided by the customer are:

- the document must be valid and not expired.
- documents must be clear, legible and of good quality.
- Mobile phone bills may not be accepted.

The Company reserves the right to close an account should any information prove to be false or misleading as a result of verification mechanisms employed by the Company. This includes documents that appear fraudulent or tampered with, or have been obtained through unauthorized third parties. Furthermore, documents provided must meet internationally recognized standards. If a customer fails to provide the required documentation or submits documents that do not meet the necessary criteria, the Company may impose account restrictions until satisfactory documents are received.

4.4. Threshold approach

The Company applies CDD measures in relation to any transaction that amounts to EUR 2000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked, engage in occasional transactions exceeding this threshold, raise suspicions of money laundering or terrorist financing, or if the casino has doubts about the accuracy or completeness of previously collected customer identification information. If the EUR 2000 threshold is met and CDD is incomplete, the customer will be prevented from depositing or withdrawing funds. If the customer does not provide the required documentation when needed, the account will be closed after 30 days, and a report of unusual activity will be filed if there is a reasonable suspicion.

"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.

Consideration will need to be given as to whether there are other circumstances in which transactions are linked, such as, whether a customer is deliberately spreading their wagering or collection of winnings over a number of transactions in order to circumvent the C/EDD requirements.

For the purpose of the CDD triggered by the threshold, the Company applies verification using risk-based approach.

4.5. Ongoing monitoring

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.

4.6. Enhanced Due Diligence

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 recognized later) only with the consent of the Compliance Officer.

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 (Certified Payslip / Certified employer letter / audited accounts 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.
- 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.

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.

Meaning of Source of Funds

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.

Meaning of Source of Wealth

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. This assessment identifies whether the customer's wealth originates from a single income stream, such as salaried employment, or multiple sources, such as business activities, investments, or inheritances. Greater attention is given to customers with multiple income streams or unverifiable sources of wealth, with the level of checks adjusted accordingly based on the nature and complexity of the information obtained.

4.7. Politically Exposed Persons and Sanctions Screening

The Company uses KYC software tool to check all customers. A PEP and Sanctions screening is performed at the registration stage for all new customers, as part of the Know Your Customer (KYC) process. In addition, if a customer's total deposits or transactions exceed €2,000 within any 30-day period, a PEP check is triggered immediately. Furthermore, the Company regularly re-screens its customer database every six months to ensure that no existing customers have changed PEP status.

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 Compliance Officer will reject registration or close the account and informed the senior management about the decision taken.

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).

4.8. Procedure for Account Closure

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 Compliance Officer will need to consider whether if an SAR was submitted as part of the concern about the player's behaviour 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.

5. Deposit and Withdrawal Management Procedures

5.1. Player Account Balance

Each player has a wallet with funds from which bets are deducted, and winnings added. All funds deposited by the player or owed by the Company are credited to the player's corresponding account. 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 do not offer credit to players. A player may not transfer funds to another player.

5.2. Payment Methods

Payments shall only be accepted and made from accounts held with licensed financial institutions or through licensed payment providers. The Company reserves the right to restrict the use of certain payment methods from specific countries based on risk assessments and regulatory requirements.

The Company does not accept or process cash deposits or withdrawals directly between the Company and its players. Where applicable, cash-related transactions conducted through authorized intermediaries are subject to limitations and verification procedures. Restrictions may apply to deposit and withdrawal amounts, with additional checks conducted as necessary.

5.3. 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 with 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.

5.4. Player Withdrawals

A player with an available balance is eligible to request a withdrawal of funds via the cashier on the site. To initiate the withdrawal, the player must specify the amount they wish to withdraw and select their preferred payout method. The withdrawal amount will then be

deducted from the player's balance.

5.5. Withdrawal Payouts

In accordance with the Company's policy and AML regulations, funds will be withdrawn to the same account from which they were deposited. This is a standard measure to prevent fraud and money laundering and to ensure that the funds are returned to the source of origin. Provided that where this is not possible, we will remit the funds to the player in line with the requirements under AML legislation.

All withdrawal processes are subject to the Company's internal rules and obligations. Withdrawals may be processed once applicable requirements, such as verification checks and promotional terms, are satisfied.

5.6. Verification and Conditions

The Company enforces strict measures to ensure that all deposits and withdrawals align with the customer's registered account information and comply with regulatory requirements.

Verification of Cardholder's Name: The name on the payment method, whether a card or bank account, must match the name registered on the player's account. Any discrepancies will trigger a review process, during which the Company may request additional documentation or suspend transactions until verification is complete.

Handling of Inconsistencies: If inconsistencies are identified between the player's account details and the payment method, the Company reserves the right to conduct further checks. This ensures the legitimacy of the payment method and its proper association with the player. Transactions may be delayed or withheld until the issue is resolved.

Minimum Wagering Activity: To prevent the abuse of bonuses or promotional offers, the Company may impose minimum wagering activity requirements before processing withdrawals. Attempts to withdraw funds without meeting these requirements will result in the suspension or delay of the transaction.

Play Before Withdrawal: The Company requires that players engage in wagering activity with deposited funds before withdrawals can be requested. This policy is designed to prevent fraudulent behaviour, money laundering, and the misuse of the platform for illicit financial activities. Withdrawals of deposited funds without prior gameplay may be restricted, and additional verification may be required to process such requests.

No Interest: Funds held in player accounts do not accrue interest. The player's balance represents available gaming funds and is not treated as a financial investment or savings account. This policy aligns with regulatory requirements and mitigates the risk of account misuse.

Funds Held Until Verification: Deposited funds cannot be used for wagering or withdrawals until the required account verification checks are completed. This includes the successful submission and approval of identification documents, proof of address, and payment method verification. The Company reserves the right to hold funds until all necessary checks are finalized, ensuring full compliance with anti-money laundering regulations and safeguarding against fraudulent activity.

Response to Breaches: In cases of unresolved inconsistencies, suspicious patterns, or repeated breaches of deposit and withdrawal rules, the Company may apply enhanced due diligence (EDD) measures. This could include requiring additional proof of identity, the source of funds, or supporting documentation. Persistent breaches may lead to account suspension or closure, with relevant authorities notified when necessary.

5.7. 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 highlights 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.

6. Suspicious and Unusual Activity Reporting

6.1. Introduction

Every employee of the Company must report to the Compliance Officer if there is suspicion or knowledge of money laundering, funding of terrorism or if the funds being used on the Company's website are the proceeds of criminal activity.

The Compliance Officer will consider each report and determine whether it gives grounds for knowledge or suspicion. If they do, then a SAR should be submitted to the Financial Intelligence Unit – Financiele Inlichtingen Eenheid (hereinafter – FIU or FIU Curaçao).

Knowledge means that the person reporting knows the event to be a fact. Suspicion implies that the person reporting the incident may have noticed something unusual or unexpected and, after making enquiries, the facts do not seem normal or make commercial or financial sense.

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.

The Compliance Officer assess 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.

In addition to suspicious transactions, the Company also has an obligation to report any unusual transactions. Unusual transactions may be identified using objective or subjective indicators issued by the FIU Curaçao. When identified, such transactions must be reported without delay.

6.2. 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 made to the Compliance 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.

6.3. Inability to Complete CDD Measures

If a customer refuses to provide CDD/EDD documentation, the Company won't immediately equate this on its own to suspicion of ML/FT.

The Company will consider all factors and information, including the payment method used, games played, playing trends and patterns, residence jurisdiction, and open-source information.

If there are grounds to suspect ML/FT after considering all of these factors, then an SAR must be submitted.

6.4. Internal Suspicious Activity Report

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 Compliance Officer to determine if the information available can be considered as sufficient for a SAR 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 Compliance Officer 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 SAR to the FIU
- make a record and inform senior management about the decision taken.

6.5. External report to FIU

Once the Compliance Officer has received an Internal SAR, she/he will decide if a SAR should be submitted to the Financial Intelligence Unit FIU.

When making this decision, the Compliance Officer 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 Compliance Officer 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 Compliance Officer, in deciding to submit the SAR or not, should answers 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.

6.6. 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 SAR, 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.

The Company doesn't execute suspicious transactions, except in cases where it cannot postpone the transaction or if the postponement could hinder the prosecution of an alleged criminal offense. In this case, the Company submits SAR immediately.

The same reporting obligation applies to any unusual transaction that meets the objective or subjective indicators defined.

6.7. Tipping-off

It is an offence to tell anyone that a SAR 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 a defence (consent) from the FIU
- can tell the customer that law enforcement is conducting an investigation.

7. Internal Control

7.1. Introduction

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.

7.2. Record keeping

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 form 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.

7.3. Appointment of Compliance Officer

The Company has appointed a Compliance Officer whose main responsibility is to review any internal suspicious transaction reports of unusual or suspicious transactions, and where necessary to submit an SAR with the FIU. The Compliance Officer is the main contact point for the Financial Intelligence Unit (FIU).

In order to ensure that the Compliance Officer is able to fulfill their role effectively, the Company guarantee that:

- Compliance Officer acts independently, has been provided the necessary knowledge of the Company's activities and is able to decide independently as to whether internal reports are to be escalated to the FIU.
- Compliance Officer has no conflicting responsibility which may pose a conflict of interest.
- Compliance Officer has sufficient time, resources and information to fulfill their responsibilities.
- Compliance Officer has a right to create work assignments to relevant employees and take decisions regarding ML/TF prevention.

The Compliance Officer and their deputy carry out the following functions (including but not limited to):

- Creation (in writing) and further development of internal risk analysis, including a complete scope of risks connected to money laundering and terrorist financing.
- Developing and updating internal policies and procedures to prevent money laundering and terrorist financing.
- Creation of uniform reporting channels.
- Involvement in other internal organizational and work instructions creation and their further development, related to implementing the regulations on the prevention of money laundering or terrorist financing.
- Ensuring compliance with current AML regulations, and other relevant legislation.

- Ongoing monitoring of the Company's business activity to comply with the money laundering regulations.
- Ensuring a proper review of the Player Accounts by the personnel.
- Ensuring CDD/EDD is undertaken.
- Suspicious activity risk assessment.
- The submission of SARs in appropriate cases.
- Contributing to the content of staff AML training.
- Maintaining a list of all inquiries received from law enforcement agencies and records relating to internal and external disclosures.
- Submitting a report to the management on Compliance Officer activities on the risk situation of the Company and the measures taken and intended to implement the obligations under money laundering regulations.

The Compliance Officer and their deputy are authorized, within the scope of their performance of their work:

- To perform their tasks independently and effectively
- To submit the necessary legally binding declarations for the undertaking and represent it externally in relevant situations.
- To provide undertaking-specific instructions for all matters relating to the prevention of money laundering and terrorist financing.
- To carry out random checks without restriction.

7.4. 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; 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 Money laundering Officer 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.

7.5. 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.

For this purpose, the Company may request the following documents (in each case with due regard to data protection):

- a valid original identity document,
- CV,
- any other documents as the Company deems necessary to request.

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.

7.6. Internal and external revision and staying up to date

The Company has compiled its policies and procedures according to the requirements of the applicable legislation and guidance of the FATF, GCB and FIU. However, the requirements and guidance, as well as external fraud trends, can and will change. Therefore, the Company has implemented the following measures to ensure the relevance of the Company's internal AML documentation:

- Key personnel have subscribed to mailing lists offered by the FIU, GCB and FATF and joined relevant forums
- The Company periodically takes legal advice from the gambling consultants for AML best practices
- In the case of an update, the Company will take the following steps, as necessary:
    - Update Company's policy documentation and training material
    - Inform all relevant staff by email regarding the updates, meet with relevant team managers, and ensure they update their teams appropriately
    - Update email communication templates and chat canned responses.
    - Update website policies, maintaining a version number and 'last update' date.
    - Update the Terms and Conditions, maintaining a version number and 'last update' date.

Any consequential update to the Terms and Conditions will trigger a pop-up notification to players on their next login where they will need to accept and agree to the new version before proceeding.

The Company may engage a third-party service provider with expertise in AML compliance to conduct independent external reviews of our AML policies and procedures. The results of these reviews will be reported to the senior management and used to enhance our AML/CTF measures and documents as needed. The frequency of external reviews is determined by senior management. It may be conducted annually or more frequently, depending on the need for an updated assessment of our AML program's effectiveness.

Approved:
Date: 25.09.2025

eMoore N.V., Managing Director
By: C. van der Leeuw, Proxy Holder

APPENDIX 1

«COUNTRIES AND TERRITORIES EXCLUDED FOR REGISTRATION»

The following list includes countries subject to restrictions. Please note that this list is not exhaustive and may also encompass other countries banned for various reasons, such as changes in FATF recommendations, restrictions due to license agreements, or other deficiencies. The Company does not provide services to clients from the countries listed below.

1. Afghanistan
2. American Samoa
3. Aruba
4. Australia
5. Belgium
6. Belize
7. Bonaire
8. Bosnia and Herzegovina
9. Burma/Myanmar
10. Burundi
11. Central African Republic
12. Curaçao
13. Democratic People's Republic of Korea
14. Democratic Republic of the Congo
15. Denmark
16. Egypt
17. Eritrea
18. Estonia
19. France
20. French Guyana
21. Greece
22. Greenland
23. Guadeloupe
24. Guam
25. Holy See (Vatican City)
26. Iran (human rights)
27. Iraq
28. ISIL and Al-Qaida
29. Italy
30. Ivory Coast
31. Kuwait
32. Lebanon
33. Libya

34. Lithuania
35. Malaysia
36. Maldives
37. Mali
38. Marshall Islands
39. Martinique (.FR)
40. Netherlands
41. Occupied Palestinian Territory
42. Puerto Rico
43. Qatar
44. Somalia
45. South Sudan
46. Sudan
47. Syria
48. USA
49. US Minor Outlying Islands
50. US Virgin Islands
51. Yemen
52. Zimbabwe