

GMB Entertainment B.V.

AML Policy

Version 1.0 (Draft)

Table of Contents

1. Overview	4
1.1. Introduction	4
1.2. Management	5
1.3. Legal framework	5
1.4. Risk-based approach	6
1.5. Data processing system	6
1.6. Staff Training	7
2. Customer Acceptance and Registration Policy	8
2.1. Introduction	8
2.2. Customer Acceptance	8
2.3. Restrictions	8
2.4. Information Entered on Registration	9
2.5. Terms Acceptance	9
2.6. Underage Customers	10
2.7. Customer Due Diligence	10
3. Customer Risk Scoring and Profiling	11
3.1. Introduction	11
3.2. Customer Risk Assessment	11
3.2.1. Individual status	11
3.2.2. Geographical location	12
3.2.3. Gambling and transactional behaviour	12
3.2.4. Payment Methods	13
3.2.5. Fraud red flags	13
3.3. Risk Score Calculation	13
3.4. Customer Due Diligence level	15
3.5. Additional Details & Source of Funds/Wealth	16
3.6. On-Going Monitoring	16
3.7. Withdrawals	16
4. Customer Due Diligence	18
4.1. Introduction	18
4.2. Standard Customer Due Diligence	18
4.3. Documents acceptance	19
4.4. Threshold approach	19
4.5. Ongoing monitoring	20
4.6. Enhanced Due Diligence	20

4.7.	Politically Exposed Persons and Sanctions Screening	22
4.8.	Procedure for Account Closure.....	24
5.	<i>Deposit and Withdrawal Management Procedures.....</i>	26
5.1.	Player Account Balance.....	26
5.2.	Payment Methods	26
5.3.	Player Deposits.....	26
5.4.	Player Withdrawals	26
5.5.	Withdrawal Payouts	26
6.	<i>Suspicious Activity Reporting</i>	28
6.1.	Introduction	28
6.2.	Red Flags Indicators	28
6.3.	Inability to Complete CDD Measures	29
6.4.	Internal Suspicious Activity Report.....	29
6.5.	External report to FIU	30
6.6.	Reporting Procedure.....	31
6.7.	Tipping-off.....	32
7.	<i>Internal Control</i>	33
7.1.	Introduction	33
7.2.	Recordkeeping	33
7.3.	Money Laundering Reporting Officer.....	34
7.4.	Training.....	35
7.5.	Employees background check	37
7.6.	Internal and external revision and staying up to date	38
7.7.	Version Control	39

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.

GMB Entertainment B.V.. 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

GMB Entertainment B.V., a limited liability company incorporated under the laws of Curaçao, with the company number 170457, having registered office at Korporaalweg 10, Willemstad, 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.

1.3. Legal framework

The Company's Policy and Procedures were created subject to the relevant applicable legislation, in particular (but not limited to):

- Curacao - National Ordinance Reporting Unusual Transactions (NORUT) of November 7, 2017
- National Ordinance Identification when Rendering Services (NOIS) of October 2, 2017;
- National Ordinance Penalization of Money Laundering (NOPML)
- EU-Directive 2015/849 of the European Parliament and of the Council of 20 May 2015;
- EU-Directive 2018/843 of the European Parliament and of the Council of 30 May 2018;

- EU-Directive 2018/1673 Of the European Parliament And Of The Council Of 23 October 2018;
- The FATF Recommendations.
- National Ordinance for Games of Chance (LOK)

1.4. Risk-based approach

The Company undertakes to prevent and combat money laundering and terrorist financing following a risk-based approach. A risk-based approach the Company summarised as covering the following areas:

- **risk identification and assessment** – identifying the money laundering risks facing the Company, given its customer, product, and services profile and having regard to available information, and assessing the potential scale and impact of the risks
- **risk mitigation** – identifying and applying adequate measures to mitigate the material risks facing the Company
- **risk monitoring** – putting in place management information systems (MIS) and keeping up to date with changes to the risk profile through changes to the business or to the threats, and
- **documentation** – documenting the risk assessment and strategy and having policies and procedures covering the above and achieving effective accountability from the board and senior management.

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 manually by internal KYC team
- politically exposed person (PeP) and sanction list checks are performed by the relevant software
- transaction monitoring is managed by trained staff
- 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 additional internal procedures 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 gamble, deposit or place a real-money stakes, the customer must register an account. Customers who do not register an account will not be able to gamble.

The Customer Acceptance and Registration Policy defines the criteria by which the Company may or not accept potential customers and describes the registration process.

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:

- Al-Qaida c.s., the Taliban of Afghanistan c.s., ISIL c.s., ANF c.s.”
- Australian Sanctions (AU)
- Bureau of Industry and Security - Entity List (US)
- Bureau of Industry and Security - Unverified List (US)
- Bureau of Industry and Security (US)
- Canada, Office of the Superintendent of Financial Institutions, OSFI Consolidated
- CIA Leader list
- Consolidated Canadian Autonomous Sanctions List
- Department of State, AECA Debarred List (US)
- Department of State, Non-proliferation Sanctions (US)
- EU Financial Sanctions (EU)
- European Union, Consolidated list of persons, groups and entities subject to EU financial sanctions
- Foreign Financial Institutions Subject to Part 561 (the Part 561 List)
- Foreign Sanctions Evaders List (FSE)
- INTERPOL Wanted List
- Islamic Republic of Iran
- Libya Sanctions
- Non-SDN Iranian Sanctions Act List (NS-ISA)
- OFAC Consolidated Sanctions List

- Office of the Superintendent of Financial Institutions (Canada)
- Palestinian Legislative Council (PLC) List
- Sectoral Sanctions Identifications (SSI) List
- Specially Designated Nationals (OFAC)
- Specially Designated Nationals List (SDN)
- Switzerland Sanction List (SECO)
- U.S. Department of Commerce, Bureau of Industry and Security - Denied Persons List
- U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC)
- UK Financial Sanctions (UK)
- UK, Consolidated Financial Sanctions list (HMT)
- United Nations Sanctions (UN)
- United Nations Security Council (UN), Consolidated Sanctions list
- US Consolidated Sanctions (US)
- US State Dept. WMD Non-Proliferation List
- Existing customers who have an existing exclusion on the site.
- Individuals with fraud red flags.

Players 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 players opening multiple accounts in order to bypass the AML threshold.

2.4. Information Entered on Registration

During the registration process and later on, the Company will 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.

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. Date of Birth will be cross checked with the provided ID upon customer Due Diligence.

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

Within the risk-based framework, The Company will undertake risk profiling of all customers from the time they are registered for the potential money laundering/terrorism financing risks.

It is important to note that the Company's policies and procedures are based on the following:

- Actual regulatory and legal requirements;
- Guidance provided by GCB and FIU;
- Our own internal evaluation of our overall business risk assessment, and our knowledge and experience with our customers.

3.2. 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 categorised as either Low, Medium or High risk for ML/FT, which will determine decisions made at later points in how they are dealt with. Customer risk assessments are made regularly and when new information comes to light.

The 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.

3.2.1. Individual status

PEP

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.

Any new or existing customer that is found to be a PEP or relative of such 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 counterterrorism 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.

3.2.2. Geographical location

If the Company finds that the customer resides in a High-risk country, 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/en/countries/black-and-grey-lists.html>

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.

3.2.3. Gambling and transactional behaviour

Each players 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.

3.2.4. 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, Vouchers and Cryptocurrency	High

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

3.2.5. Fraud red flags

The Company has 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, it will automatically be a subject for EDD.

3.3. 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 higher 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	100
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:

<u>CMM Score</u>	<u>Risk Category</u>
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.

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	X
Collect additional personal details		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

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 Customer Due Diligence (hereinafter – CDD) and Enhanced Customer Due Diligence (hereinafter – EDD)

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.

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

- a) First and Last Name
- b) Date of birth
- c) address (street, no., ZIP code, city)
- d) ID
- e) Proof of Address (POA)

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 6 months.
- Correspondence or any other government-issued document from a central or local government authority, department or agency issued in the last 6 months.
- Lease agreement (Does not have to be issued in the last 6 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.

4.4. Threshold approach

The Company will apply EDD 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.

"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 EDD 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 recognised 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.

4.7. 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.

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/en/countries/black-and-grey-lists.html>

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 licenced financial institutions or through licenced payment providers.

No cash deposits/withdrawals will be effected between the Company and its players.

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 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.

5.5. Withdrawal Payouts

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.

6. Suspicious 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 – Financiële 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.

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 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 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.

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.

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. Recordkeeping

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.

7.3. Money Laundering Reporting 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 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 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.

7.7 Version Control

The Company is constantly improving its policies to actively combat Money Laundering and the Financing of Terrorism and therefore requires Version control to keep track of Changes and Approval by the Director.

Version	Date	Approved By
1.0 (Draft)	July 2025	Xecutive Corporate Management B.V., Director

For Approval

Xecutive Corporate Management B.V.

Appendix 1

- Afghanistan
- Aland Islands
- American Samoa
- Angola
- Anguilla
- Antarctica
- Antigua and Barbuda
- Barbados
- Belize
- Benin
- Bhutan
- Bonaire (including Sint Eustatius and Saba)
- Bouvet Island
- British Indian Ocean Territory
- Burundi
- Cape Verde
- Central African Republic
- Chad
- Cocos (Keeling) Islands
- Cook Islands
- Comoros
- Congo, Democratic Republic of
- Congo, Republic of
- Crimea
- Cuba
- Curacao
- Djibouti
- Donbas
- Equatorial Guinea
- Eritrea
- Fiji
- French Guyana
- French Polynesia
- French Southern Territories
- Gabon
- Gambia
- Grenada

- Guadeloupe
- Guam
- Guinea
- Guinea-Bissau
- Guyana
- Haiti
- Heard Island and McDonald Islands
- Holy See (Vatican City State)
- Iran
- Iraq
- Ivory Coast (Côte d'Ivoire)
- Kherson
- Kiribati
- Kosovo
- Kyrgyzstan
- Lao People's Democratic Republic
- Lebanon
- Liberia
- Libya
- Macao
- Malawi
- Mali
- Marshall Islands
- Martinique
- Mauritania
- Mayotte
- Micronesia, Federated States of
- Montserrat
- Myanmar
- Nauru
- Netherlands
- New Caledonia
- Niger
- Niue
- Norfolk Island
- North Korea
- Northern Mariana Islands
- Palau
- Palestinian Territory
- Papua New Guinea
- Pitcairn
- Puerto Rico

- Rwanda
- Saint Barthelemy
- Saint Helena
- Saint Kitts and Nevis
- Saint Lucia
- Saint Martin
- Saint Pierre and Miquelon
- Saint Vincent and the Grenadines
- Sao Tome E Principe
- Seychelles
- Sint Maarten
- Sierra Leone
- Solomon Islands
- Somalia
- South Georgia and the South Sandwich Islands
- Sudan (North and South)
- Suriname
- Svalbard and Jan Mayen
- Syria
- Tajikistan
- Timor-Leste
- Togo
- Tokelau
- Tonga
- Turkmenistan
- Turks and Caicos Islands
- Tuvalu
- United States of America
- United States Minor Outlying Islands
- US Virgin Islands
- Uzbekistan
- Vanuatu
- Venezuela
- Wallis and Futuna
- Western Sahara
- Western Samoa
- Yemen
- Zaporizhzhia
- Zimbabwe