Bluewave Interactive N.V

Payment and Fraud Department
Procedures manual

Date	Version	Name
01.10.2023	Version 1.0	Mr. Andreas Andreou
10.01.2024	Version 1.1	Mr. Andreas Andreou
29.01.2025	Version 2.0	Mr. Andreas Andreou
09.06.2025	Version 2.1	Mr. Gian Carlo Comla

CONTENTS

1 Introduction 5
1.1 List of Abbreviations 5
1.2 About this Document 5
2 Background 6
2.1 What is Money Laundering? 6
2.2 What is funding of Terrorism? 6
2.3 The threats facing the online gambling sector 6
2.4 The Need to Combat Money Laundering and Financing of Terrorism 7
2.5 The AML requirements focus in the following areas: 7
3 Customer acceptance 9
3.1 Age Verification 9
3.2 Countries and territories excluded from registration 9
3.3 Politically Exposed Person Checks 10
3.4 Sanction Checks 11
4 Risk Based approach 12
4.1 Setting up the risk factors 12
4.2 Investigating unusual activities 12
4.3 Automatically higher risk participants 12
4.4 Risk Assessment 13
4.5 No cash policy 13
4.6 Risk Profiles 13
5 Payment and Fraud department structure 14
6 Customer Due Diligence 15
6.1 Simplified Due Diligence 16
6.2 Regular Due Diligence 16
6.3 CONTINUED DUE DILIGENCE 16
6.4 Documentary Evidence Method 17
6.5 Enhanced Due Diligence 18
6.6 Pending withdrawal cancelation 19
6.7 Client refusing to send documents 19
7 Source of Wealth Questionnaire/Documentation 19
8 Monitoring 19
8.1 Daily Monitoring 19
8.2 Suspicious Behavior 19
8.3 KYC documentation review 20
9 Money Laundering Reporting Officer 20
9.1 MLRO's responsibilities 20
9.2 Suspicious accounts – internal reporting to MLRO 21
9.3 Internal Fraud 21
9.4 Staff Training 21
9.5 Business RElations 21

10 Funds Management 21
10.1 Accepted Payment methods 21
10.2 22
10.3 Dormant Accounts Procedure 22
10.4 THIRD-PARTY RISK MANAGEMENT 23

1 INTRODUCTION

1.1 LIST OF ABBREVIATIONS

Term	Definition
ST	Suspicious Transaction
AML	Anti-Money Laundering
CFT	Combating the Financing of Terrorism
CS	Client Support
KYC	Know Your Customer
MLRO	Money Laundering Reporting Officer
FATF	Financial Action Task Force
FT	Financing of Terrorism

1.2 ABOUT THIS DOCUMENT

This Anti-Money Laundering (AML) and Counter-Financing of Terrorism (CFT) Policy outlines the internal governance framework adopted by [Company Name] to meet its obligations under the regulatory requirements of the Curacao Gaming Control Board (GCB), including those deriving from NORUT, NOIS, and internationally accepted FATF standards.

Specifically, this document aims to:

- Provide an overview of the legal and regulatory landscape surrounding money laundering and terrorist financing;
- Outline the Company's internal policies, controls, and procedures to prevent and detect AML/CFT risks;
- Define the roles and responsibilities of staff and senior management in relation to AML/CFT compliance;
- Affirm the Company's zero-tolerance policy toward criminally derived funds and the facilitation of any form of money laundering or terrorist financing.

The Company is committed to ensuring that no business relationship is established or maintained with any person or entity whose funds originate from illicit sources. Prior to the commencement of any business relationship, all customers will be subject to identity verification in line with our risk-based approach (RBA). Verification triggers include, but are not limited to:

- First deposit;
- Cumulative deposits or withdrawals exceeding EUR 2,000;
- Activity patterns that raise suspicion or meet defined internal red flags.

2 BACKGROUND

2.1 WHAT IS MONEY LAUNDERING?

Generally, money laundering is described as the process by which the illegal nature of criminal proceeds is concealed or disguised in order to lend a legitimate appearance to such proceeds. This process is of crucial importance for criminals as it enables the perpetrators to make legitimate economic use of the criminal proceeds. When a criminal activity generates substantial income, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or to the persons involved. Criminals do this by disguising the sources, changing the form or moving the funds to a place where they are less likely to attract attention.

Traditionally, three stages were identified for the process of money laundering – the placement stage, the layering stage and the integration stage.

a) Placement: the first introduction of the cash proceeds of criminal conduct into the financial system, especially via deposit-taking institutions and, again, particularly in jurisdictions with extensive banking secrecy laws and little or no anti money laundering legislation.

b) Layering: separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.

c) Integration: the provision of apparent legitimacy to criminally 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 appearing to be normal business funds.

2.2 WHAT IS FUNDING OF TERRORISM?

Funding of terrorism is the process by which terrorist organisations or individual terrorists are funded in order to be able to carry out acts of terrorism.

The funding of terrorist activity, terrorist organisations or individual terrorists may take place through funds deriving from legitimate sources or from a combination of lawful and unlawful sources. Indeed, funding from legal sources is a key difference between terrorist organisations and traditional criminal organisations involved in money laundering operations. Another difference is that while the money launderer generates income by obscuring the link between the crime and the generated funds, the terrorist's ultimate aim is not to generate income from the fund-raising mechanisms but to obtain resources to support terrorist operations.

2.3 THE THREATS FACING THE ONLINE GAMBLING SECTOR

The Curacao Gaming Control board has made an assessment of the threats facing the gambling sector. In any quantification of the threats facing a given sector there will be a natural emphasis on the threats that have been revealed from investigations and an absence of information on those threats that criminals have been able to keep hidden.

The threat rating identified by the GSC from highest to lowest is as follows:

- Criminal ownership, infiltration or coercion of an online gambling licensee to either launder on an ongoing basis or to launder a limited number of large transactions (perhaps to associated, unlicensed companies) before simulating business failure and surrendering the licence;
- Criminal ownership, infiltration or coercion of a domestic casino license;
- Undetected, high-volume, systematic laundering by organised crime of an online gambling platform;
- Use of an online gambling platform to benefit from manipulation of outcomes in sport;
- Opportunistic laundering by individuals or dedicated criminal rings on an online gambling platform, including instances where the predicate offence (e.g. credit card theft, cheating) first occurs on the platform;
- Use of an online gambling platform as an informal payroll, banking system or money/value transfer system ("MVTS") for criminals or terrorists (including use by PEPs, etc. to transfer value across borders where currency controls exist);
- Collusion with business to circumvent statutory restrictions in another jurisdiction;
- Introduction of proceeds of crime on to an online gambling platform as part of criminal lifestyle spend;
- Use of an online gambling platform to generate personal or corporate income without declaring to tax authorities (including by licensees);
- Use of high street shops affiliated with online operations to place dirty cash into the online environment;
- Extension of credit in order to create then exploit debt;
- Introduction of proceeds of crime to an online gambling platform by gamblers who steal money to fund gambling;
- Use by hackers of stolen passwords to transfer value from hacked online accounts to other withdrawal mechanisms or confederates;

2.4 THE NEED TO COMBAT MONEY LAUNDERING AND FINANCING OF TERRORISM

The Company has three main concerns:

- Reputation Risk
- Regulatory Risk
- Litigation Risk

2.5 THE AML REQUIREMENTS FOCUS IN THE FOLLOWING AREAS:

a) Identification procedures;
b) Record Keeping;
c) Internal procedures;
d) Staff Education, Training and Development;
e) Internal controls and communication procedures that are appropriate for the purposes of forestalling and preventing money laundering and the financing of terrorism;
f) Procedures, controls and evaluation; and
g) Take appropriate measures from time to time for the purpose of making employees and workers aware of:
   - the procedures established, maintained and operated under sub-paragraph; and
   - the provisions of the money laundering and terrorist financing requirement

2.6 SUSPICIOUS TRANSACTION REPORTING (STR) OBLIGATIONS

The Company is subject to the requirements of the **National Ordinance on the Reporting of Unusual Transactions (NORUT)** in Curaçao, which obliges reporting entities to identify, document, and report suspicious transactions or attempted transactions to the competent authority.

2.6.1 Legal Obligation to Report

- The Company is legally required to submit **Suspicious Transaction Reports (STRs)** to the **Financial Intelligence Unit Curaçao (FIU-Curaçao)** without delay upon identifying a transaction or attempted transaction that:
    - Appears inconsistent with the known legitimate business or personal activities of the customer;
    - Raises suspicion of money laundering (ML) or the financing of terrorism (FT);
    - Matches typologies outlined by FIU-Curaçao or other competent authorities.

2.6.2 STR Triggers and Indicators

STRs may be triggered by, but are not limited to, the following:

- Unusual transaction sizes or patterns;
- Multiple or structured transactions to evade reporting thresholds;
- Use of high-risk payment channels (e.g. crypto, vouchers, e-wallets);
- Transactions involving high-risk jurisdictions;
- Refusal or failure to provide KYC documents;
- Rapid movement of funds with no apparent economic rationale;
- Customers attempting to influence or avoid CDD procedures.

2.6.3 STR Process and Responsibility

- All employees are required to escalate any suspected activity to the **Money Laundering Reporting Officer (MLRO)** using internal reporting channels.
- The MLRO is responsible for assessing whether the suspicion meets the reporting threshold and, if so, for submitting a formal STR to **FIU-Curaçao** via the designated reporting platform or secure channel.
- STRs must be filed **without tipping off** the subject (customer or third party) in accordance with NORUT and international best practices.

2.6.4 Documentation and Confidentiality

- The Company maintains a secure **STR Register**, including:
    - A unique reference number;
    - Summary of the suspicion;
    - Action taken and date of submission;
    - Decision rationale (if not submitted).
- All STR documentation is confidential and access is restricted to the MLRO and designated compliance personnel.

2.6.5 Retention and Audit

- All STRs, including those assessed but not submitted, are retained for **at least five (5) years** from the date of filing or decision not to file.
- The Company's STR processes are subject to internal audit and regulatory review, and may be revised in line with updated guidance from **FIU-Curaçao** or the **Curaçao Gaming Control Board (GCB)**.

3 CUSTOMER ACCEPTANCE

3.1 AGE VERIFICATION

The Company will not accept any player unless of legal age, 18 years or older (Estonia 21 years or older). The registration process requires the date of birth to be over 18 years and will not permit a user to input a date, which would contradict that.

3.2 COUNTRIES AND TERRITORIES EXCLUDED FROM REGISTRATION

1. Afghanistan
2. Australia
3. ISIL and Al-Qaida
4. Bosnia and Herzegovina
5. Burma/Myanmar
6. Burundi
7. Central African Republic
8. China
9. Crimea and Sevastopol
10. Curacao
11. Democratic Republic of the Congo
12. Denmark
13. Egypt
14. Eritrea
15. Estonia
16. Federal Republic of Yugoslavia & Serbia
17. Great Britain
18. Honk Kong
19. Hungary
20. Israel
21. Iran
22. Iraq
23. Ivory Coast
24. Latvia
25. Lebanon
26. Libya
27. Lithuania
28. Maldives
29. Mali
30. Netherlands
31. North Korea (Democratic People's Republic of Korea)
32. Republic of Guinea
33. Republic of Guinea-Bissau
34. Republic of Moldova
35. Somalia
36. South Sudan
37. Sudan
38. Syria
39. Tunisia
40. Yemen
41. Venezuela
42. USA
43. Ukraine
44. Zimbabwe.

Clients from countries that the FATF has indicated are deficient (High-risk and non-cooperative jurisdictions)

1. Bahamas
2. Bosnia and Herzegovina (Not in the FATF list anymore)
3. Botswana
4. Democratic People's Republic of Korea
5. Ethiopia
6. Ghana
7. Iraq (Not in the FATF list anymore)
8. Iran
9. Pakistan
10. Serbia
11. Sri Lanka
12. Syria
13. Trinidad and Tobago
14. Tunisia
15. Vanuatu (Not in the FATF list anymore)
16. Yemen

The following categories of players will not be accepted at registration/post registration checks:

- Players residing in non-reputable jurisdictions,
- IP login registered in a non-reputable jurisdiction,
- Sanctioned individuals,
- Players under the age of 18

3.3 POLITICALLY EXPOSED PERSON CHECKS

The Company must carry out PEP checks at Sumsub (https://sumsub.com/)

All PEP's are checked against multiple lists with the use of 3rd party software.

When a player is a confirmed PEP, it will be classified as high risk and senior management approval will be sought before any business is undertaken. In such cases, adequate measures will be taken to establish the source of funds and source of wealth involved in the prospective business relationship. If senior management decides to establish a relationship with the PEP, enhanced ongoing monitoring will be carried out in order to mitigate this high risk.

As a general company policy, the Company prefers not to accept any PEPs, however senior management has discretion to alter the policy.

Politically Exposed Person is defined as any of the following resident in any country:

(a) a natural person who is or has been entrusted with prominent public functions, including —

- a head of state, head of government, minister or deputy or assistant minister;
- a senior government official;
- a member of parliament;
- a senior politician;
- an important political party official;

- a senior judicial official;
- a member of a court of auditors or the board of a central bank;
- an ambassador, chargé d'affaires or other high-ranking officer in a diplomatic service;
- a high-ranking officer in an armed force;
- a senior member of an administrative, management or supervisory body of a State-owned enterprise;
- a senior official of an international entity or organisation; and
- an honorary consul;

(b) any of the following family members of a person mentioned in sub-paragraph (a) —

- a spouse;
- a partner considered by national law as equivalent to a spouse;
- a child;
- the spouse or partner of a child;
- a sibling;
- a parent;
- a parent-in-law;
- a grandparent; or
- a grandchild;

(c) any close associate of a person mentioned in sub-paragraph (a), including —

- any natural person who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with such a person;
- any natural person who has sole beneficial ownership of a legal entity or legal arrangement that is known to have been set up for the benefit of such a person;
- any natural person who is in a position to conduct substantial financial transactions on behalf of such a person.

3.4 SANCTION CHECKS

The online checks the Company processes on the registration of the client, cross checks against multiple Sanctions list with the use of 3rd party software Sumsub (https://sumsub.com/)

These list include:

- **Bank of England (BOE)**
- **Office of Foreign Assets Control (OFAC)**
- **CONSOLIDATED UNITED NATIONS SECURITY COUNCIL SANCTIONS LIST**
- **Consolidated list of EU financial sanctions and Consolidated list of persons, groups and entities subject to EU financial sanctions.**

As a general company policy, the Company prefers not to accept any Sanctioned Individuals

These clients are classified as High risk.

Any client which is flagged in these lists:

- Will have his account locked;
- the client may be asked for enhanced due diligence to verify the customer

Clients in this list are required to send their:

- Passport/Driver's licence
- Send an original utility bill;

The Customer Support officers contact the client and ask for additional due diligence documentation until they ascertain the identity of the client.

4 RISK BASED APPROACH

4.1 SETTING UP THE RISK FACTORS

The Company made a list of risk factors to determine a client's risk profile in relation to ML & CFT.

The list includes the following:

- A list of countries which the FATF considers to apply deficient AML/CFT controls;
- A list of countries which in the licensee's opinion represent heightened ML/FT risk (which may or may not be on the first list);
- A value which represents the upper value of a typical player's transactions;
- A list of payment channels which are considered higher risk;
- A list of any other indications which in the opinion of the licensee's MLRO indicates higher risk;
- A list of the subjects of AML/CFT related warning notices; and
- Screening for politically exposed persons, sanctions and adverse information.
- Product risk (Casino, Live Casino)

Irrelevant of how money is transferred to any of our casino, there is always a risk that this money would have originated from illegal activities, such as credit/debit card fraud, theft from player's employer or even narcotics trafficking. Hence, by paying greater attention and increase monitoring of high spenders, the Company will be able to mitigate this risk

- If a client is suspected of money laundering or terrorist financing and decides not to exit the participant, then this too will be flagged as above.

4.2 INVESTIGATING UNUSUAL ACTIVITIES

If unusual activities are identified through the ongoing monitoring, the client must be investigated. If no satisfactory explanation can be recorded for the deviation behaviour in the account, then the MLRO shall submit a Suspicious Transaction Report (STR) to FIU Curaçao, in accordance with NORUT obligations.

4.3 AUTOMATICALLY HIGHER RISK PARTICIPANTS

Where participants are flagged with a notification after the account opening, accounts are locked until customer due diligence procedures are in place. Some of the possible notifications that can be triggered are:

- A client who is a Politically Exposed Persons (PEPs), their family members or close business associates ("persons linked thereto");
- A client residing or located in a country, the AML/CFT credentials about which the Company has doubts;
- A client who has been the subject of a disclosure
- A client flagged on the sanctions list.
- A client depositing gambling/withdrawing big amounts.
- A client flagged as a fraudster (reported by PSP)

The Company holds registers for PEP/Sanctioned clients.

4.4 RISK ASSESSMENT

Risk Assessments are done on regular basis, depending on the business needs and also on the need of reviewing new markets or closing existing ones.

4.5 NO CASH POLICY

No cash deposits / withdrawals are accepted from customers.

4.6 RISK PROFILES

1. Low: default risk level
2. Medium:
    - Non closed loop withdrawal
    - Accumulated net income of 500 USD
    - 5K Deposits accumulated (All Methods)
    - Third party deposit (block the card/payment method, request third party KYC and payment method)
    - Velocity Limits
        - 500 euros' deposits within 1 hour
        - 1000 euros' deposits within 24 hours
        - 1000 euros' deposits within 72 hours
        - 10 failed transactions in 60 minutes
    - Bin-Country Mismatch
    - Stolen/Restricted Card used
    - IP Login from non-reputable jurisdiction
    - IP mismatch with Country
    - IP link with other customers (if benefitting from bonus abuse or live casino)
    - Customer creates Multiple Accounts

Actions:

- KYC Requested
- EDD if needed

3. High:
    - 1K deposits PSC in 90 days
    - 5K deposits PSC
    - 10K deposits PSC
    - 5K deposits e-wallets
    - 10K deposits e-wallets
    - 25 K deposits e-wallets
    - 50 K deposits e-wallets
    - 50K deposits accumulated (All methods)
    - 5k losses in 30 days
    - 5 – 10 losses in 90 days

- 10K losses anytime
- 20K losses anytime
- 30K losses anytime
- 40K losses anytime
- 50K losses anytime
- Sanction, PEP, SIP (Not accepted as clients)

Actions:

- KYC
- EDD
- SOW questionnaire
- Source of wealth documentation if needed

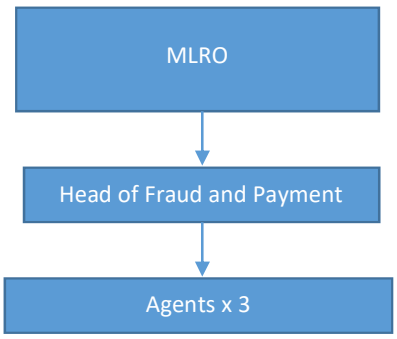
Electronic wallets (e-wallets) Usually, electronic wallets which only accept money from financial institution accounts held in the player's name (for instance Skrill) will not pose any greater or lesser money laundering risk than funds received directly from the financial institution itself. Certain e-wallets do accept deposits via pre-paid vouchers (for instance Neteller) and hence these pose a higher risk as money launders and/or terrorists may choose such payments methods to disguise the origin of their funds or to obstruct the audit trail. In order to mitigate this risk, the Company takes due care in choosing which e-wallets it will commit to provide to players, especially since not all e-wallets are licensed in reputable countries. Thus, due diligence checks are undertaken to ensure that the Company is only contracting with reputable companies

4.7 FATF Country Risk Classification and Register

In accordance with its obligations under NORUT and FATF Recommendations 1 and 19, the Company maintains a live **FATF Country Risk Register** to assess jurisdictional risk exposure.
This register classifies countries into three tiers based on the FATF's public statements and the Company's internal risk evaluation:

- **Prohibited**: Countries listed on the FATF "Call for Action" list (e.g., DPRK, Iran). No business is conducted with clients or third parties from these jurisdictions.
- **High-Risk (EDD Required)**: Countries under **Increased Monitoring** (grey list). Clients or third parties from these countries may be accepted subject to Enhanced Due Diligence (EDD) and senior management approval.
- **Monitored/Reviewed**: Countries with relevant AML/CFT deficiencies flagged by the Company, GCB, or other competent authorities.

5 PAYMENT AND FRAUD DEPARTMENT STRUCTURE



Head of Fraud and Payment:

Responsibilities:

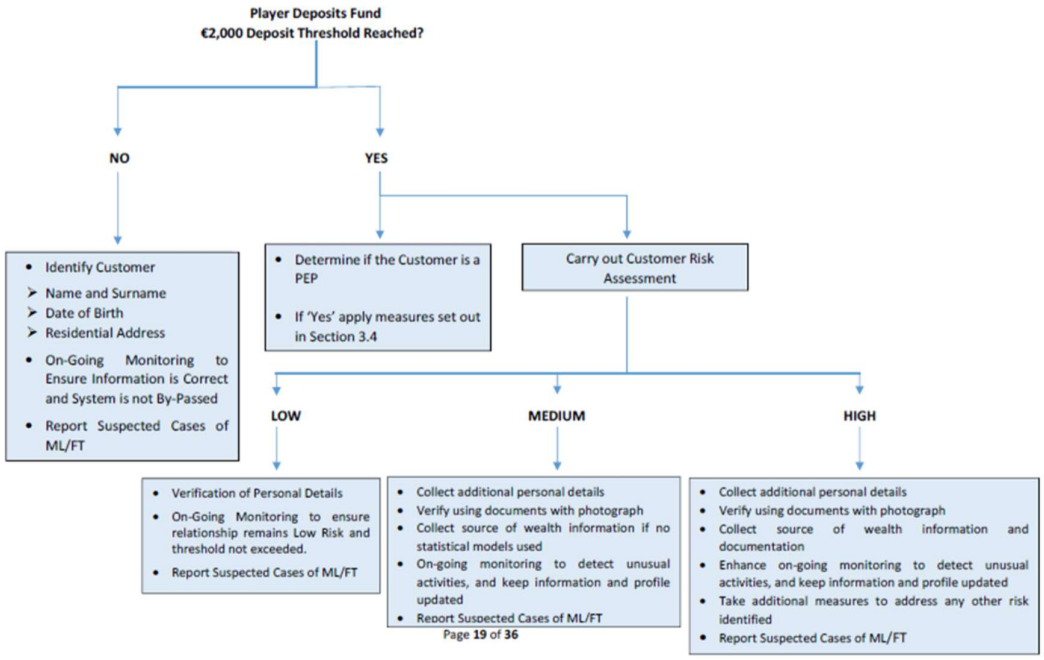
- Organizing department work.
- Creating and implementing AML, Anti-Fraud and payments procedures.
- Optimizing and insuring that departments work quality and stable workflow.
- Preparing monthly reports for management.
- Daily transactions monitoring.

Fraud and Payments Agents:

Responsibilities:

- Sign-up and new account check. Address, Country, name, email, IP
- Daily reports check
- Monitoring incoming and outgoing transactions
- Processing Withdrawals
- Calculating bonus rollover
- Checking that account is in order to our Anti-Fraud and AML requirements
- Must insure that withdrawals are kept in the loop. That means that withdrawals must be processed to the same account that deposit were made from, if it is possible.
- PEP and Sanctions list monitoring
- Checking that deposit was wagered at least once

6 CUSTOMER DUE DILIGENCE



- KYC to be always requested when the accumulated deposit amount hits medium risk
- KYC always to be requested when winnings are generated from non-deposit bonus/free spins.
- KYC + Photo holding ID and explanation why IP is shared, will be requested on withdrawal if there is shared IP.
- Skype video or phone verification maybe performed in case of any suspicion.

Customer due diligence is the process of identifying and verifying the identity of players. There are three levels of customer due diligence that the company must carry out:

1) Simplified Due Diligence
2) Regular Due Diligence
3) Enhanced Due Diligence

6.1 SIMPLIFIED DUE DILIGENCE

A Simplified Due Diligence process will be the first stage of a risk based process. Simplified Due Diligence is carried out between Registration and First Deposit on Customers that hail from low risk jurisdictions.

Simplified due diligence is performed by the customer providing identification details prior to registration.

Every registering player must provide all the details / fields included in the registration process document of the company. This document meets the requirements for “identification of customers”, and include:

- the date of birth;
- the player’s identity;
- the player’s place of residence; and the player’s valid e-mail address.

Every registering player must activate the account via the email, SMS or call activation procedure. Once a customer completes the registration form and verifies the email or SMS, then the account is opened and found within the back office system.

It is company policy not to allow players to deposit or withdraw any funds whatsoever before Standard Due Diligence is carried out.

6.2 REGULAR DUE DILIGENCE

The company conducts Regular Due Diligence in two distinct methods, which are both equally acceptable. Therefore, the company are able to select the method they can adopt from the following:

- Electronic Verification
- Documentary Evidence

6.3 CONTINUED DUE DILIGENCE

When a customer hits the Medium or High on the Risk Based Approach we will carry out further checks on the account and leave a clear note:

Is ID expired? Have new payment methods been used that we need copies of?

Has pattern changed, do we need to update risk level of customer?

If we have SOW questionnaire do the answers still match the pattern?

KYC requests will have the same 7/14/30 day grace periods to send documents

A clear note should read something like:

CDD: ID expired, new ID requested, CC**6789 not yet received, requested now. Deposit and gameplay pattern remains unchanged

6.4 DOCUMENTARY EVIDENCE METHOD

KYC- Standard Due Diligence - This is achieved by the following thresholds triggering the Standard Due Diligence process:

- Cumulative deposits exceeding EUR 2,000;
- Attempt to withdraw to a different card or payment method;
- Attempt to make a name change;

In order to verify the details on their account, the company must ask the customer to send customer care a photocopy or scan of one document from each of the categories listed below:

1) Personal Identification - one photo ID from the following list (valid for 6 months):
2) Current Signed passport
3) Current photo-card Driver's License (Provisional or Full)
4) Current Full Driver's License (old style paper version)
5) Current EU National Identify Card
6) Other recognized identity card such as an Armed Forces Identity Card
7) Norwegian credit cards with photo and ID number can be accepted as ID

Please note regarding some cards from Finland: It can be a debit card and credit card in one, number in the front is for Credit Card and number in the back for Debit Card usually.

Credit-numero etupuolella
Creditillä maksaessasi tarvitset allekirjoituspaneelin vieressä olevan kolminumeroisen tarkisteluvun.

Debit-numero kääntöpuolella

Address Verification - one of the following:

1) Utility bill (within last 3 months)
2) Current photo-card Driver's License (Provisional or Full) (Applies for UK DL's)
3) Current Full Driver's License (old style paper version)
4) ID card with address + Passport or additional ID
5) Bank/Credit Union/Building Society/Credit Card statement or passbook (within last 3 months)
6) Council tax bill or payment book (within last 3 months)
7) Recent mortgage statement (within last 3 months)
8) Current local council rent card or tenancy agreement (private tenancy agreements are not acceptable)
9) Home Insurance certificate or policy
10) Motor Insurance certificate or policy
11) Electoral roll
12) Credit reference agency
13) Mobile bills are not accepted

Source of Payment Verification/Proof of Payment - one of the following:

1) Company account registered Credit or Debit card
2) Copy of Credit or Debit card account statement of a card registered on with Company account (less than 3 months old)
3) Copy of bank statement - must have Company transaction or card number visible on it (less than 3 months old)

When requesting such documentation, the customer must always be informed that:

1) The card number must be blanked out leaving only the last four digits visible together with the start and expiry date.
2) The documents must be clear and legible.
3) The documents should show the residential address.

6.5 ENHANCED DUE DILIGENCE

Enhanced Due Diligence (EDD) is applied to business relationships that present a higher risk of money laundering or terrorist financing. EDD will be initiated where:

- The customer is identified as a Politically Exposed Person (PEP), or a close associate/family member;
- Lifetime deposits exceed EUR 50,000;
- The player resides in or is transacting from a jurisdiction flagged as high-risk by FATF or the GCB;
- Transactional or behavioural anomalies are identified through monitoring systems;
- Source of funds (SoF) and source of wealth (SoW) cannot be verified through initial documentation or soft checks.

Enhanced due diligence is achieved by the following processes:

If we have	Ask for
a utility bill	a bank statement
a bank statement	a utility bill
a passport	driver's license
driver's license	a passport
national ID	a passport

EDD Measures Include:

- Certification or notarization of identity and address documents;
- Additional proof of source of funds, including:
    - Payslips, employment contracts, tax returns;
    - Inheritance documentation, legal settlements, or donation deeds;
    - Bank statements indicating consistent income patterns;
- Cross-referencing with adverse media, sanctions, and open-source intelligence tools;
- Senior management approval prior to continuing or establishing the business relationship.

Failure to provide satisfactory EDD documentation within 7 working days will result in account suspension and notification to the Money Laundering Reporting Officer (MLRO) for further action.

6.6 PENDING WITHDRAWAL CANCELATION

KYC will be requested by the RPF Agents. A reminder will be sent to customers in 4 days. I**f no documents are received within 7 days from the initial KYC request, the customer's account will be closed. If no further communication is received the account will remain closed and the withdrawal will be cancelled.** The RPF Agents will also send an email to the customer, explaining the situation and letting them know that prior to opening account, we will need to receive the required KYC documents.

6.7 CLIENT REFUSING TO SEND DOCUMENTS

Any client who refuses to send documents will have their account disabled. CS will try to explain to the client the importance of receiving and verifying their documents, however if the client is still refusing to listen and will not send documents, the compliance department / MLRO will be notified. The MLRO will then review the clients account and communications and consider whether to submit an STR, providing all details and information as appropriate, if the MLRO decides not to submit an STR they need to include their reason/s in the suspicious register.

7 SOURCE OF WEALTH QUESTIONNAIRE/DOCUMENTATION

Customer due diligence is an ongoing process and as a result there are trigger events which warrant the collection of additional documentation. Upon classifying a player as High risk, as shown in sections 4 in the Risk Based Approach, the client will be requested to complete a Source of Wealth (SOW) questionnaire and if warranted the client will be asked to provide SOW documentation.

It is understood that the players may not have at hand the requested information thus the company has determined an acceptable timeframe of 7 days shall pass before we close the customer's account.

During this period, the players' account will remain operational however, no withdrawals will be processed.

8 MONITORING

8.1 DAILY MONITORING

A number of on-going monitoring checks are done on a daily basis that prevents fraudulent and/or unwanted clients.

8.2 SUSPICIOUS BEHAVIOR

Below provide some examples of what the Company considers suspicious in relation to a client's behaviour or transactions.

Suspicious Indicators:

- Information provided by the client contains a number of mismatches (e.g. email domain, telephone or postcode details do not correspond to the country);
- The registered credit card or bank account details do not match the client's registration details;
- The client tries to open multiple accounts under the same name;

- The client tries to open several accounts under different names using the same IP address;
- The source of funds being deposited appears to be suspicious and it is not possible to verify the origin of the funds; or
- The client has links to previously investigated accounts.

Suspicious Transactions:

- The client logs on to the account from multiple countries;
- Different clients are identified as sharing bank accounts from which deposits or withdrawals are made;
- E-wallets that are registered with different names

8.3 KYC DOCUMENTATION REVIEW

The below mentioned table depicts the manual trigger event based on KYC aging, warranting a player review (player interaction required) or desk top review (no player interaction review required).

Risk Rating	Frequency from date of last review or customer interaction.	Registered through conventional channel
High	Every 3 months or upon withdrawal	Check Identification document expiry date, collect new one where warranted and assess if an updated SOW document needs to be collected
Medium	Every 6 months	Check Identification document expiry date, collect new one where warranted and assess if an updated SOW document needs to be collected
Low	As triggered through the transaction monitoring process	Check Identification document expiry date, collect new one where warranted and assess if an updated SOW document needs to be collected

9 MONEY LAUNDERING REPORTING OFFICER

9.1 MLRO'S RESPONSIBILITIES

The Money Laundering Reporting Officer (MLRO) is responsible for overseeing the Company's full compliance with AML/CFT obligations under Curacao law and applicable international standards. The MLRO's responsibilities include:

- Ensuring timely filing of Suspicious Transaction Reports (STRs) with the FIU Curacao;
- Maintaining an up-to-date AML/CFT framework and risk assessments;
- Reviewing internal reports of suspicious behaviour and escalating them to regulatory authorities when warranted;
- Acting as the main point of contact with regulatory authorities;
- Ensuring timely and effective AML training for all staff members whose roles involve exposure to financial transactions or customer on boarding;
- Maintaining registers of PEPs, sanctioned individuals, STRs filed, and any internal AML/CFT decisions.

The MLRO is granted unrestricted access to all company systems, transaction logs, and customer records necessary to discharge their functions effectively and independently.

Name: XXXXXXXXXXXXXXXXXXX

Email: compliance@slott.com

9.2 SUSPICIOUS ACCOUNTS – INTERNAL REPORTING TO MLRO

All suspicious accounts are reported to MLRO internally and recorded in spreadsheet. The MLRO will then review the clients account and communications and consider whether to submit an STR, providing all details and information as appropriate. Where the MLRO decides not to submit an STR they need to include their reason/s in the suspicious register.

Spreadsheet location - Internal Suspicious Account report

9.3 INTERNAL FRAUD

To avoid possible internal fraud and unapproved withdrawals, for the sake of transparency. All internal withdrawals have to be logged and checked by two team members. Also email with the request of withdrawal have to be sent to (Email address)

9.4 STAFF TRAINING

The MLRO also keeps a record of all training conducted and given to employees in Money Laundering and Terrorist Financing Prevention Measures. These sessions are done yearly for all employees that fall under operations.

9.5 BUSINESS RELATIONS

The MLRO also keeps all KYC and EED of all Companies that conduction business with Leon. All checks are done before any business relationship is started and they are updated on a yearly basis

10 FUNDS MANAGEMENT

10.1 ACCEPTED PAYMENT METHODS

List of all payment methods

Deposits	**Withdrawals**

VISA/MasterCard Skrill Neteller Paysafecard by Skrill Mifinity (Klarna and others via this wallet) Ezeewallet Dimoco (mobile payments) Cashto2code Crypto payments Multibanco Mbway Astropay Onetouch – 200 Astropay India UPI – 200 Astropay India Google pay – 200 Astropay India PhonePe – 200 Astropay India Net Banking – 200 Netbanking via UPI – 500 Astropay India Airtel Money – 200 Astropay India FreeCharge – 200 Astropay India Jio Money – 200 Rupeepay (netbanking) – 200 Crypto payments - 5000 (depending on the cryptocurrency) Astropay India Ola Money	VISA/MasterCard Skrill Neteller Mifinity (Klarna and others via this wallet) Ezeewallet Inpay Crypto payments SEPA Astropay Onetouch Netbanking via UPI Rupeepay

10.2

All the funds deposited by the player or owned by the licensee shall be credited to the player's corresponding account.

10.3 DORMANT ACCOUNTS PROCEDURE

The Company has established the following procedure for identifying, managing, and reactivating dormant accounts, in accordance with AML/CFT obligations and regulatory expectations set by the Curaçao Gaming Control Board.

10.3.1 Definition

A dormant account is defined as a player account that has registered no login, deposit, wager, or withdrawal activity for a continuous period of **12 months**.

10.3.2 Monitoring and Notification

- A monthly internal review is conducted to flag accounts approaching dormancy.
- Players will be notified via email **30 days in advance** that their account will be classified as dormant unless activity is resumed.
- Once the account becomes dormant, a **monthly administrative fee of €0.25** may be applied, provided such fees are permitted under applicable laws.

10.3.3 Reactivation of Dormant Accounts

- A player may request account reactivation at any time.

- Reactivation is subject to **Customer Due Diligence (CDD)**, including:
    - Identity verification (valid ID and proof of address)
    - Review of historical account and transactional behavior
    - Screening against updated sanctions, PEP, and adverse media databases
- No withdrawals will be processed until the re-verification process is completed and approved.

10.3.4 AML Considerations

- Dormant accounts may pose a risk of being exploited during the layering or integration stages of money laundering.
- Upon reactivation, a **risk assessment** is conducted by the Compliance or Fraud team.
- Where warranted, **Enhanced Due Diligence (EDD)** may be applied.
- Any reactivation that raises red flags will be escalated to the **MLRO**. If deemed suspicious, an **STR will be filed with FIU Curaçao** in accordance with NORUT obligations.

10.3.5 Final Closure and Disposal of Funds

- If a dormant account remains inactive for **five (5) years**, and all reasonable efforts to contact the player have failed, the account may be closed.
- Remaining balances will be remitted to the **Regulator or other competent authority**, in line with legal requirements.
- All related records and audit trails shall be retained for a minimum of **five (5) years** after account closure.

10.4 THIRD-PARTY RISK MANAGEMENT

The Company recognises that engaging with third parties introduces potential risks related to money laundering, terrorist financing, fraud, and reputational harm. In line with its AML/CFT obligations, the Company has implemented a structured framework to assess, manage, and monitor these risks before and during the course of any business relationship.

10.4.1 Definition of Third Parties

A “third party” is any external person or entity that provides a product or service to the Company or acts on its behalf in a manner that may impact AML/CFT exposure. This includes, but is not limited to:

- Payment service providers (PSPs), banks, and payment processors;
- Game developers and content providers;
- Platform providers or white-label operators;
- Affiliates and marketing intermediaries;
- Software or technical service vendors;
- External consultants or introducers involved in onboarding or payment flows.

10.4.2 Third-Party Due Diligence (TPDD)

Prior to onboarding any third party, the Company conducts **Third-Party Due Diligence (TPDD)** to assess the nature and level of risk they pose. This includes:

- Collection and verification of corporate registration documents;
- Identification of **Ultimate Beneficial Owners (UBOs)**;
- Confirmation of regulatory status, licenses, and supervisory authorities (where applicable);
- Screening against **international sanctions**, **PEP lists**, and **adverse media**;
- Review of the third party’s AML/CFT policies and internal controls.

Each third party is assigned a **risk rating (Low, Medium, or High)**, based on their jurisdiction, role, exposure to player funds, and compliance track record.

10.4.3 Contractual Safeguards

All third-party relationships must be governed by a **written agreement** that includes the following clauses:

- Obligation to comply with AML/CFT laws, including applicable FATF Recommendations;
- Commitment to maintain robust internal controls and cooperate with regulatory inquiries;
- Right of the Company to request AML-related documentation and conduct compliance audits;
- Right to terminate the agreement immediately in cases of non-compliance, sanctions listing, or reputational damage.

10.4.4 Monitoring and Ongoing Oversight

The Company applies a **risk-based approach** to ongoing monitoring of third parties, including:

- **Annual re-verification** of corporate documents and ownership structure;
- Review of the third party's ongoing compliance performance;
- Monitoring of transaction activity and referral patterns where relevant (e.g. affiliates or PSPs);
- Immediate escalation to the MLRO of any unusual or suspicious conduct.

High-risk third parties may be subject to **Enhanced Due Diligence (EDD)**, periodic risk reviews, or approval by senior management before continuation of the relationship.

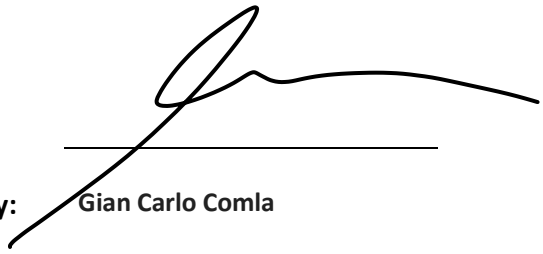
10.4.5 High-Risk Jurisdictions and Prohibited Relationships

The Company does not enter into or maintain relationships with third parties that:

- Operate from **FATF blacklisted jurisdictions**;
- Are subject to financial sanctions or have unresolved regulatory enforcement actions;
- Refuse to provide UBO information or sufficient AML documentation;
- Present unresolved compliance deficiencies or reputational risks.

10.4.6 Recordkeeping

The Company retains all third-party due diligence documentation, risk assessments, monitoring records, and relevant correspondence for a minimum of **five (5) years** from the date the relationship is terminated. These records are available to the **MLRO**, auditors, and competent authorities upon request.

Signature: 

Name of Signatory: **Gian Carlo Comla**

Date: 10th June 2025.