

# AML Policy and Procedures

*This Policy is amended and is in effect as of 1<sup>st</sup> day of June, 2025 and contains provisions applicable to the website of the company SHARKSCODE B.V.*

*(hereinafter referred to as the "Company" or "We").*

## Table of Contents

1. **AML MANAGEMENT OVERVIEW**
  - 1.1. **Introduction**
  - 1.2. **Management**
  - 1.3. **Risk-based approach**
  - 1.4. **Data processing system**
  - 1.5. **Staff Training**
2. **CUSTOMER ACCEPTANCE AND REGISTRATION POLICY**
  - 2.1. **Introduction**
  - 2.2. **Customer Acceptance**
  - 2.3. **Restrictions**
  - 2.4. **Information Entered on Registration**
  - 2.5. **Terms Acceptance**
  - 2.6. **Underage Customers**
  - 2.7. **Customer Due Diligence**
3. **CUSTOMER RISK SCORING AND PROFILING**
  - 3.1. **Introduction**
  - 3.2. **Customer Risk Assessment**
    - 3.2.1. Individual status
    - 3.2.2. Geographical location
    - 3.2.3. Gambling and transactional behaviour

3.2.4. Payment Methods

3.2.5. Fraud red flags

**3.3. Risk Score Calculation**

**3.4. Customer Due Diligence**

**3.5. Additional Details & Source of Funds/Wealth**

**3.6. Ongoing Monitoring**

**3.7. Withdrawals**

**4. CUSTOMER DUE DILIGENCE**

**4.1. Introduction**

**4.2. Standard Customer Due Diligence**

**4.3. Documents acceptance**

**4.4. Threshold approach**

**4.5. Ongoing monitoring**

**4.6. Enhanced Due Diligence**

**4.7. Simplified Due Diligence**

**4.8. Sanctions screening. Politically Exposed persons**

**4.9. Sanction screening Process**

**4.10. Third-party Service Providers**

**4.11. Account Closure Procedure**

**5. DEPOSIT AND WITHDRAWAL MANAGEMENT PROCEDURES**

**5.1. Player Account Balance**

**5.2. Payment Methods**

**5.3. Player Deposits**

**5.4. Player Withdrawals**

**5.5. Withdrawal Payouts**

**6. SUSPICIOUS ACTIVITY REPORTING**

- 6.1. Introduction**
- 6.2. Recognition of unusual transactions**
- 6.3. Red Flags Indicators**
- 6.4. Inability to Complete CDD Measures**
- 6.5. Internal Suspicious Activity Report**
- 6.6. External report to FIU**
- 6.7. Tipping-off**
- 7. INTERNAL CONTROL**
  - 7.1. Introduction**
  - 7.2. Record Keeping requirements**
  - 7.3. AML/CFT Compliance Officer**
  - 7.4. Employees background check**
  - 7.5. Training**
  - 7.6. Internal revision and staying up to date**
  - 7.7. Restricted Territories**

## History of Changes

| Version | Date       | Change details                                                                                                                                                                           | Author             | Approver |
|---------|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|----------|
| 1.0     | 23.12.2020 | Initial development                                                                                                                                                                      | Compliance Officer | Director |
| 2.0     | 01.09.2024 | Upgrade of the Policy from scratch to comply with the GCB Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction | Compliance Officer | Director |
| 3.0     | 29.05.2025 | Amendments throughout the Policy to comply with the GCB comments.                                                                                                                        | Compliance Officer | Director |
|         |            |                                                                                                                                                                                          |                    |          |

## Key Information

Approving Official(s): Director

Responsible Office: Compliance

Effective Date: December 23, 2020

Next Review Date: May 1, 2026

Policy URL: <https://slotscity.com/general-information/aml-crf-policy>

## 1. AML Management Overview

### 1.1. Introduction

Money laundering is the process of concealing, disguising, converting, transferring, or removing criminally derived 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 the 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 transactions 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 of terrorism.

The key differences between ML and TF are:

- For money laundering to occur, the funds involved must be the proceeds of criminal conduct.
- For terrorist financing to occur, the source of funds is irrelevant, i.e., the funds can be from a legitimate or illegitimate source.

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

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

## **1.2. Management**

SHARKSCODE B.V. (hereinafter – the Company) has designated AML/CFT Compliance Officer (hereinafter – CO) as an element of the AML/CFT Compliance Program.

CO, the key individual responsible for the prevention of money laundering and the financing of terrorism, is not involved in the operation activity and has overall responsibility for ongoing regulatory compliance and anti-money laundering procedures, namely:

- AML program
- Verification of compliance with law and policies and procedures
- Training employees
- Internal / external UTRs
- Management reporting.

In the Company, the CO is Oleksandr Zaitsev, who should be contacted via email [aml@sharkscore.com](mailto:aml@sharkscore.com) or mobile +38 093 225 02 36 concerning the AML Policy requests. The CO will report directly to the director.

CO, together with other senior management, 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 uses a hybrid approach in KYC procedures, using both electronic verification and verification by documents request.
- The Company assumes that most customers are not money launderers. However, it identifies players since it requires the Curaçao Gaming Control Board (GCB).
- 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.

This Policy applies to all Company's employees, contractors and senior management, to all customers registered with the <https://slotscity.com/> platform, all affiliates and third-party vendors involved in player acquisition or payment processing, and any partner or agents representing the Company in operational capacity.

## **1.3. 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 summarized 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 to the board and senior management.

### 1.4. 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:

- collecting information about all customers such as their first and last name, date of birth and residential address before the business relationship is established;
- identification and verification of all customers is carried out by third-party KYC software integrated into the website;
- politically exposed person (PeP) and sanction list checks are performed by third-party KYC software;
- transaction monitoring is managed by trained staff using relevant software;
- reporting all suspected money laundering cases and unusual transactions to the CO or his deputy for further reporting to the director and FIU.

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

### 1.5. 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 according to individual work specialization.

## 2. Customer Acceptance and Registration Policy

### 2.1. Introduction

Before gambling, depositing or placing real-money bets, the customer must register on the website and set up an account. Customers who do not register 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 make a deposit and play on a Company's website, a customer must first register on the website.

Registration is limited to individuals who are over eighteen years of age, and are non-residents of Curaçao.

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

## **2.3. Restrictions**

Not permitted to register on the website:

- Individuals under 18 years of age.
- Individuals from other countries than Curaçao.
- Individuals under Sanctions or listed in any blacklists.

Not allowed to make transactions and place bets:

- Existing customers who have an existing exclusion on the website.
- Individuals participating in national self-exclusion schemes.
- Individuals with fraud red flags.

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

## **2.4. Information Entered on Registration**

During the registration process, the customer provides identifying information and contact details:

- First Name and Last Name,
- Date of Birth,
- Gender,



- Address and country of residence,
- Email address and phone number,
- Currency that will be used on the website,
- Place of birth,
- Nationality,
- Identity number

## **2.5. Terms Acceptance**

During the registration process, the customer must also confirm acceptance of the website's general Terms and Conditions and its Privacy Policy.

## **2.6. Underage Customers**

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

## **2.7. Customer Due Diligence**

To complete registration the customer must pass Customer Due Diligence. The Customer Due Diligence (hereinafter - CDD) is conducted by the third-party service provider COMPLIGATE LIMITED (doing business as "KYCAID") as stated in more details in section 4.10 Third-Party Service Providers). If the CDD fails, 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 each customer 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 the GCB;
- Our own internal evaluation of our overall business risk assessment, and our knowledge and experience in dealing 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 categorized 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 behavior
- payment methods used by player
- fraud red flags triggered by the customer
- source of income and wealth of the customer

Customers identified as High Risk are subject to the EDD. Categories of customers whose activities may indicate a higher risk include:

- Customers who have multiple sources of income;
- Customers with irregular income;
- PEPs;
- High spenders (money can be derived from illegal activities);
- Disproportionate spenders (inconsistent with casino's information about customer's known source of income/assets);
- Casual customers like locals/tourists, especially when spending pattern changes;
- Improper use of third parties, criminals use third parties to gamble to break up large amount of cash, to buy chips or to cash out on behalf of others to avoid CDD measures;
- Multiple casino player rating accounts to hinder a casino to track their gambling activities;
- Unknown customers (redeeming large amounts of chips);
- Junkets (junket operators monitor player activity and issues and collect credit).

### **3.2.1. Individual status**

#### **Politically Exposed Person**

Politically Exposed Person (hereinafter referred to as the "PEP") means any person who has been entrusted with a high-ranking prominent public function at the international, European, or national level or who is or has been entrusted with a public position of comparable political importance below the national level.

Any new or existing customer that is found to be a PEP or family member or close associate are considered high level risk and will be subject to enhanced due diligence (EDD) measures.

### **Sanctions list**

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

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

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

### **Adverse media**

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

Any new or existing customer mentioned in adverse media will be a subject to 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 result in EDD measures being taken.

The Company takes into account a variety of sources of information produced by the FATF and non-governmental well-known bodies, including the following:

- Countries on the FATF list of High - Risk Jurisdictions subject to a Call for Action;
- Countries on the FATF list of Jurisdictions under Increased Monitoring;
- Countries on the CFATF Public Statement;
- Countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR);
- Countries on the European Commission's list of third countries having strategic deficiencies in their AML/CFT regime;
- Specially Designated Nationals (SDN) listed by the OFAC;
- Countries identified by credible sources as providing funding or support for terrorist activities or have terrorist organizations operating within them;
- Countries on the Corruption Perception Index compiled by Transparency International.

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 websites:

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

<https://ofac.treasury.gov/sanctions-programs-and-country-information>

The Company defines a High-Risk countries as follows: Afghanistan, Argentina, Barbados, Burkina Faso, Cameroon, Chile, China, Cuba, Democratic Republic of the Congo, Gibraltar, Haiti, Jamaica, India, Indonesia, Iran, Mali, Myanmar, Mozambique, Nigeria, North Korea, Panama, Philippines, Russia, Senegal, Syria, Tanzania, Trinidad and Tobago, Uganda, United Arab Emirates, Vanuatu, Vietnam, Venezuela, Yemen.

The Company defines jurisdictions under Increased Monitoring: Bulgaria, Croatia, Kenya, Monaco, Namibia, South Africa, Algeria, Barbados, Belarus, Bolivia, Brazil, Colombia, Ecuador, Egypt, Guatemala, Mexico, Pakistan, Paraguay, Peru, Thailand, Turkey, Turkmenistan.

### 3.2.3. Gambling and transactional behavior

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

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

If any examples of overt ML/FT behavior are observed, then an EDD measures must be undertaken immediately towards the customer.

### 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 and vouchers, traveler's checks, P2P transactions                | High        |

Manipulations with payment methods (e.g. deposits using one method, withdrawals using another) also considered as high-risk and not allowed by the Company.

### 3.2.5. Fraud red flags

The Company has an 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, etc. Some of the fraud red flags may also be related to money laundering.

If the Company becomes aware a player triggered a fraud red flag, it may lead to EDD measures being applied.

### 3.3. Risk Score Calculation

The purpose of this procedure is to identify minor incidents of ML/FT behavior that by themselves may not warrant suspicion but, if combined with other behaviors, can do so.

A player will be scored by the internal CMS system according to part of the factors above, and a risk score will be assigned.

Each factor will generate a score, and the overall risk score will be a sum of the individual scores. The more negative the score, the higher the risk.

Note that these factors, the scores and the thresholds are internal, and will be adjusted as we improve and update the RS Calculation.

| Indicator                    | Description                                                                                          | Score |
|------------------------------|------------------------------------------------------------------------------------------------------|-------|
| <b>Individual status</b>     |                                                                                                      |       |
| PEP                          | A customer considered to be PEP                                                                      | 50    |
| Adverse media                | A customer was mentioned in negative news or information the company discovered from various sources | 50    |
| Sanctions list               | A customer is under international sanctions                                                          | 50    |
| <b>Geographical location</b> |                                                                                                      |       |

|                                 |                                                                                                                |    |
|---------------------------------|----------------------------------------------------------------------------------------------------------------|----|
| Not at home                     | A customer whose IP location is different from Restricted territories                                          | 20 |
| High-risk country resident      | A customer resides in a High-risk country                                                                      | 30 |
| Restricted Territories resident | A customer is resident of Restricted Territories                                                               | 50 |
| <b>Gambling behaviour</b>       |                                                                                                                |    |
| Large sums no play              | A customer deposits large sums and then withdraws all their funds                                              | 50 |
| Large sums big losses           | A customer deposits large sums and repeatedly loses large sums as if the loss is of no consequence (5,000 NAF) | 50 |
| Low odds betting                | A customer repeatedly places bets on short odds (such as red/black on roulette or repeated bets on favorites)  | 25 |
| Big changes in money            | Dramatic changes in terms of volume and size of player deposits or staking activity                            | 20 |
| Multiple gaming accounts        | A customer is trying to set up multiple gaming accounts                                                        | 30 |
| <b>Transactional behavior</b>   |                                                                                                                |    |
| Smurfing                        | A customer makes multiple deposits or withdrawals of small amounts without no objective reasons                | 30 |

|                                             |                                                                                                                          |     |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|-----|
| Spending above wages and salaries           | The customer is spending money beyond their means                                                                        | 20  |
| No withdrawals                              | Player has never made a withdrawal request                                                                               | -20 |
| Withdrawal without playing                  | Money is deposited by a customer or held over a period and withdrawn by the customer without being used for placing bets | 30  |
| <b>Payment methods used by the player</b>   |                                                                                                                          |     |
| Card switching                              | A customer opens an account, uses several different cards and makes transfers between them                               | 20  |
| High risk payment methods                   | A customer uses high-risk payment methods                                                                                | 30  |
| <b>Fraud red flags a customer triggered</b> |                                                                                                                          |     |
| VPN                                         | Customer used a VPN                                                                                                      | 30  |

### 3.4. Customer Due Diligence

The level of customer due diligence (CDD) measures conducted on a player depends on the risk score assigned to the player as follows:

|                                     | Low | Medium | High |
|-------------------------------------|-----|--------|------|
| Verify ID and address with docs     | X   | X      | X    |
| Collect additional personal details | X   | X      | X    |

|                                                          |   |   |                        |
|----------------------------------------------------------|---|---|------------------------|
| Collect Source of Funds/ Wealth info                     |   | X | X (with documentation) |
| Ongoing monitoring                                       | X | X | X (Enhanced)           |
| Additional measures to address any other risk identified |   |   | X                      |
| Report suspected cases of ML/FT                          | X | X | X                      |

### 3.5. Additional Details & Source of Funds/Wealth

A daily report will be sent to the CO. 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:
  1. Checking what information the Company already have on them
  2. Checking open Internet sources
  3. Checking if they are in any way suspicious
2. The AML manager will then take appropriate action:
  1. Block account if needed
  2. Apply appropriate Customer Due Diligence measures
  3. Review the responses, correspondence with the support team, and the information provided by the player
  4. 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 the AML manager's approval before any withdrawal request can be processed.

All decisions made by the AML manager must be documented.

### 3.6. Ongoing Monitoring

The AML team will conduct ongoing 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 processed.

## **4. Customer Due Diligence**

### **4.1. Introduction**

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

The customer is obliged to cooperate concerning the fulfillment of the due diligence obligations. If the Company cannot undertake the due diligence measures, 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.
- risk assessment – identifying the level of risk for the Company to be used by this customer for ML / FT.

There are two verification methods the Company uses within the risk-based approach:

- Electronic verification – verifying the identity of the customer using information from reliable databases. Electronic verification is based on the 2+2 rule:
  - verifying an individual to an address by surname and forename on two separate databases, or

- verifying an individual to an address by surname and forename on one database & verifying an individual by forename, surname and date of birth.
- Documentary verification – verifying the identity of the customer using information from the documents provided by the customer.

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

- I. full name;
- II. permanent residential address;
- III. date of birth;
- IV. place of birth;
- V. nationality;
- VI. identity number;
- VII. photographic identification;
- VIII. phone number;
- IX. e-mail address;
- X. currency used;
- XI. payment method ownership;
- XII. IP address, Browser and Operating System information, geolocation details, etc.

### **4.3. Documents acceptance**

For ID, the Company requires 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
- birth certificate
- current photo card driving license
- residence permit issued by the Home Office
- firearms certificate or shotgun license
- council tax bill
- utility bill or statement that can, on a risk basis, be verified as true by the company that issued it, commonly by confirmation of a reference number, name

and address, or a certificate from a utilities supplier confirming an arrangement to pay services on pre-payment terms

- bank, building society or credit union statement or passbook containing current address that can, on a risk basis, be verified as true by the company that issued it, commonly by confirmation of a reference number, name and address - bank or credit cards alone will not be sufficient as these do not provide either residential address or date of birth.

The Company requires a single document for each fact about a customer. If the ID document includes the customer's address, then the document may be used either for ID or proof of address (POA).

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 can not be accepted.

#### **4.4. Threshold approach**

The Company can apply CDD measures in relation to any transaction, whether the transaction is executed in a single operation or in a series of operations which appear to be linked.

“Transaction” consists of the placing of a bet, including:

- making a deposit of funds required to take part in the online gambling process
- collection of winnings, including
  - withdrawal of funds deposited to take part in the online gambling process or
  - winnings arising from the placing bets with 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 placing of

bets or collection of winnings over a number of transactions in order to circumvent the C/EDD requirements.

For the purpose of the CDD triggered by the threshold, the Company applies both electronic and documentary verification using a risk-based approach.

The Company undertakes Customer Due Diligence measures when:

- a) players engage in financial transactions equal to or above Naf. 4,000, since the business relationship has been established;
- b) carrying out occasional transactions above the monetary equivalent of NAF. 4,000;
- c) there is a suspicion of money laundering or terrorist financing; or
- d) the casino has doubts about the veracity or adequacy of previously obtained customer identification data.

The threshold value is calculated in the Curaçao currency Netherlands Antilles Florin (NAF), also called Netherlands Antilles Guilder (NAG) and can be converted to the currencies provided on the website.

A transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount in excess of the monetary equivalent of NAF. 4,000.

The Company will identify the player, carry out a customer risk assessment and verify the identity of the player.

The CDD measures to be taken are as follows:

- a) Identifying the player and verifying that customer's identity using a reliable, independent source of documents, data or information;
- b) Identifying the ultimate beneficial owner (UBO), and taking reasonable measures to verify the identity of the UBO, so that the casino is sure it knows who the UBO is. For legal persons and legal arrangements this should include understanding the ownership and control structure of the customer;

Since the Naf. 4,000 threshold is reached, the player cannot deposit funds into the account or withdraw funds from the account until the verification process is completed. Besides, if the requested information and documentation is not received within 30 days from the moment the Naf. 4,000 threshold was met in order for the Company to complete the CDD, the Company has to terminate the business relationship with the customer and in case of presumption that money laundering or terrorist financing has taken place, report to the FIU.

## **4.5. Ongoing monitoring**

The general due diligence duties include the ongoing monitoring of the business relationship, namely:

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

- Questioning the data and information the Company has whenever inconsistencies with the customer profile or behavior 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.

#### **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;
- residents of higher risk geographic areas;
- products or transactions that might favor anonymity;
- 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 made the deposits,
- 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 CO.

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).

- Obtaining additional information on the customer, like occupation, previous address and information available through public databases, internet, etc.
- Establishing how the customer acquired their 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.
- Obtaining information on the reasons for intended or performed transactions;
- Obtaining the approval of senior management to commence or continue the business relationship.
- Ensure that deposits originate from payment methods and do not allow anonymity by requesting copies of bank statements or account statements.
- In the case of a PEP, gain a better understanding of the customer's reputation and/or role in public life and assess how this affects the level of risk associated with the business relationship.
- 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. Examples of source of funds include personal savings, employment, pension releases, share sales and dividends, property sales, gambling winnings, inheritances and gifts and compensation from legal rulings.

#### **4.7. Simplified Due Diligence**

In case of a low level of money laundering or terrorist financing risks, the Company can apply simplified due diligence measures in accordance with applicable legislative requirements.

Simplified CDD measures include:

- Obtaining the player's identity:
  - I. full name;
  - II. permanent residential address;
  - III. date of birth;
- Verifying the identity of the customer and the ultimate beneficial owner after the establishment of the business relationship.

#### **4.8. Sanctions screening. Politically Exposed persons**

The Company checks all new customers at the verification stage against the PEP and Sanctions databases. These service providers also regularly check the whole customer database every six months to ensure existing customers have not changed their status.

All players should be screened against sanctions lists of the UN and EU. Before doing business or performing an occasional transaction for the first time with a player, the Company ensures checking on published lists of known or suspected terrorists or other sanctioned persons or companies:

- U.S. Treasury's Office of Foreign Assets Control's Specially Designated Nationals (SDN) and Blocked Persons List, Human Readable Lists - <https://home.treasury.gov/>
- EU Sanctions List <http://www.sanctionsmap.eu/#/main>.
- For PEP status screening casinos can rely on internet search or consult reports and databases on corruption risk, like the Transparency International Corruption Perceptions Index or on [www.knowyourcountry.com](http://www.knowyourcountry.com)

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 CO who in turn will send a report to the senior management.

The CO will investigate each case to identify positive or false-positive PEP alerts. 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 CO will decide to reject registration or close the set up account and inform 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 organization.

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,
- both parents.

#### **4.9. Sanction screening process**

The Company will conduct the following screening process for each prospective User to identify whether they fall under certain categories of unwanted persons.

##### **Politically Exposed Persons**

A prospective User will be screened to identify whether he/she falls under the definition of a domestic and/or foreign Politically Exposed Person ("PEP"), Relative & Close Associate ("RCA"), and/or Head of International Organization ("HIO").



According to [FATF Guidance on Politically Exposed Persons \(Recommendations 12 and 22\)](#), PEP shall be defined as an individual who is or has been entrusted with a prominent public function. The position of PEP can be potentially abused for the purpose of committing Money Laundering, corruption, bribery, Terrorism Financing, and related unlawful actions. By screening the prospective Users, the Company implements a risk-based management system to detect such potential abuse if and when it occurs. Besides, the prospective Users will be screened to identify whether they fall under the category of a “close associate” of a PEP, or are their family members and, therefore, constitute high risk.

## Sanctions

The prospective Users are screened to identify whether they fall under certain sanctions lists. They include, but not limited by:

- [Interpol lists](#)
- [United Nations Security Council Consolidated List](#)
- [CIA world leaders](#)
- [Global PEP List](#)
- [Office of Foreign Assets Control \(OFAC\)](#)
- [Federal Bureau of Investigation \(FBI\)](#)
- [Denied Persons List with Denied US Export Privileges](#)
- [United States Drug Enforcement Administration](#)
- [Bureau of Industry and Security](#)
- [Europol](#)
- [European Securities and Markets Authority](#)
- [Ministry of Internal affairs of Ukraine lists](#)
- National Security Service of Ukraine black lists
- National Security and Defense Council of Ukraine
- Public register of politically exposed persons of Ukraine
- State migration service of Ukraine lists
- [Terrorists Lists](#)
- [Consolidated Canadian Autonomous Sanctions List](#)
- [SECO Switzerland Overall list of sanctioned individuals, entities and organizations](#)
- [Meghalaya Police](#)
- [Cambodia Police](#)
- Ludoman registry of Republic of Kazakhstan
- [New Zealand Police](#)
- [Polish Police](#)
- [The Insolvency Service](#)
- [National Crime Agency](#)
- [Consolidated list of financial sanctions targets in the UK](#)
- [Individual Insolvency Register](#)
- State authority of financial monitoring of Ukraine
- [Politically Exposed Persons \(PEPs\)- opensanctions.org](#)
- [Warrants and Criminal Entities- opensanctions.org](#)
- [OpenSanctions Default- opensanctions.org](#)
- [OCC Enforcement Actions](#)
- [WorldBank Debarred Provider](#)
- [African Development Bank Debarred Entities](#)
- [Asian Development Bank Sanctions](#)
- [UK Companies House Disqualified Directors](#)
- [Inter-American Development Bank Sanctions](#)
- [FBI Most Wanted](#)

- [UNOPS Vendor Sanctions](#)
- [Europe's most wanted fugitives](#)
- [NCA Most Wanted](#)
- [Consolidated Sanctions opensanctions.org](#)

Identification, verification of the client (its representative) is conducted based on the information and documents provided by the User. In case of doubts about the authenticity or completeness of the provided information about the User, the measures are taken to conduct an in-depth inspection of the User and clarify the information.

#### 4.10. Third-party Service Providers

The Company uses the following service providers for due diligence procedures:

- **COMPLIGATE LIMITED**, incorporated and registered in England with company number 15376538, whose registered office is at 85 Great Portland Street, First Floor, London, England, W1W 7LT, doing business as “KYCAID”. Services: Document verification, Facial verification, AML Screening, Tax ID check, Text recognition, Identity Check, Payment method ownership, Video verification, PEP and Sanctions screening, Additional Check.

#### 4.11. Account Closure Procedure

There are numerous reasons why the Company may close a customer’s account:

- Fraud
- Cheating
- Bonus Abuse
- Allowing a third person to use their account
- Setting up multiple accounts
- 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 CO will need to consider whether SAR was submitted as part of the concern about the player's behavior, or 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 or terminate the business relationship with the customer, the Company will:

- at the point where the threshold is reached, put all funds owed to the customer into an account from which no funds can be withdrawn
- further deposits can not be made to that account as long as it is locked until CDD is completed
- bets can be placed from the account but any winnings will be blocked until the CDD is completed
- once CDD is completed, the account will be unlocked and business continue as normal
- if CDD cannot be completed within 30 days since the specified threshold of transactions is reached, the Company will terminate the existing business relationship with the customer and close the account
- if funds are to be repaid, then the amount repaid should consist of all funds owed to the customer at the point when the threshold was reached, plus all deposits made at that point and thereafter
- funds should be refunded back to the originating account, and:
  - there should be appropriate risk mitigation
  - where it is suspected that the funds are the proceeds of crime, the Company will submit SARs to the FIU or seek a defense (appropriate consent) before refunding any of the funds
- if the refund is to be completed back to another account (whether partially or completely):
  - risk assessment must be done that should take into account information such as:
    - § multiple destinations – is the customer requesting that the money be sent to several bank accounts?
    - § high-risk destination – is the customer requesting that the money be returned to a country where there is a significant money laundering or terrorist financing concern?
- there should be an appropriate risk mitigation

- where it is known or suspected that the funds are the proceeds of crime, the Company submit SARs or seek a defense (appropriate consent) before refunding any of the funds
- there should be ongoing monitoring of the account and, if necessary, reporting of findings via relevant fraud monitoring services in the public and private sector.

## **5. Deposit and Withdrawal Management Procedures**

### **5.1. Player Account Balance**

Each player has a wallet with funds from which bets are deducted, and to which winnings are 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/her account by depositing through the cashier section on the website and then use these funds to place bets.

A player can withdraw available funds directly from their cash balance, but not from their bonus balance.

The Company does not provide credit to players.

A player can 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 deposit funds in CAD, EUR or cryptocurrency authorized on the website into their account through the cashier section.

The company offers deposit options via payment systems.

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 cash balance is able to request a withdrawal of the funds via the cashier section on the website.

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 cash 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 CO 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 CO 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 Curaçao (hereinafter – FIU).

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. The CO assesses all the circumstances and asks 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. Recognition of unusual transactions**

An unusual transaction is a transaction inconsistent with the player's profile.

It may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount of the monetary equivalent of NAf. 5,000.

The following transactions or intended transactions are deemed unusual:

- a) Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;
- b) Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- c) Transactions in the amount of NAf. 5,000 or more, regardless whether the transaction is made in cash, by check or other form of payment, or through electronic or other non- physical means. This includes but is not limited to:
  - 1) A cashless transaction in the amount of NAf. 5,000 or more. A cashless transaction is a transfer from a bank account of the casino to a local or international bank account, at the request of the client.

- 2) Accepting or releasing a deposit in the amount of NAf. 5,000 or more at the request of the client;
  - 3) Sale to a customer of chips in the amount of NAf. 5,000 or more. "Chips" include but are not limited to tokens and credits.
  - 4) A cash out in the amount of NAf. 5,000 or more;
- d) Presumed money laundering transactions or terrorist financing: Transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

### **6.3. Red Flags Indicators**

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

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 website.
- Customer places small bets, 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/she 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/she never deposited with.
- Customer opens an account and registers several different cards and, in fact, makes transfers between them,
- Customer deposits large sums, then places minimal bets, then withdraws all their funds,
- Customer deposits large amounts and repeatedly loses large amounts as if the loss is of no consequence.

### **6.4. 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.

## **6.5. 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 CO within 24 hours. All employees are expected to report suspicious transactions to the CO. 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 CO to determine if the information available may be considered as sufficient for filing a SAR with the FIU.

Internal SARs must be submitted to the CO's email – [aml@sharkscore.com](mailto:aml@sharkscore.com)

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 CO 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.

## **6.6. External report to FIU**

Once the CO has received an Internal SAR, she/he will complete relevant research within 10 working days and decide if a SAR should be submitted. If presumption of ML/TF exists, CO to report within 48 hours to the FIU.

When making this decision, the CO 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/TF, 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 CO 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 behavior, instances of chargebacks or identity fraud. For example, these may consist of common or related persons, common IP addresses etc.

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

- Who is involved?
- How are they involved?
- What is 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 are you suspicious or knowledgeable?
- 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 offense 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 defense (consent) from the NCA
- can, later, tell a customer that a transaction or activity was delayed because a report had been made under POCA or the Terrorism Act, unless law enforcement or the NCA agrees, or a court order is obtained permitting disclosure
- can tell the customer that law enforcement is conducting an investigation.



## **7. Internal Control**

### **7.1. Introduction**

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

### **7.2. Record keeping requirements**

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 (e.g. copies or records of the government issued documents like passport, identity card, driving licenses or similar documents)
- all records (receipts) relating to transactions, i.e., deposits made, winnings paid out or refunds to customer accounts (including the amounts and types of currency involved, if any),
- 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 NCA 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 training (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 CO 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 or the transaction was processed. 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. AML/CFT Compliance Officer**

The Company has appointed as Anti Money Laundering / Combat Financing of Terrorism Compliance Officer (CO):

Oleksandr Zaitsev, email – [aml@sharkscod.com](mailto:aml@sharkscod.com)

whose main responsibility is to review any internal reports of unusual or suspicious transactions, and where necessary to submit an SAR with the FIU. The CO is the main contact point for the FIU.

In order to ensure that the CO is able to fulfill his role effectively, the Company guarantee that:

- CO 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.
- CO has no conflicting responsibility which may pose a conflict of interest.
- CO is not involved in the operation activity.
- CO has sufficient time, resources and information to fulfill his responsibilities.
- CO has a right to create work assignments to relevant employees and take decisions regarding ML/TF prevention.

The CO and his 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 combat 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 and terrorist financing.
- Ensuring compliance with current AML/CFT regulations, and other relevant legislation.
- Ongoing monitoring of the Company's business activity to comply with the anti money laundering / combat financing of terrorism regulations.
- Ensuring CDD/EDD is undertaken.
- Suspicious activity risk assessment.
- The submission of SARs in appropriate cases.
- Contributing to the staff AML/CFT 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 CO activities to assess the risk situation of the Company and the measures taken and intended to implement the obligations under money laundering regulations.

The CO and his 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. Employees background check**

Prior to engaging employees, the Company will carry out relevant integrity checks (including checks for criminal records), 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 terrorism financing, 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 behavior 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 the 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.

#### **7.5. 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 finalized 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:

- Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction (May 15, 2024), Curacao;
- The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92);
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99);
- Regulation Indicators Unusual Transactions (N.G. 2015, no. 73);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National decree for general measures (N.G. 2015, no. 29);
- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- The provisions of the anti money laundering and combat the terrorist financing requirements;
- Staff personal obligations under the money laundering and terrorist financing requirements applicable internal reporting procedures;

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

## **7.6. Internal revision and staying up to date**

The Company has compiled its policies and procedures according to the requirements and guidance of the GCB. 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 GCB, FATF and joined relevant forums
- The Company periodically takes legal advice from the gambling consultants for AML/CFT 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.

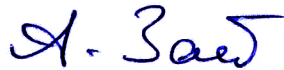
Any consequential update to the Terms and Conditions will trigger a pop-up notification to players on their next login where they will need to accept and agree to the new version before proceeding.

### **7.7. Restricted Territories**

The Company services are not provided to Customers located in Australia, Aruba, Bonaire, Curaçao, France, the Netherlands, Saba, Statia, St. Maarten, Singapore, Spain, the United Kingdom, the USA, all of the named Nations' Territories and Possessions and in the province of Ontario in Canada, Belarus, Russian Federation, the temporarily occupied territories of Donetsk and Luhansk regions of Ukraine.

Also the Company services are not provided to Customers located in Afghanistan, American Samoa, Barbados, Botswana, Burundi, Cambodia, Central African Republic, Cuba, Democratic People's Republic of Korea (DPRK) or North Korea, Democratic Republic of Congo, Fiji, Guam, Iran, Iraq, Lebanon, Libya, Mali, Myanmar (Burma), Nicaragua, Pakistan, Palau, Palestine, Samoa, Somalia, South Sudan, Sudan, Syria, The Crimea Region (Russia/Ukraine), Trinidad and Tobago, Uganda, Venezuela, Yemen, Zimbabwe and any other jurisdiction that the Central Government of Curaçao deems online gambling illegal. Customers the Company website is not allowed in territories with an undefined legal status.

The Policy is signed on this day May 29, 2025



---

Oleksandr Zaitsev,

CO of Sharkscod B.V.