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@sharkscode.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@sharkscode.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 August 20, 2024

Oleksandr Zaitsev,

CO of Sharkscode B.V.