

NATURAL NINE B.V.

ANTI-MONEY LAUNDERING POLICY

1. Introduction

Natural Nine B.V. (“Shuffle” or the “Company”) is a Curaçao company incorporated in 2022. It operates the online casino www.shuffle.com under Curaçao licence no. 8048/JAZ issued to Antillephone.

This policy (the “AML Policy”) sets out Shuffle’s approach to preventing and countering Money Laundering (“ML”) and Terrorist Financing (“TF”). In developing this policy, Shuffle has considered all current Anti-Money Laundering (“AML”) and Countering the Financing of Terrorism (“CFT”) obligations required under Curaçao law, as well as best practice guidance issued for the gaming sector. This policy has been created utilising guidance issued by the Curaçao Gaming Control Board.

Shuffle acknowledges that its products and services are at risk from individuals or groups seeking to launder criminal proceeds or facilitate funds designated for the financing of terrorism. As such, Shuffle is committed to fostering and promoting a compliance culture throughout the company which highlights the importance of preventing ML and TF.

2. Policy Statement and Objectives

Shuffle prohibits the use of its products and services for any form of illicit activity, including ML, TF and sanctions violations, and is committed to following global best practices in guarding against such use. Those best practices include:

- Adopting a written policy, and procedures and controls, reasonably designed to guard against ML, TF and sanctions violations;
- Designating a compliance officer to oversee the implementation of the policy, procedures and controls;
- Providing appropriate education and training to relevant personnel; and
- Conducting independent reviews, monitoring and maintenance of the policy, procedures and controls.

DS
CVR

DS
X

The objectives of this AML Policy are to set out the main procedures, systems, and controls Shuffle has implemented to follow the above best practices, and in particular to prevent and detect ML and TF.

3. Chief Compliance Officer

Shuffle has appointed a Chief Compliance Officer (“CCO”), who is responsible for coordinating the implementation of the AML Policy. The CCO’s duties also include developing AML initiatives, working with other stakeholders to revise the AML policy, assessing new regulatory requirements and investigating and reporting potentially suspicious or unusual activity.

The CCO has an independent and direct reporting line to the Board, and will act on his/her own authority. The CCO will be authorised to submit suspicious transaction reports (“STRs”) to the Financial Intelligence Unit of Curaçao (the “FIU”) without requiring approval to do so.

4. Responsibility of Employees, Directors and Officers

All of Shuffle’s employees, directors and officers, regardless of their position, are required to comply with this policy, and have a duty to be aware of the need to prevent ML and TF. Should they have reason to believe or suspect that any transaction, or potential transaction, could involve the proceeds of criminal conduct, they must report this to the CCO without delay. Failure to do so may result in disciplinary action.

As the business grows and the number of employees increases, Shuffle will ensure that employees are trained to identify and report suspicious activity. Shuffle will provide AML training to its employees on a regular basis.

5. Know-Your-Customer Measures and Transaction Monitoring

Shuffle recognises the risks it faces of being used for ML and TF and has implemented controls, policies and procedures which are proportionate and targeted to those risks. Shuffle applies appropriate know-your-customer (“KYC”) and ongoing monitoring measures to further the objectives of this AML Policy and as required by law.

DS
CVR

DS
X

5.1. KYC Measures

Shuffle has adopted risk-based Customer Due Diligence (“CDD”) processes to enable it to develop a customer risk profile. These processes involve collecting certain information on customers at the onboarding stage and also monitoring customer activity. Shuffle’s CDD includes the following measures:

- **Collecting Customer Information.** Shuffle will collect details on each customer to form a reasonable belief that it knows the identity of its customers. Shuffle may collect such details as a customer’s wallet address, name, address, country, date of birth, or postal code (collectively, “KYC Information”). Shuffle will collect any of the above KYC Information before issuing a Shuffle funding address (e.g., QR code) to customers. Shuffle does not presently allow customers who are non-natural persons. Shuffle may utilise a third-party service provider to help it to determine the validity of the information provided by customers.
- **Excluding and Geoblocking Prohibited Jurisdictions.** Customers are notified at onboarding that Shuffle does not offer services in jurisdictions where such services are not permitted to be offered (“Prohibited Jurisdictions”), and requires customers to declare that they are not located in a Prohibited Jurisdiction. Shuffle has implemented IP address-based geo-blocking of identified Prohibited Jurisdictions.
- **Excluding and Geoblocking Sanctioned Jurisdictions.** Customers are notified at onboarding that Shuffle does not offer services in jurisdictions subject to United States, European Union, or other global sanctions or watch lists, including Iran, Cuba, North Korea, Syria and the Crimean region of Ukraine (“Sanctioned Jurisdictions”), and requires customers to declare that they are not located in a Sanctioned Jurisdiction are not personally subject to international sanctions. Shuffle has implemented IP address-based geo-blocking of identified Sanctioned Jurisdictions.
- **Screening for Sanctioned Parties.** Before issuing a Shuffle funding address to a customer, Shuffle will screen a customer’s wallet address against applicable sanctions databases. Such screening measures rely on third-party blockchain forensics vendors such as Chainalysis.

5.2. Ongoing Monitoring

Shuffle performs ongoing monitoring of its customers in order to detect any behaviour or circumstances that might indicate ML or TF activity, sanctions breaches or other illicit activity. Shuffle has implemented a range of processes to help it achieve this goal:

- Transaction Monitoring for Sanctioned or Prohibited Jurisdictions.** Shuffle presently conducts a mixture of manual and automated transaction monitoring processes to identify “red flag” behaviour. Where such red flag behaviour is identified, Shuffle may refuse to process any withdrawal attempts or require additional information from the customer. Shuffle will further endeavour to limit any attempted customer account funding from Prohibited Jurisdictions where the associated wallet address indicates that the customer or the customer’s funds are located in such a Prohibited Jurisdiction. For instance, Shuffle may prohibit a customer from funding their Shuffle account using a known U.S.-based exchange wallet, as this may indicate that the customer is a U.S. person. Customers will have the ability to rebut any suspension with additional information as part of Shuffle’s ongoing transaction monitoring and customer due diligence standards.
- Transaction Monitoring for Sanctioned Parties.** Shuffle will periodically re-screen customers’ wallet addresses against applicable sanctions databases.
- Identification of Unusual Activity.** Shuffle will monitor account activity for unusual size, volume, pattern or type of transactions, taking into account risk factors and any other red flags. Monitoring will be conducted running regular reports of unusual, high-risk, or suspicious customer activity.
- Anti-Mixing Measures.** Shuffle does not allow the use of anonymity-enhancing technologies such as mixers, tumblers, or certain coins and tokens. Where Shuffle becomes aware that an anonymity-enhancing technology is being used on the Shuffle platform, Shuffle will disallow such use. Shuffle may also take steps to address suspicious deposit or withdrawal patterns; such instances will be dealt with on a case-by-case basis, depending on the perceived level of risk.
- Chainalysis Review.** Each crypto deposit and withdrawal will be run through Chainalysis and reviewed for signs of fraud or suspicious behaviour. A customer’s

account will be suspended and reviewed upon alert of potential illicit behaviour. Sufficient proof of wealth may be requested from high-risk accounts. Shuffle may refuse to withdraw to certain “high-risk” addresses as determined in consultation with Chainalysis risk scoring.

- **Withdrawal Threshold KYC.** Additionally, and independently, any account’s withdrawal function may be suspended until adequate due diligence has been carried out once that account has reached a withdrawal threshold dependent on the account’s risk characterisation over the life of the account, assessed according to Shuffle’s sole discretion.
- **Ban Evasion Detection.** Shuffle will utilise third-party service providers to detect the use by one customer of multiple accounts, in breach of Shuffle’s terms of service. Shuffle further prohibits peer-to-peer account transfers within the Shuffle platform infrastructure. Any attempts to circumvent this restriction will be treated as a red flag.
- **Time Zone Monitoring.** Shuffle has implemented time zone controls which check customers’ device location information against restricted jurisdictions to determine whether they are trying to use software to mask their true location.
- **Vendor Management.** Shuffle will periodically assess the strength of its key third-party service providers to determine whether additional services are needed, the third-party service provider is not performing in accordance with its contractual obligations, or if other remedial action is necessary for Shuffle to comply with this AML Policy. Shuffle may request information from any third-party service provider as part of its vendor review process.
- **Compliance Innovation.** In addition to vendor management, Shuffle will continuously monitor any non-documentary compliance mechanisms to determine whether their use on the Shuffle platform would be viable. Shuffle may run test or trial mechanisms on a limited basis with such compliance vendors to determine their effectiveness. Blockchain-native compliance tools may include fraud prevention services, on-chain KYC providers, and other tools designed to reflect the technological features associated with blockchain platforms.

DS
CVR

DS
X

5.3. Enhanced Due Diligence

Whenever a red flag is triggered, the relevant customer's account will be suspended and Shuffle will perform enhanced due diligence ("**EDD**"). EDD may include, but is not limited to, requiring customers to provide their:

- Full legal name;
- Country of citizenship;
- Permanent address (which must be a residential or business street address);
- Identification number (a passport number and country of issuance, a taxpayer identification number, an alien identification card number or number and country of issuance of another government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard);
- Government-issued identification document (e.g. a passport); and
- Source of funds and source of wealth.
- Shuffle may use third-party service providers to verify any of the above information.

5.4. Blocking of Customers

Shuffle will not onboard / will block or suspend customers who:

- Do not provide the identification information requested by Shuffle;
- Provide fake identification documents;
- Adopt measures to conceal their true location;
- Are from restricted or prohibited jurisdictions;
- Are subjected to United States, European Union, or other global sanctions or watch lists;
- Are addicted to gambling or have mental health issues; or
- Deposit funds which originate from exchanges in restricted jurisdictions.

In addition, Shuffle reserves the right to block and suspend players for any other reason at its sole discretion.

DS
CVR

DS
X

6. Reporting

If a customer is identified as being on a sanctions list, or linked to ML or TF or other criminal activities, Shuffle will make an appropriate report to the FIU.

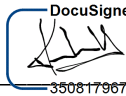
Accepted by:

Signatures:

Names:

Titles:

Date:

DocuSigned by:

3508179679034CB...

DocuSigned by:

E9G1A4A3F74E4ED...

Christopher van Rosberg and Lorenza Godett

Directors obo Xecutive Corporate Management B.V.

4/9/2024