

NATURAL NINE B.V.

ANTI-MONEY LAUNDERING POLICY

Key Information:

Approving Official(s):	Analissa Heiland and Lorenza Godett Directors obo Xecutive Corporate Management B.V.
Version:	2.0 14 December 2025

ANTI-MONEY LAUNDERING POLICY

1. Introduction

Natural Nine B.V. (“Shuffle.com” or the “Company”) is operated by Natural Nine B.V., a company incorporated under the laws of Curaçao with Company Number 160998 and licensed by the Curaçao Gaming Authority to offer games of chance under license number OGL/2024/1337/0628 in accordance with the National Ordinance on Games of Chance (Landsverordening op de kansspelen, P.B. 2024, no. 157).

The license was granted on 16/10/2024 and its current status is Active.

This Anti-Money Laundering Policy (the “AML Policy”) outlines Shuffle’s approach to preventing and countering Money Laundering (“ML”) and Terrorist Financing (“TF”). In developing this policy, Shuffle has considered all current AML and Countering the Financing of Terrorism (“CFT”) obligations required under Curaçao law and 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 to facilitate funds designated for the financing of terrorism. The Company is committed to fostering and promoting a culture of compliance throughout the organisation and emphasising the importance of preventing ML and TF.

2. Policy Statement and Objectives

Shuffle prohibits using its products and services for illicit activity, including ML, TF and sanctions violations. It is committed to following global best practices to mitigate such risks. These practices include:

Adopting written policies, procedures and controls designed to prevent ML, TF and sanctions violations;

- Designating a Compliance Officer to oversee the implementation of these policies, procedures and controls;
- Providing appropriate education and training to relevant personnel; and
- Conducting independent reviews, monitoring, and maintaining the policy, procedures and controls.

This AML Policy aims to define the key procedures, systems and controls that Shuffle has implemented to uphold the above standards, particularly to prevent and detect ML and TF. The effectiveness of this AML Policy and related controls shall be subject to independent compliance assessment periodically, with material findings reported to the Board and remedial actions implemented as necessary.

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 include developing AML initiatives, collaborating with stakeholders to revise the policy, assessing new regulatory requirements, and reporting potentially suspicious or unusual activity.

The CCO has an independent and direct reporting line to the Board and is empowered to act with their authority. The CCO is authorised to submit Suspicious Transaction Reports (“STRs”) to the Financial Intelligence Unit of Curaçao (the “FIU”) without requiring prior approval.

4. Responsibility of Employees, Directors and Officers

All of Shuffle’s employees, directors, and officers are required to comply with this policy and have a duty to remain vigilant regarding the prevention of ML and TF. If they have reason to believe or suspect that any transaction or potential transaction may involve criminal proceeds, they must immediately report this to the CCO. Failure to report may result in disciplinary action. In addition, prior to employment, all personnel undergoes appropriate background screening, including verification of identity, employment history and criminal record checks where legally permissible.

Shuffle will ensure employees receive training to identify and report suspicious activity as the business grows. AML training will be provided regularly. Shuffle provides comprehensive training programs to all its personnel as part of its commitment to maintaining strong ethical standards and ensuring full compliance with applicable regulatory requirements. The Company will maintain records of all AML training sessions, including attendance, materials covered, and assessments completed.

5. Risk Assessment

5.1. Business Risk Assessment (BRA)

The basis for the risk-based approach is the risk assessment which Shuffle must carry out of its own operation.

Shuffle carries out a business risk assessment to identify the ML/TF risks that it is exposed to and ensure that the policies, controls and procedures adopted are adequate to prevent and mitigate those risks. The risk assessment addresses the ways in which Shuffle’s products and services could be used to launder money, finance terrorism and finance proliferation, and the extent of the risk that this will happen. The end result is to assign risk ratings (low, medium, high) based on specific factors. All factors that may have an impact

on the risks of money laundering, financing of terrorism and financing of proliferation shall be taken into account in the risk assessment, but special consideration is given to the type of customers, products and services offered, delivery channels and geographical risk factors.

Shuffle shall also revise its business risk assessment whenever there are changes to the environment within which it operates and within its business activities, such as introduction of new games or regulatory changes. In the absence of changes, Shuffle shall assess its business risk at least once a year, to evaluate whether any changes thereto are necessary.

This risk assessment will be documented and approved by the Board. It should also be made available to the GCB upon request. All aspects of the Business Risk Assessment should be covered, including:

- The methodology adapted;
- The reasons for considering a risk factor as presenting a low, medium or high risk;
- The outcome of the BRA;
- Any information sources used.

5.2. Customer Risk Assessment (CRA)

The customer specific risk assessment shall be carried out either prior to the carrying out of an occasional transaction, or during establishing a business relationship. This initial customer-specific risk assessment shall also be revised at a later stage of the business relationship and this may result in a customer's risk rating having to be adjusted.

The Customer Risk Assessment will assess the risks Shuffle will be exposed to when providing its services or products to customers. The information collected to draw up the CRA will formulate the customer's risk profile.

6. Know-Your-Customer Measures and Transaction Monitoring

Shuffle recognises the risks of ML and TF and has implemented proportionate controls, policies, and procedures to mitigate these risks. It applies appropriate Know-Your-Customer ("KYC") and ongoing monitoring measures to further this AML Policy's objectives and comply with legal obligations.

6.1. KYC Measures

Shuffle has adopted risk-based Customer Due Diligence ("CDD") processes to create customer risk profiles. These processes involve collecting specific information at the

onboarding stage and monitoring customer activity.

Full CDD measures, including identity verification, may be undertaken required when:

- Customers engage in financial transactions equal to or above applicable thresholds described by law (such as NAf4,000);
- Carrying out occasional transactions above the monetary equivalent threshold described by law;
- There is a suspicion of money laundering or terrorist financing; or
- They have doubts about the veracity or adequacy of previously obtained customer identification data.

CDD measures include:

- **Collecting Customer Information:** Shuffle collects details such as wallet address, name, country, date of birth, and postal code ("KYC Information") before issuing a Shuffle funding address (e.g., QR code). Only natural persons are permitted. Third-party providers may be used to verify customer information.
- **Excluding and Geoblocking Prohibited Jurisdictions:** Customers must declare that they are not in jurisdictions where Shuffle's services are prohibited. IP-based geoblocking is enforced.
- **Excluding and Geoblocking Sanctioned Jurisdictions:** Shuffle blocks customers from jurisdictions under international sanctions (e.g. Iran, Cuba, North Korea, Syria, Crimea). Declarations and IP-based controls are used to enforce this.
- **Screening for Sanctioned Parties:** Wallet addresses are screened using third-party blockchain forensics services such as Chainalysis.
- **Screening for Politically Exposed Persons ("PEPs"):** Shuffle screens customers that have submitted KYC Information to identify PEPs (individuals holding or having held prominent public functions, their immediate family members, and known close associates) and the risk category of the PEP. Enhanced Due Diligence measures are applied to PEPs relative to their risk category, including obtaining senior management approval to service the PEP, account flagging, reasonable measures to establish source of wealth and source of funds and enhanced ongoing monitoring of the relationship and customer activities.

6.2. Ongoing Monitoring

Shuffle monitors customers for behaviours indicative of ML, TF, sanctions breaches, or other illicit activities through:

- **Monitoring Transactions from Prohibited Jurisdictions:** Automated/manual monitoring identifies red flags. Transactions from or associated with prohibited jurisdictions may be declined. Additional information may be requested to rebut suspicions.
- **Sanctioned Party Screening:** Ongoing re-screening of wallet addresses against sanctions databases.
- **Identification of Unusual Activity:** Patterns of unusual size, volume, or behaviour are flagged and investigated.
- **Anti-Mixing Measures:** Mixers, tumblers, or anonymity-enhancing coins/tokens are prohibited.
- **Chainalysis Review:** All deposits and withdrawals are analysed. Suspicious activity

may lead to suspension and requests for proof of wealth.

- **Withdrawal Threshold KYC:** Accounts reaching certain withdrawal thresholds may be paused pending further due diligence.
- **Ban Evasion Detection:** Third-party tools identify multiple accounts by the same user. Peer-to-peer transfers are prohibited, and circumvention attempts are flagged.
- **Time Zone Monitoring:** Device time zones are checked against IP data to detect attempts to mask location.
- **Vendor Management:** Periodic reviews of third-party providers are conducted to assess performance and compliance.
- **Compliance Innovation:** Non-documentary compliance technologies (e.g. on-chain KYC, fraud detection tools) are evaluated and trialled appropriately.

6.3. Enhanced Due Diligence (EDD)

When red flags are triggered, accounts are suspended, and Shuffle conducts EDD, which may include collecting:

- Full legal name;
- Country of citizenship;
- Permanent (residential or business) address;
- Identification number (e.g., passport or tax ID);
- Government-issued identification;
- Source of funds and wealth.

Third-party providers may be used to verify this information.

6.4. Blocking of Customers

Shuffle will block or suspend customers who:

- Fail to provide requested identification;
- Provide false documents;
- Conceal their actual location;
- Are from restricted/prohibited jurisdictions;
- Appear on global sanctions/watch lists;
- Exhibit signs of problem gambling or mental health issues;
- Deposit from exchanges in restricted jurisdictions.

Shuffle reserves the right to suspend players for any other reason at its sole discretion.

6.5. Record Retention

Shuffle maintains all records relating to customer identification, transaction data, risk assessments, and suspicious transaction reports for a minimum period of five (5) years following the termination of the business relationship or completion of the transaction. Records shall be maintained in a manner that allows them to be provided promptly to competent authorities upon request.

7. Reporting

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

7.1. Unusual Transaction Indicators

An unusual transaction is any transaction that deviates from normal patterns or lacks apparent economic or lawful purpose. Shuffle identifies unusual transactions using both objective and subjective indicators:

Examples of Objective Indicators include:

- Transactions at or above certain monetary thresholds (such as USD100,000) or as otherwise described in applicable laws and regulations;
- Unusual rapid movement of funds (deposit and immediate withdrawal with minimal play);
- High-value transactions inconsistent with customer profile (such as deposits greater than 10 times the customer's historical average);
- Use of multiple accounts or structured transactions to avoid thresholds;
- Wallet addresses flagged by blockchain analytics tools.

Examples of Subjective Indicators include:

- Customer reluctance to provide identification or source of funds;
- Transactions that appear inconsistent with the customer's stated occupation or income;
- Unusual patterns of play or betting behavior;
- Customer behavior suggesting knowledge of reporting requirements;
- Any other circumstances that raise suspicion based on employee judgment and experience.

When appropriate, unusual transactions are (a) documented, (b) investigated by the CCO and/or (c) reported to the FIU as Suspicious Activity Reports.

8. Independent Audit Function

Shuffle's AML compliance program is monitored and evaluated at least annually by an adequately resourced internal audit department or an outside independent party.

The audit must be independent and performed by people not involved with Shuffle's AML compliance staff. Those performing the audit are sufficiently qualified to ensure that their findings and conclusions are reliable.

These tests include at least:

- An evaluation of Shuffle's anti-money laundering, counter terrorist financing and counter financing of proliferation manuals;
- Customer's file review;
- Compliance management;
- Performance of transaction testing;
- Assessment of training adequacy;
- Assessment of compliance with applicable laws and regulations;

- Evaluation of Shuffle's personnel ability to identify unusual activity;
- Interviews with employees who handle transactions and with their supervisors;
- A sampling of unusual transactions on and beyond the threshold(s) followed by a review of compliance with the internal and external policies and reporting requirements; and
- An assessment of the adequacy of the record retention system.

The scope of the testing and the testing results must be documented, with any deficiencies reported to senior management and/or the Board, and to the designated officers with a request to take prompt corrective actions by a certain deadline.

These corrective actions could also include enhancement of controls and procedures.

APPENDIX A - Definitions

Politically Exposed Persons (PEP)

Natural persons, currently or previously entrusted with a prominent public function include:

- Head of state, heads of government, ministers and deputy of assistant ministers
- Members of parliament or of similar legislative bodies;
- Members of the governing bodies of political parties;
- Members of supreme courts, of constitutional courts or of other high- level judicial bodies, the decision of which are not subject to further appeal, except in exceptional circumstances;
- Members of courts of auditors or of the boards of central banks;
- Ambassadors, charges d'affaires and high-risk ranking officers in the armed forces;
- members of the administration, management or supervisory bodies of State-owned enterprises;
- Directors, deputy directors and members of the board or equivalent function of an international organization.

Natural persons considered family members of politically exposed persons by way of their close relations:

- The spouse, or a person considered to be equivalent to a spouse
- The children and their spouses, or persons considered to be equivalent to a spouse
- The parents of a politically exposed person.

Natural persons known to be close associates with politically exposed persons include:

- Any natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements.
- Any other close business relations, with a politically exposed person and natural persons who have sole beneficial ownership of a legal entity.
- Any person holding a legal arrangement which is known to have been set up for the de facto benefit of a politically person.

Suspicious and/or Unusual Transaction

A transaction that matches the indicators set forth by Ministerial Decree No. 73 of 2015.