

AML/CFT Policy – Dragon Money N.V.

Approving Official(s):

This policy was reviewed and approved by the Compliance Officer (MLRO) on behalf of senior management.

Name: Veremiienko Kateryna

Title: Compliance Officer (MLRO)

Date: July 3, 2025

Signature: _____



Responsible Office: Compliance Department (AML Compliance Officer)

Effective Date: April 10, 2025

Next Review Date: April 10, 2026

Policy Version: 2.0

1. Policy Statement

Dragon Money N.V. is fully committed to preventing money laundering and terrorist financing in all aspects of its operations. This Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Policy establishes the framework of principles, mechanisms, and internal controls that Dragon Money N.V. follows to ensure compliance with all applicable laws and regulations, and to protect the integrity of its services. We maintain a zero-tolerance stance toward the misuse of our platform for illicit activities. This policy applies to all employees, management, and relevant third-party partners of Dragon Money N.V., and covers all products and services offered to our customers (players) worldwide.

2. Purpose

The purpose of this policy is to outline the measures and procedures implemented by Dragon Money N.V. to detect and prevent money laundering, terrorist financing, and related illegal activities. It provides a clear directive to staff and stakeholders on their obligations under this policy. In particular, this document ensures that Dragon Money N.V. meets or exceeds the requirements of the Curaçao Gaming Control Board and the Curaçao Gaming Authority (CGA), as well as international standards (e.g. EU AML Directives and FATF Recommendations). By adhering to this policy, Dragon Money N.V. safeguards its operations from abuse, protects its reputation, and complies with all legal and regulatory obligations, including the prevention of the financing of terrorism and proliferation of weapons of mass destruction. Ultimately, the policy's goal is to maintain the highest level of security and integrity for our platform and our customers.

3. Audience

This policy is applicable to all personnel of Dragon Money N.V., including full-time and part-time employees, management, and any contractors or agents involved in our gaming operations. All departments (such as customer support, finance, security, and compliance) must adhere to the procedures and controls set forth in this policy. Additionally, third-party service providers who assist in customer due diligence or payment processing are expected to comply with the relevant portions of this policy and with Dragon Money's AML/CFT standards. Every individual with responsibilities under this policy is obligated to understand and follow it; failure to do so may result in disciplinary action and other consequences as outlined in this document.

4. Definitions

For the purposes of this policy, the following key terms are defined:

• Money Laundering (ML):

The process by which criminals conceal or disguise the origins of illicit funds (proceeds of crime) by introducing them into the legitimate financial or gaming system, making the funds appear lawful. Money laundering is understood to include:

- Conversion or transfer of property, knowing it is derived from criminal activity, for the purpose of concealing its illicit origin or helping someone evade legal consequences of their actions.
- Concealment or disguise of the true nature, source, location, disposition, movement, or ownership of property, knowing it is derived from criminal activity.
- Acquisition, possession or use of property, knowing at the time of receipt that it was derived from criminal activity.
- Participation in, association with, or conspiracy to commit, attempts to commit, or aiding, abetting, facilitating, or counseling the commission of any of the above actions.

Note: Money laundering is considered an offense even if the predicate offense (the crime generating the illicit funds) was committed outside of Curaçao.

• Terrorist Financing (TF):

The act of providing, collecting, or using funds, from either legal or illegal sources, with the knowledge that they will be used to support terrorist acts or organizations. Terrorist financing includes the financing of terrorist acts, terrorists, and terrorist organizations as defined by international conventions and local laws.

• Politically Exposed Person (PEP):

An individual who holds or has held a prominent public function, such as a government official, politician, senior executive of a state-owned corporation, judicial or military official, or an immediate family member or close associate of such a person. PEPs are considered higher-risk customers due to the potential for their position to be abused for money laundering or bribery, and thus require enhanced due diligence (see Section 5.4).

• Beneficial Owner (BO):

The natural person(s) who ultimately owns or controls a customer, or the person on whose behalf a transaction is conducted. In the context of a legal entity (e.g. a company or trust), a beneficial owner is the individual who directly or indirectly owns or controls 25% or more of the entity's shares or voting rights, or otherwise exercises effective control. If no individual meets this threshold, any senior managing official may be considered the beneficial owner for due diligence purposes.

- **Unusual Transaction:**

A transaction or activity that is inconsistent with a customer's known profile or that has no apparent economic or lawful purpose, raising suspicion of potential money laundering or terrorist financing. Indicators of unusual transactions can be objective (e.g., transactions exceeding certain monetary thresholds) or subjective (transactions that are out-of-character for a given customer). Unusual transactions must be investigated and, if deemed suspicious, reported to the authorities as required by law (see Section 5.7).

- **FIU:**

The Financial Intelligence Unit of Curaçao, which is the government agency responsible for receiving and analyzing reports of unusual or suspicious transactions (often referred to as the Meldpunt Ongebruikelijke Transacties, or MOT, under the National Ordinance for the Reporting of Unusual Transactions). Dragon Money N.V. is legally required to report any unusual transaction to the FIU without delay.

- **CDD:**

Customer Due Diligence, which refers to the process of identifying and verifying the identity of customers (players) and assessing their risk profile. CDD measures range from basic Know Your Customer (KYC) identification steps to Enhanced Due Diligence (EDD) for higher-risk scenarios. CDD includes understanding the purpose of the business relationship and, when applicable, identifying the beneficial owner of accounts.

- **EDD:**

Enhanced Due Diligence, which involves additional measures beyond standard CDD for customers who present higher risk of money laundering or terrorist financing (e.g., high-volume transactions, PEPs, high-risk countries). EDD may include obtaining more detailed information about the customer's source of wealth, closer monitoring of transactions, and senior management approval to continue the relationship.

(Additional relevant terms and acronyms used in this policy are explained in context below. Dragon Money N.V. adheres to definitions as per the applicable Curaçao legislation and international standards.)

5. Policy Implementation

This section outlines the specific policies, controls, and procedures that Dragon Money N.V. has implemented to prevent and mitigate the risks of money laundering and terrorist financing. Our AML/CFT program is risk-based, meaning resources and scrutiny are aligned with the levels of risk identified through formal assessments. Key components of our implementation strategy include periodic risk assessments, a multi-tiered customer due diligence process, ongoing monitoring of customer activity, reliance on trusted third parties where appropriate, strict reporting

protocols, and a comprehensive compliance program encompassing training, record-keeping, and independent audit.

5.1 Business Risk Assessment (BRA)

Dragon Money N.V. maintains a documented Business Risk Assessment (BRA) that is reviewed and updated at least annually and approved by the Board of Directors (general management). The BRA identifies and evaluates the money laundering (ML) and terrorist financing (TF) risks inherent to our business. This assessment covers the nature of our products and services, the types of customers (players) we serve, the geographical regions of our customer base, the payment methods and delivery channels we use, and any other relevant factors (including emerging risks such as those associated with new technologies). By analyzing how our online casino platform and games could potentially be misused to launder funds or finance terrorism/proliferation, the BRA ensures that our policies, procedures, and controls are appropriately designed to mitigate those risks.

Key outcomes of the BRA:

- Identification of areas of higher risk (e.g. certain products, transaction types, or customer segments) so that enhanced controls can be applied.
- Confirmation that existing controls are adequate for low- and medium-risk areas, or recommendations for improvements where gaps are found.
- Documentation of risk appetite and risk tolerance levels, aligned with regulatory expectations and industry best practices.

(Dragon Money N.V. will provide its BRA documentation to the Curaçao Gaming Control Board or other competent authorities upon request. The BRA process ensures continuous improvement of our AML/CFT measures in light of the evolving risk environment.)

5.2 Customer Risk Assessment (CRA)

For each customer (player), Dragon Money N.V. conducts a Customer Risk Assessment (CRA) at the start of the business relationship (onboarding) and updates it as necessary. The CRA evaluates the specific risk level associated with the customer, taking into account factors such as the customer's nationality and country of residence, occupation, financial profile, source of funds, and intended gaming activity. Based on the information collected, each customer is assigned a risk category (e.g., low, medium, or high risk). This risk profile determines the depth of due diligence to be applied (see Section 5.4) and the level of ongoing monitoring required (Section 5.5).

- Low-Risk Customers: Those whose attributes and behavior present minimal indications of ML/TF risk (e.g., local players with small, routine transactions) may qualify for simplified due diligence measures, in line with permitted regulatory exceptions.
- Medium-Risk Customers: Customers with some risk indicators (e.g., higher transaction volumes or from jurisdictions with some risk factors) undergo standard due diligence, including identity verification and monitoring.
- High-Risk Customers: Those who present significant risk factors (e.g., Politically Exposed Persons, customers from high-risk jurisdictions, or customers with large or complex transaction patterns) are subject to Enhanced Due Diligence (EDD) as described in Section 5.4.3.

The CRA process is critical in formulating an appropriate customer due diligence approach. It is done before or during account opening and updated whenever a customer's risk factors change (for example, if a customer's transaction behavior escalates or if new adverse information arises). By tailoring CDD efforts to the customer's risk level, Dragon Money ensures effective allocation of resources and compliance with the risk-based approach mandated by regulators.

5.3 Customer Acceptance Policy (CAP)

Dragon Money N.V. operates under a defined Customer Acceptance Policy (CAP) that sets clear criteria for which customers are allowed to use our services and what verification measures are required. In accordance with our risk assessments (BRA and CRA), the CAP outlines the following principles and actions:

- **Acceptance Criteria:** Customers must successfully complete the required level of due diligence (verification steps) corresponding to their risk level. All players must at least pass basic identity verification (see Step 1 in Section 5.4.2), and medium or high-risk players must undergo additional checks (Step 2 and Step 3 as applicable). Any refusal or failure to provide required information will result in denial of service or account closure.
- **Risk-Based Verification:**
 - **Low-Risk Players** – May undergo simplified due diligence in certain limited cases, consistent with regulatory allowances, if risk is demonstrably low.
 - **Medium-Risk and High-Risk Players** – Are subject to full standard due diligence (identity and age verification, proof of address) and, where applicable, Enhanced Due Diligence (EDD) including Source of Wealth inquiries (see Section 5.4.3).
 - **Prohibited Customers:** Dragon Money does not accept players from specified high-risk jurisdictions or sanctioned countries. During the onboarding process, if an applicant's country of residence or nationality is on a prohibitive or high-risk list (as determined by our BRA and international sanctions lists), the registration will be rejected outright. Similarly, known criminals or persons with a history of fraudulent or suspicious activities are barred from opening an account.
 - **Politically Exposed Persons (PEPs):** While PEPs may not be outright rejected solely for their status, they are classified as high-risk. The decision to onboard a PEP requires senior management approval and the implementation of EDD measures, including detailed Source of Wealth verification and continuous monitoring of their transactions (see Section 5.4.3). If the risks associated with a particular PEP are deemed too great to manage, the customer will not be accepted.

All customer acceptance decisions are made in accordance with Curaçao regulations and the CGA guidelines. Dragon Money's CAP helps ensure that our player base remains within our risk appetite. It prevents the platform from being exposed to undue risk by proactively filtering out those individuals who pose an unmanageable risk of money laundering, terrorist financing, or other financial crime.

The latest version of CAP Policy is published on Dragon Money N.V.'s official website for transparency. It can typically be found in the "CAP Policy" section.

5.4 Customer Due Diligence (CDD)

Customer Due Diligence is the cornerstone of Dragon Money's AML/CFT program. We have implemented a multi-tiered CDD process to verify the identity of our players and assess their suitability to use our platform, in line with legal requirements. The CDD process includes collecting customer information, verifying identification documents, understanding the source of funds, and ongoing monitoring of the customer's activity. The level of diligence increases with the customer's risk level or as transaction amounts exceed defined thresholds.

5.4.1 Three-Step Verification Process:

Dragon Money employs a three-step verification procedure for all customers, ensuring a thorough Know Your Customer (KYC) process that escalates with higher risk or higher transaction volumes. The steps are as follows:

1. Step One – Basic Customer Information (KYC): (Original content: Step 1 verification)

Scope: This is required for every user at the time of registration and before any withdrawal is permitted. Regardless of the customer's chosen payment method, deposit amount, withdrawal amount, or nationality, Step One must be completed first.

Process: The customer must provide basic personal information by completing an electronic KYC form (the "basic document") accessible via their account settings page on [Dragon Money's website](#). The information required includes:

- First Name and Last Name
- Date of Birth (to verify age and identify the individual)
- Gender
- Nationality (Country of citizenship)
- Country of usual residence (and full residential address, including city and postal code)

By submitting this information, the customer attests that the details are accurate and up-to-date. Dragon Money's system, assisted by automated checks, initially verifies that the provided data is complete and internally consistent. This basic information establishes the customer's identity profile and allows Dragon Money to perform preliminary screening (e.g., against sanction or PEP lists – see Section 5.4.4). No withdrawals are allowed from a customer's account until Step One is successfully completed.

(Note: The personal data collected is handled in compliance with data protection regulations; see Section 5.8.5 on Data Security for details on privacy.)

2. Step Two – Identity Verification: (Original content: Step 2 verification)

Trigger: Step Two must be completed by any user who deposits a cumulative amount exceeding NAF 4,000 (Netherlands Antillean Guilders) or its equivalent, or requests a withdrawal of any amount (i.e., any withdrawal transaction triggers the need for identity verification if not already done). In practical terms, even if the deposit threshold hasn't been reached, the first withdrawal request will prompt Step Two. Until Step Two is satisfied, the pending withdrawal (or any deposit/tip beyond the threshold) will be placed on hold and not processed.

Process: In Step Two, the customer is directed to a secure verification page to upload a valid government-issued photo identification. Acceptable forms of ID include a passport, national identity card, or driver's license (the types of IDs accepted may vary by country, but only official government IDs are permitted). The verification procedure requires the following:

- The customer must provide a photograph of their ID document. The image must clearly show all four corners of the ID and all details must be legible (the customer is allowed to blur out sensitive personal information such as an ID number or personal attributes not needed for KYC, but the name, date of birth, nationality, gender, and photograph must remain visible and clear).
- For additional security, Dragon Money requires a selfie (self-portrait photograph) of the customer holding the ID next to a piece of paper with a randomly generated six-digit code provided by Dragon Money. This step helps ensure that the person submitting the ID is the legitimate owner of that ID ("liveness" check) and that the verification is happening in real-time. The handwritten code and the ID must both be visible in the photo.

Electronic Verification: Upon upload, Dragon Money utilizes automated identity verification services and databases to cross-check the information provided in Step One against the identification documents from Step Two. This includes validating that the name, date of birth, and other details match public or proprietary databases, and that the ID is genuine and has not been tampered with. We perform these checks through at least two independent databases or verification services to ensure reliability.

- If the electronic checks confirm the details and authenticity of the ID, Step Two is considered successfully completed.
- If an electronic check fails or is inconclusive, or if such checks are not possible (due to the customer's country not supporting database verification, for example), then Dragon Money will request additional manual documentation. In such cases, the customer is required to provide proof of current address or other corroborating documents. Acceptable proof of address may include an official document such as a recent utility bill, bank statement, or a government-issued residence certificate, dated within the last 3 months, showing the customer's name and residential address. This document helps confirm that the personal information given in Step One is accurate and that the ID document corresponds to a real, traceable individual. The customer will be guided to upload such a document if needed.

(Dragon Money's support team is available to assist customers during this process and to clarify documentation requirements. All documents are reviewed by trained compliance personnel if automatic validation fails.)

Timeframe and Failure to Comply: Dragon Money imposes a strict timeframe for completing Step Two once it is triggered. If the requested identity verification documents and information are not provided by the customer within 30 days from the moment the NAF 4,000 deposit threshold was reached (or from the first withdrawal request), the following actions are taken:

- The customer's account will be suspended and the business relationship terminated due to non-compliance with KYC requirements. No further gaming activity will be permitted.
- If there is a reason to suspect money laundering or terrorist financing (for example, the circumstances that triggered Step Two or the subsequent failure to comply raise suspicion of illicit intent), Dragon Money will file a report with the FIU for the attempted transaction or account activity, as required by law.

- If no clear suspicion of ML/TF arises from the information available (i.e., the trigger was purely threshold-based and the customer appears to simply be non-responsive or unwilling to comply), any funds that were pending or in the customer's account will be returned to the same bank account or cryptocurrency wallet from which they originated, to the extent possible. This ensures that funds are not retained by Dragon Money without verification.

Dragon Money carefully balances its obligation to report suspicious activity with the need to avoid "tipping off" the customer. For instance, outright freezing an account and communicating that it's due to a suspicion of money laundering could alert the customer that they are under scrutiny. Therefore, in cases where funds are frozen or an account is blocked pending investigation, such actions are taken discreetly and only the minimum necessary information is communicated to the customer (e.g., stating that additional verification is required or that withdrawals are on hold pending compliance checks). Any decision to maintain an account freeze without immediately reporting to the customer will involve consideration by the Compliance Officer and, if appropriate, consultation with legal counsel or the FIU.

3. Step Three – Enhanced Due Diligence (EDD): (Original content: Step 3 verification)

Trigger: Step Three constitutes Dragon Money's Enhanced Due Diligence measures. It is automatically required for any customer whose transactions exceed NAF 5,000 (or equivalent), and for any customer categorized as high-risk (even if transactions have not yet exceeded NAF 5,000). Concretely, EDD (Step Three) is triggered when a user:

- Deposits over NAF 5,000 (or equivalent in other currencies) in total,
- Withdraws over NAF 5,000 in total, or
- Sends (tips/transfers) over NAF 5,000 to another user on our platform.

Once this threshold is reached or a high-risk profile is identified, all pending deposits, withdrawals, or transfers are put on hold until the Enhanced Due Diligence process is completed and reviewed.

Scope: EDD involves deeper investigation and the collection of additional information to ensure we thoroughly understand the customer's profile and the source of their funds. The rationale is to apply stricter scrutiny where the risk of money laundering or terrorist financing is higher. Some examples of situations that inherently would invoke EDD (even aside from the NAF 5,000 threshold) include:

- The customer is a Resident of a High-Risk Jurisdiction (as identified by the FATF or local regulators, or as determined by Dragon Money's risk rating of countries – see Section 5.4.5 on Risk-Based Segmentation).
- The customer is a Politically Exposed Person (PEP) or a close associate/family member of a PEP.
- The products or transactions in use favor anonymity or obscurity (e.g., use of certain cryptocurrencies or privacy coins, unusual gaming patterns intended to mask transactions).
- Introduction of new products, services, or technologies that have not been previously used by the customer, which might increase risk (e.g., the customer starts using a new payment method that is considered higher risk).

Process: Under EDD, Dragon Money's Compliance Team will undertake one or more of the following measures, as necessary, to build a more complete picture of the customer and the nature of their transactions:

- Obtain additional identification information: We may ask for further identity documents or information, such as a second form of government ID, or verification of previous addresses, to ensure we have robust evidence of the customer's identity over time.
- Detailed personal information: Gathering more data on the customer's background, such as occupation, name of employer, source of income, and any relevant financial history. Public databases, internet searches, and commercial risk intelligence tools may be used to supplement the information the customer provides (for example, checking if the customer appears on any adverse media or legal records).
- Clarification of the intended nature of the business relationship: Understanding why the customer is using Dragon Money's platform. Are they a casual player, a professional gambler, or perhaps acting on behalf of someone else? We may require the customer to state their expected level of activity (e.g., anticipated frequency of deposits/withdrawals, average bet sizes) and the purpose of their play (entertainment, professional poker, etc.) to see if future activity aligns with these statements.
- Source of Funds and Source of Wealth inquiry: (See Section 5.4.3 below for detailed Source of Wealth requirements.) In EDD, it is mandatory to ascertain where the money comes from. The customer will be asked to provide documentation or explanation for the origin of the funds they are gambling with. For example, this could include bank statements showing salary credits (if the funds come from employment income), documents evidencing a recent sale of an asset, inheritance documents, or other proof depending on what the declared source is. Dragon Money will verify these explanations to the extent possible (e.g., verifying business ownership via company registries if the source is business income).
- Reason for transactions: If there are specific large or unusual transactions, we might ask the customer to clarify the reason. For instance, if a customer suddenly deposits a very large sum or makes an atypical purchase of in-game credits ("chips"), we may inquire why (e.g., they might claim a big win at another casino or a one-time special event).
- Senior management approval: For a high-risk customer to continue using our services, approval from senior management (executive level) may be required. The Compliance Officer will prepare a summary of the case (risk factors, due diligence findings, and any mitigating factors) for review by the General Manager or Board of Directors. Continuation of the business relationship with a high-risk customer is a risk-based decision that Dragon Money's leadership must consciously make and document.
- Enhanced monitoring: The customer's account will be flagged for continuous, enhanced monitoring (see Section 5.5 on Ongoing Monitoring). This means their transactions will be reviewed more frequently and in greater detail, and any deviation from expected activity will be scrutinized. The threshold for what is considered an "unusual" transaction is set lower for high-risk customers.

Throughout the EDD process, Dragon Money remains vigilant for any indication that the account or transactions are linked to illicit activities. If at any point the information obtained does not satisfy our requirements or if the customer refuses to cooperate with EDD, we will deny further services to the customer. In such cases, the relationship is terminated, any remaining balance may

be frozen or returned (depending on legal guidance), and a report to the FIU will be made if grounds for suspicion exist.

Examples of EDD measures in practice:

- A customer has cumulative deposits of NAF 6,000 over a short period. Dragon Money contacts the customer to request proof of Source of Wealth such as pay slips and a bank statement. The customer provides pay slips indicating a monthly salary consistent with the deposited amounts and a bank statement showing the funds came from their personal account. The Compliance team verifies the employer's existence and the plausibility of salary. This satisfies EDD, so the account is allowed to continue, but with ongoing monitoring.
- Another customer is identified as a PEP (a member of a foreign parliament). The customer is asked for Source of Wealth documentation despite having deposited only NAF 2,000 (because PEP status triggers high-risk categorization). The customer provides disclosures of assets and a letter from their bank. Senior management is notified and approves continuing with the customer under close monitoring. Any transactions by this customer above a nominal threshold are manually reviewed by Compliance.
- If a customer failed to provide satisfactory additional information, Dragon Money would freeze the account, prevent all transactions, and file an FIU report if appropriate.

5.4.2 Identification and Verification of Beneficial Owners:

While Dragon Money N.V. primarily serves individual players, we recognize that there can be situations where accounts are funded or controlled by someone other than the named account holder (for example, if a player is using funds provided by a third party, or if an account is opened on behalf of a legal entity or trust). In compliance with Curaçao laws and international AML standards, we have measures to identify and verify the Beneficial Owner (BO) in relevant cases.

Dragon Money will determine the beneficial owner(s) and take additional steps in the following scenarios:

- If the customer account is registered under a name of a legal entity (e.g., a company or partnership) or a legal arrangement (e.g., a trust or foundation). (Note: Typically, our platform is for individuals, but in any exceptional cases such as VIP high-rollers playing via a company, this applies.)
- If there is reason to believe the customer is acting on behalf of another person or entity, or using funds provided by someone else (e.g., an account that shows funding from multiple sources not in the account holder's name).
- When a customer's behavior suggests that the account is being used by a third party, or there is a power of attorney or similar arrangement in place.
- Whenever required by the outcome of the Customer Risk Assessment – for instance, if a customer's profile or transaction pattern hints that they might be a front for another individual.

When identifying a Beneficial Owner, Dragon Money will:

1. Obtain identifying information for potential BOs: If the customer is a legal entity, we will gather the full legal name, registration number, and ownership structure of that entity. We require the

names of all individuals who own or control 25% or more of the entity's shares or voting rights. In higher-risk cases, or if no one meets the 25% threshold (perhaps ownership is very spread out), we lower the threshold (e.g., anyone with 10% ownership) or identify persons with control (such as directors or settlors of a trust – the “control test”). For each person identified as a BO, we collect their full name, date of birth, nationality, and address.

2. Verify the identity of BOs: Each Beneficial Owner identified is subject to verification similar to an individual customer. This means we will request official identification documents (passport, ID card, etc.) for those individuals and verify them using the methods described in Step Two above.

3. Obtain supporting documentation: In complex ownership cases, we may ask for additional documents such as corporate share registers, organization charts, shareholder agreements, trust deeds, or powers of attorney to confirm the ownership or control structure as represented by the customer. These documents help us understand who is ultimately behind the account.

4. Documentation and decision: If beneficial owners are identified and verified with confidence, the account can proceed (assuming the BOs themselves do not present disqualifying risks such as sanctions listing). If Dragon Money cannot identify or verify the beneficial owner(s) of an account to a satisfactory degree, we will not establish or continue the business relationship. The account will be refused or closed because we cannot fulfill our CDD obligations. Additionally, if the lack of transparency itself raises suspicion (for example, the customer is evasive about who the funds belong to), a report to the FIU may be considered.

All information regarding beneficial ownership is documented in our records. Dragon Money retains records of identification documents and due diligence findings for at least ten (10) years after the end of the business relationship (see Section 5.8.4 on Record Keeping). This ensures that if authorities ever need to trace the chain of ownership or investigate past transactions, the necessary information is available.

5.4.3 Source of Wealth (SoW) Requirements:

As part of Enhanced Due Diligence, Dragon Money N.V. will obtain and assess the Source of Wealth (SoW) of a customer in certain scenarios. Establishing SoW means understanding how the customer acquired the funds they are using to gamble (the economic or business activities that generated the customer's wealth). SoW verification is mandatory in the following circumstances:

- High-Value Transactions: When a single transaction or a series of linked transactions equals or exceeds NAF 5,000 (Netherlands Antillean Guilders) or equivalent in other currencies (approximately USD/EUR 2,800).
- High-Risk Customer Profile: When the customer is categorized as high-risk per the CRA (Section 5.2). This includes (but is not limited to) cases such as:
 - The customer is a Politically Exposed Person (PEP).
 - The customer is a resident of a high-risk jurisdiction (country known for elevated ML/TF risk or subject to sanctions).
 - The customer uses anonymous payment methods or new, untested technologies that increase opacity (e.g., certain cryptocurrencies or mixers).

- The customer exhibits unusual behavior or transactions that do not match their stated profile (for instance, a low-income occupation but very large gambling transactions).
- Whenever the origin of funds is unclear or raises any suspicion of illicit activity, regardless of amount.

Documentation and Verification: To satisfy SoW requirements, Dragon Money will request that the customer provide documentary evidence of how they obtained their wealth/funds. Examples of acceptable documentation include:

- Proof of employment and income (recent pay stubs, an employment contract, or a letter from an employer stating salary).
- Recent bank statements showing accumulation of funds or regular income deposits.
- Proof of an inheritance or gift (e.g., a will or notarized letter along with bank records of the transfer).
- Sale agreements or contracts demonstrating the sale of a significant asset (property, vehicle, business, investments) and receipt of funds from that sale.
- Legal compensation or court award documents (if the funds come from a legal settlement).
- Evidence of investment income, such as dividend statements, stock trading account records, or cryptocurrency trading history that align with the funds deposited.

The Compliance Team will review all provided SoW documents for authenticity and sufficiency. They may follow up with the customer if clarification is needed or if additional verification steps are warranted (for example, verifying an employer's existence, or checking public records to confirm a property sale). Failure or refusal to provide satisfactory SoW documentation when required will result in consequences up to and including account restrictions, denial of transactions, or account closure. Furthermore, if the lack of proof or the nature of the funds gives rise to suspicion of money laundering or terrorist financing, Dragon Money will file a report with the FIU.

(SoW information, like all due diligence data, is stored securely and kept confidential, used only for compliance purposes. It is retained for at least 10 years after the end of the relationship.)

5.4.4 Sanctions and PEP Screening:

Dragon Money N.V. complies fully with all international sanctions obligations. We conduct sanctions screening of all customers at onboarding and continuously throughout the customer relationship. This means we check the names and identifying information of our players (and in relevant cases, beneficial owners or payers/payers in transactions) against the following sanctions lists, among others:

- United Nations Security Council sanctions list
- European Union Consolidated sanctions list
- United States Office of Foreign Assets Control (OFAC) list

- Kingdom of the Netherlands sanctions lists (applicable to Curaçao)
- Lists issued by the Central Bank of Curaçao and Sint Maarten (CBCS)
- Any other relevant national/international lists, including those Curacao authorities circulate (e.g., local terrorism watchlists or fraud blacklists).

We also screen for Politically Exposed Persons (PEPs) and other high-risk profiles using specialized databases. Screening is facilitated by automated systems that are updated in real-time with the latest sanctions and PEP data. If during screening a customer's details produce a match (a "hit") on any sanctions or prohibited parties list, or if a customer is identified as a prohibited player (such as appearing on the list of known fraudsters or PEPs from sanctioned countries):

- Dragon Money will immediately freeze the account and/or the specific transaction. No further transactions (deposits, withdrawals, or gameplay) will be permitted on the account.
- A report will be filed without delay to the FIU and/or appropriate law enforcement, in compliance with the National Ordinance on the Reporting of Unusual Transactions. The customer will not be notified of the exact reason for the freeze (to avoid tipping off). They may simply be informed that their account is under review or "temporarily suspended."
- The account will remain frozen until the Compliance Department, in coordination with relevant authorities, has resolved the alert. If the match is confirmed to be a true positive (the person is indeed the one on the sanctions list), the relationship will be terminated and any further steps will follow legal instructions (such as asset freezing or confiscation by authorities). If the match is a false positive (e.g., a name similarity), the account may be unfrozen after adequate due diligence.

The sanctions and PEP screening process is overseen by the AML Compliance Officer. The AMLCO ensures that our screening software is maintained and updated, and that any potential matches are escalated appropriately. Regular audits of the screening process are conducted to ensure we remain aligned with evolving geopolitical risks and regulatory expectations.

(Note: Players from comprehensively sanctioned countries or regions are blocked from account creation altogether as part of our CAP – see Section 5.3. If a customer becomes sanctioned mid-relationship, the above freeze and report process applies.)

5.4.5 Risk-Based Approach to Geographic Regions:

Dragon Money recognizes that the risk of money laundering can vary significantly by a customer's country of origin or residence. In line with guidance from the Curaçao Gaming Control Board, we categorize countries into three risk tiers – Low, Medium, and High – and adjust our due diligence requirements accordingly:

- Region One – Low Risk: This category includes countries with strong AML regulations and low corruption and terrorism risk (for example, EU member states, UK, Canada, etc.). Customers from low-risk regions undergo the standard three-step verification as described above (Step 1 at signup, Step 2 at NAF 4,000 or any withdrawal, Step 3 at NAF 5,000). No additional early measures are required beyond the baseline policy.
- Region Two – Medium Risk: This includes countries that are not high risk but still present more risk than Tier One (this could be emerging markets or countries with some identified AML

deficiencies). For customers from medium-risk regions, Dragon Money applies enhanced vigilance at lower thresholds. In practice, this means:

- Step Two (ID Verification) is triggered earlier – after cumulative deposits or withdrawals of NAF 1,800 (≈\$1,000 USD), or if a customer sends (tips) another user NAF 900 (≈\$500). In other words, players from medium-risk countries must verify their identity sooner than those from low-risk countries. Until Step Two is completed, further withdrawals or deposits beyond those amounts are on hold.
- Step Three (EDD) is likewise triggered at a lower level – after deposits or withdrawals reaching NAF 4,500 (≈\$2,500), or sending another user NAF 1,800 (≈\$1,000). This ensures Enhanced Due Diligence (such as Source of Wealth checks) is performed at a lower activity level for these higher-risk customers.
- Additionally, if a supposedly low-risk customer exhibits behavior common to higher-risk regions (for example, using an exchange to convert cryptocurrency into another currency frequently), we may treat that customer as medium risk in terms of when we apply Step Two and Three.
- Region Three – High Risk: This category comprises countries with high levels of corruption, subject to international sanctions or embargoes, or otherwise deemed unacceptable risk. Dragon Money does not onboard customers from high-risk regions. Such jurisdictions are blocked in our system (meaning players cannot select those countries during registration). If it is later discovered that a customer has circumvented this control (e.g., by using VPN or false information to appear from elsewhere), the account will be closed. The list of high-risk regions is regularly reviewed and updated to reflect the global risk environment.

This geographically risk-tiered approach is part of Dragon Money's risk-based AML strategy. By tailoring verification requirements to country risk, we ensure that we apply stricter controls where the probability of illicit activity is higher, and we remain compliant with Curacao GCB guidance on international best practices. These measures are in addition to any sanction-related prohibitions described above.

In summary, all customers, regardless of origin, must complete our KYC steps, but those from medium-risk countries face earlier identity checks and EDD, while those from high-risk countries are not accepted at all.

5.5 Ongoing Monitoring

Even after initial customer due diligence is completed, Dragon Money maintains vigilant ongoing monitoring of all player transactions and activities. The goal of ongoing monitoring is to detect unusual or suspicious patterns as they occur, ensuring timely intervention. Our monitoring program operates on multiple levels of control:

1. First Line of Defense – Payment Provider Screening: Dragon Money works exclusively with reputable Payment Service Providers (PSPs) (banks, e-wallets, crypto processors) that themselves employ robust AML controls. These providers are the entry point for customer funds. By partnering only with PSPs that enforce KYC on their end, a significant portion of obviously illicit funds are filtered out before reaching our platform. For instance, if a bank flags a credit card deposit to us as suspicious, that deposit will not be completed. This first line largely prevents many high-risk transactions from ever occurring on Dragon Money.

2. Second Line of Defense – Automated and Staff Monitoring: Once funds are on the platform, Dragon Money’s internal systems and staff take over monitoring:

- Automated Transaction Monitoring System: We utilize an AI-driven monitoring system that continuously analyzes all betting and transactional activity on the platform. This system is calibrated to look for red flags and atypical patterns, such as:
- Large deposits followed by immediate withdrawals without proportional gameplay (possible sign of money laundering “layering”).
- Sudden changes in a player’s behavior or transaction size/frequency.
- Use of multiple payment methods or bank accounts by the same user, especially if inconsistent with their profile.
- Multiple accounts logging in from the same device or IP (potential sock-puppet or mule accounts).
- Frequent currency conversions or movement of funds between different cryptocurrencies and fiat in ways that obscure traceability.
- Any other patterns identified from past cases or risk typologies (our AI is updated based on known schemes).
- Real-Time Alerts: If the system flags an unusual transaction or pattern, it generates an alert for the Compliance Team. For example, if a user tries to withdraw using a different payment method than they deposited with (bypassing our rule that withdrawals must go back to the original deposit source for the same amount), an alert is triggered.
- Human Review and Intervention: Every alert from the automated system is reviewed by a trained compliance analyst or the AML Compliance Officer. The analyst will cross-reference the player’s profile (KYC information, Source of Wealth if available, playing history) to determine if the activity is explainable or genuinely suspicious. In many cases, an alert leads to contacting the player for additional information or requesting updated documents. This human “second look” is crucial to filter out any false positives and to decide on the appropriate action (allow, suspend, or report).
- Employee Awareness: Beyond automated systems, all Dragon Money staff who interact with customers (especially customer support and VIP managers) are instructed to be alert to any signs of irregular activity. They are trained to escalate any concerns to the Compliance Officer. For instance, if a support agent notices a customer asking unusual questions about payout limits or expressing urgency in withdrawing after a deposit, the agent will inform Compliance.
- Information Sharing within the Company: Our internal procedures ensure that knowledge about potentially suspicious players is shared with relevant teams on a need-to-know basis. This way, if any department engages with a flagged customer, they do so with heightened scrutiny.

All transactions on the platform are logged and subject to this ongoing review. The AML Compliance Officer oversees the automated monitoring parameters and periodically updates them in line with new risk insights or regulatory advisories.

3. Third Line of Defense – Enhanced Manual Review: As a final backstop, Dragon Money’s Compliance Department conducts manual reviews of accounts and transactions, focusing on suspicious and high-risk cases identified from the above layers. This may involve a full audit of a particular customer’s activity history, deeper open-source intelligence gathering (public record searches, social media checks), or coordination with external investigative agencies. The AML Compliance Officer, along with senior management if needed, will determine if any further action is required. If clear evidence of fraud, money laundering, or other criminal behavior is found, Dragon Money will immediately involve law enforcement and notify the FIU, as appropriate. This third line ensures that nothing slips through unchecked and that complex or borderline cases receive a thorough, qualitative assessment.

In summary, ongoing monitoring is an active and continuous process. It combines technology, human expertise, and defined procedures to ensure that any unusual customer behavior is promptly detected, evaluated, and addressed. By having these three lines of defense, Dragon Money aims to catch suspicious activities early and prevent our platform from being misused after initial onboarding.

5.6 Reliance on Third Parties for CDD

Dragon Money N.V. may rely on third-party service providers to perform certain Customer Due Diligence elements, such as identity verification, document authentication, or database screening. For example, we utilize external vendors for automated ID document validation and sanction/PEP screening software. In addition, as noted, our payment processors conduct their own KYC on funds entering their systems. Such reliance on third parties is done in accordance with Curaçao regulations, which permit delegation of CDD tasks provided that:

- The third-party is a regulated and reputable entity (e.g., a financial institution or licensed KYC service provider) that is subject to equivalent AML obligations. Dragon Money conducts due diligence on any third-party to ensure they have adequate AML/CFT controls.
- There is a written agreement or understanding that the third-party will perform specified CDD measures on our behalf and will share all relevant CDD data (copies of ID documents, verification results, etc.) with Dragon Money in a timely manner. Dragon Money must have prompt access to this information and must be able to provide it to regulators upon request.
- Ultimate responsibility for compliance remains with Dragon Money N.V. We acknowledge that even when third parties assist, Dragon Money is accountable for any shortcomings. As such, we verify that the third party’s performance is adequate (through periodic audits or reviews of their work). If a third-party fails in their duties, Dragon Money will take corrective action or cease relying on them.

In practice, reliance on third parties helps streamline the customer experience (for instance, allowing ID verification to happen seamlessly via an integrated vendor API) but does not weaken our compliance. All third-party actions are integrated into our internal compliance program. Dragon Money’s Compliance Officer maintains a list of all third-party partners used for CDD and regularly evaluates their compliance with agreed standards.

(At present, our primary reliance is on payment providers for initial KYC and specialized firms for document and sanctions screening. We do not outsource the decision-making of customer risk acceptance – that remains internal.)

5.7 Recognition and Reporting of Unusual Transactions

Curaçao law (specifically, the National Ordinance on the Reporting of Unusual Transactions (NORUT)) requires Dragon Money N.V. to monitor, recognize, document, and report any transactions that are deemed unusual. An unusual transaction is one that deviates from the normal expected behavior of a customer or that has characteristics known to be linked with money laundering or terrorist financing. Dragon Money has developed clear procedures to ensure we meet these obligations:

a. Recognition of Unusual Transactions:

To recognize unusual transactions, Dragon Money relies on the combination of knowing the customer (via KYC information and customer profile) and specific indicators defined by law and our own risk criteria. All staff are trained to understand these indicators. In general, a transaction or series of transactions may be considered unusual if it lacks an apparent economic or lawful purpose, is inconsistent with the player's profile, or matches a pattern identified as suspicious. Examples include a player suddenly gambling far beyond their known income level, or frequent large transactions with no logical explanation.

Dragon Money follows the objective and subjective indicators issued under NORUT:

- Objective indicators (set by law): For instance, any cash or non-cash transaction (deposit, withdrawal, transfer) of NAF 5,000 or more in value is automatically considered an unusual transaction under Curaçao rules. This threshold applies whether the transaction is a single event or a series of transactions that appear to be linked within a single day ("gaming day") totaling NAF 5,000 or more. This means:
- A single or cumulative deposit of NAF 5,000+, whether by cash, bank transfer, cryptocurrency or any method, is unusual.
- A single or cumulative withdrawal of NAF 5,000+ is unusual.
- Purchasing casino credits (chips) worth NAF 5,000+ is unusual, as is cashing out such an amount.

These objective criteria ensure any large transaction is flagged regardless of other context.

- Subjective indicators: These rely on the judgment and knowledge of the customer. For example:
- Transactions that are reported to law enforcement (police or Justice Department) by any party in connection with money laundering or terrorism financing concerns.
- Transactions involving a person or entity who is listed on a sanctions list as described in Section 5.4.4 (since dealing with sanctioned parties is prohibited, any such attempt is inherently unusual/suspicious).
- Any transaction where there is reason to presume ML or TF – even if below objective thresholds. This could be based on patterns (structuring deposits just under reporting thresholds, rapid movement of funds between accounts, etc.) or based on external information (e.g., we learn a customer is under investigation elsewhere).

By maintaining robust customer profiles (via CDD) and automated monitoring (Section 5.5), Dragon Money is positioned to recognize when a transaction does not fit a customer's known

profile or seems intentionally obscured. For instance, if a normally small-stakes player suddenly receives a large sum from another user and immediately attempts to withdraw it without gaming activity, this would be recognized as unusual.

All staff receive specific training on recognizing unusual transactions, and internal guidelines are provided to help differentiate between legitimate high-value play and suspicious activity. Staff are required to promptly document and internally report any unusual transaction to the Compliance Officer using a standardized Unusual Transaction Report (UTR) form. This report includes details of the transaction, the reason it's considered unusual, and any supporting documentation (e.g., ID copies, screenshots, correspondence).

b. Internal Documentation and Analysis:

Every unusual transaction identified (either via automated means or manual observation) is documented by the Compliance team. The Compliance Officer maintains an internal log of unusual transactions reported by staff or systems, noting the date, customer, nature of the unusual activity, and the outcome of internal analysis. All supporting documents, such as identification copies, transaction records, account histories, etc., are attached to this internal case file. If, after analysis, an unusual transaction is not reported externally to the FIU (perhaps it was explained upon further review), the Compliance Officer will record the rationale and obtain sign-off from senior management, to have an audit trail of why it was not escalated. This internal decision will be signed by the Compliance Officer and/or senior management, as required by regulation, to show accountability for the decision.

Additionally, in line with FATF Recommendation 11, Dragon Money pays special attention to all complex or unusually large transactions and patterns that have no visible lawful purpose. Even if such transactions are not explicitly covered by predefined indicators, they are documented and evaluated.

c. External Reporting to FIU:

Pursuant to Article 11 of NORUT, Dragon Money reports any unusual transaction to the FIU without delay once determined as such. We have clear procedures for this external reporting:

- The Compliance Officer (AMLCO) is the designated point of contact for filing reports via the FIU's online portal (currently the goAML system). The report (often called a Suspicious Activity Report, SAR, or Unusual Transaction Report, UTR) is prepared with all required details: customer information, transaction details (amount, date, type), and description of the suspicious indicators.
- Reports are submitted electronically through the secured FIU reporting system. Dragon Money follows the specific formats and indicator codes as defined in the Ministerial Decree of November 11, 2015 (Regulation Indicators of Unusual Transactions). This ensures our report clearly cites which indicators (objective or subjective) triggered the filing.
- The reporting is done without tipping off the customer. The customer is not informed when a report is made. Internally, once a report is filed, a hold might be placed on the account pending instruction from authorities, but the customer may simply experience this as a "technical" or routine delay.

After reporting, the Compliance team continues to monitor the account closely. Any additional unusual activity will be reported in follow-up filings. If the FIU or law enforcement requests

further information, Dragon Money cooperates fully, providing all documentation and even freezing assets if instructed.

Summary of Unusual Transaction Types (per Curacao GCB guidelines): To reiterate, the following are examples of transactions that Dragon Money will deem unusual and likely report:

- Any transaction (or aggregated transactions) of NAF 5,000 or more in a day, whether in or out of the platform.
- Transactions involving a known sanctioned or blacklisted person or entity.
- Transactions that are structured or broken up in an apparent attempt to evade the NAF 5,000 threshold (smurfing).
- Complex transactions that make no economic sense (e.g., multiple players sending chips or credits in circles amongst themselves).
- Situations where fraud or theft is suspected (e.g., a player depositing with many stolen credit card numbers). In such cases, in addition to AML reporting, other actions (like blocking the account and contacting police) are taken.
- Any other transaction that staff cannot reasonably attribute to lawful behavior after review.

All unusual transaction reports (internal and external) are retained in our compliance archives for at least ten years and are subject to strict confidentiality.

Escalation Procedure for Suspicious Transactions (STRs):

The Company has a clear escalation procedure for handling suspicious transaction reports (STRs). Upon identification of a suspicious transaction, the following steps are taken:

1. Initial Detection — The employee detecting the unusual activity must report it to the Compliance Officer (MLRO) within 24 hours using the internal reporting channel.
2. Internal Review — The Compliance Officer must review the report within 2 business days, assess the circumstances, and decide whether the transaction meets reporting thresholds.
3. Regulatory Reporting — If deemed reportable, the Compliance Officer must file the STR to FIU Curaçao without undue delay, following the applicable format and procedures.
4. Documentation and Record-Keeping — All steps, findings, and decisions must be logged and archived, including reasons for reporting or not reporting.

The Compliance Officer has authority to escalate STRs directly to senior management or the Board if the case involves high-level risk, reputational exposure, or legal uncertainty.

5.8 AML/CFT Compliance Program and Governance

Dragon Money N.V. has established an overarching AML/CFT Compliance Program designed to ensure effective implementation of all the policies described above. This program is built on several pillars: clear organizational responsibilities, comprehensive record-keeping, ongoing employee training, regular independent audit, and strict adherence to data protection rules. It is also dynamic, meaning it will be updated as needed to respond to new risks or regulatory changes. Key components of our compliance program include:

5.8.1 Organization and Oversight:

Anti-money laundering compliance at Dragon Money is driven from the top. The General Management (executive management/Board) bears ultimate responsibility for maintaining an effective AML/CFT framework. Dragon Money has appointed a dedicated Anti-Money Laundering Compliance Officer (AMLCO) who oversees day-to-day compliance with this policy and related procedures. The AMLCO operates at a senior level and has direct access to the General Management, ensuring that any significant AML concerns are escalated and addressed promptly. The AMLCO's duties include: coordinating risk assessments, ensuring CDD is properly conducted, filing reports to FIU, training staff, and serving as the main contact for regulators and law enforcement on AML matters.

All employees are expected to adhere to this AML/CFT Policy, and managerial staff must enforce compliance within their teams. To formalize accountability, any major changes or updates to this AML/CFT Policy require approval from General Management and sign-off by the AMLCO. This ensures that policies remain current and effective, and that leadership is continuously engaged. The policy will be reviewed at least annually (or more frequently if required by regulatory updates or internal audit findings) to incorporate any new legal requirements or lessons learned. Minor procedural adjustments can be made by the Compliance team as needed, but substantive policy revisions follow the formal approval process above.

5.8.2 Record-Keeping:

In compliance with Curaçao laws, Dragon Money maintains thorough records of all relevant data collected under this policy. This includes copies of customer identification documents, address proofs, Source of Wealth documentation, records of transactions, internal and external reports of unusual transactions, and correspondence with customers regarding compliance matters. Key record-keeping provisions are:

- Customer Identification Records (KYC files) are kept for at least 10 years after the end of the business relationship with the customer (i.e., 10 years from account closure).
- Transaction Records (transaction logs, deposit/withdrawal histories, etc.) are kept for at least 10 years after the transaction date.
- Reporting and Audit Records: Any internally generated compliance reports, training attendance logs, audit reports, and communications with regulators are also preserved for a minimum of 10 years, or longer if required by law or company policy.

All records are stored in a secure and encrypted manner. Digital records are kept in secure servers with access controlled by the Compliance Department (and IT with proper oversight), and backups are stored offline in encrypted form. Physical records (if any) are stored in locked cabinets in a secure area. By retaining these records, Dragon Money can readily reconstruct customer accounts and activity if needed for an investigation or audit, even many years later. We understand the importance of this in identifying historical patterns or assisting authorities, and we commit to full record availability within the required timeframe.

5.8.3 Employee Training and Awareness:

Dragon Money invests in regular training programs to ensure that all relevant employees are well-versed in AML/CFT obligations and red flags. Our training and awareness program includes:

- **Mandatory AML Training** for all new hires whose role touches financial transactions or customer data (including customer support, finance, and management). New employees receive an introduction to AML/CFT regulations, Dragon Money’s specific policies, and their personal responsibilities (such as the duty to report unusual activity).
- **Annual Refresher Training** for all staff, which covers any changes in laws or internal policies, and reinforces key concepts. We update scenarios and case studies to reflect current trends (e.g., new types of cryptocurrency fraud, recent money laundering schemes in the gaming industry).
- **Targeted Workshops** for specialized teams (e.g., the payments team or VIP hosts) focusing on issues they might encounter, such as identifying fake IDs or handling high-roller clients in line with AML rules.
- **Testing and Acknowledgment:** We test employees on their understanding (through quizzes or interactive case studies) to ensure the training is effective. Employees must acknowledge in writing that they have completed the training and understand the policies.
- **Records of Training:** The Compliance Officer keeps records of who has completed training and when. This is monitored to ensure 100% participation.

Our training content is aligned with the latest regulatory developments and best practices. Sessions are often led by the AMLCO or an AML specialist and may include external experts or resources provided by the Gaming Control Board. By educating staff continuously, Dragon Money fosters a culture of compliance where employees at all levels serve as the “eyes and ears” of the company in AML matters.

5.8.4 Employee Integrity Screening

The Company maintains a robust integrity screening process for all employees, especially those involved in AML/CFT-related activities. Prior to hiring, candidates for AML-sensitive positions undergo background checks to assess criminal history, financial integrity, conflicts of interest, and reputational risks. These checks may include:

- Verification of identity and previous employment;
- Criminal record checks where permitted by law;
- Assessment of AML training or experience;
- Declarations of conflicts of interest.

Current employees in AML functions are periodically re-evaluated to ensure ongoing suitability and trustworthiness. Any employee who fails to meet the Company’s standards for integrity will not be permitted to perform AML duties.

5.8.5 Independent Audit:

Dragon Money’s AML/CFT program is subject to periodic independent audit to evaluate its effectiveness and identify any deficiencies. We arrange for an internal audit unit or qualified third-party auditors to review our AML compliance at least annually. The audit typically includes:

- A review of policy documents and risk assessments (BRA/CRA) to ensure they are up-to-date and comprehensive.
- Sampling of customer files to verify CDD was performed correctly and on time.

- Testing of the transaction monitoring system (e.g., did alerts generate as expected, were they handled appropriately).
- Reviewing training logs and interviewing staff to gauge awareness.
- Checking that all unusual transactions that should have been reported were indeed reported (back-testing).
- Evaluating record-keeping and data security measures.

The results of these audits are documented in an audit report. Any findings or recommendations are presented to senior management and the AMLCO. Dragon Money commits to addressing audit findings promptly to continually improve our AML controls. Regulators will be provided access to these audit results upon request, demonstrating our proactive stance on compliance.

5.8.6 Data Security and Privacy:

Handling sensitive personal data is inherent to AML efforts. Dragon Money takes data security and customer privacy extremely seriously. All personal data collected under this policy (IDs, documents, personal information, transaction histories) is protected in line with industry best practices and legal requirements. Key measures include:

- Confidentiality: Only authorized personnel in the Compliance, Security, or Management teams can access sensitive AML data, and only for legitimate purposes. We enforce access controls and confidentiality agreements with staff.
- Encryption: Electronic data is stored in encrypted form. Communications containing personal data (e.g., emailing an ID copy internally) are encrypted or done through secure channels.
- No Unauthorized Sharing: Dragon Money will never disclose customer personal data to third parties except: (1) if required by law or regulation (e.g., to the FIU or law enforcement under proper authority), or (2) to comply with a lawful court order, or (3) to authorized third-party service providers as described in Section 5.6 (and even then, those providers are bound by confidentiality). We do not sell customer data or share it for marketing or any non-compliance purpose.
- Data Protection Compliance: We adhere to relevant data protection laws, including the principles of the EU General Data Protection Regulation (GDPR) as applicable. (Curaçao's data protection framework is informed by EU standards.) This means we ensure data is processed lawfully and kept no longer than necessary. Dragon Money's practices align with the EU Data Protection Directive (95/46/EC) and its successor GDPR.

In the event that regulators from another jurisdiction require information (e.g., as part of an international investigation), we will only provide it through proper legal channels (such as mutual legal assistance treaties), ensuring customer rights are respected. Our Privacy Policy (separate document) further details how we handle personal information. By integrating strong data protection into our AML program, we maintain customer trust and comply with privacy regulations while fulfilling our AML obligations.

5.8.7. Technological Controls for AML/CFT Compliance

Dragon Money employs a combination of automated and manual tools to support AML/CFT controls, including:

- Transaction Monitoring Systems that flag unusual deposit/withdrawal behavior in real time;
- PEP and Sanctions Screening Tools, integrated into the onboarding and ongoing monitoring process;
- Audit Logging functionality that records all user and system actions for compliance oversight;
- Case Management Tools that allow the Compliance Officer to manage alerts, investigations, and reporting workflows.

These systems are configured to comply with Curaçao AML/CFT requirements and are regularly tested for effectiveness. Updates and adjustments are made as typologies evolve or regulatory guidance changes.

5.8.8 Procedures for Suspected ML/TF Activity:

(As a concluding note to the program description, we highlight our procedure for handling detected suspicion.)

Dragon Money's compliance program includes clear procedures for responding to incidents of suspected money laundering or terrorist financing. If at any point a customer's activity is conclusively deemed suspicious or illicit:

- The AMLCO, in consultation with senior management, will block or freeze the customer's account immediately to prevent further transactions. This may include freezing all funds in the account.
- A detailed report will be compiled and sent to the FIU (if not already done through an earlier unusual transaction report).
- We will await guidance from the FIU or law enforcement. Funds will remain frozen until authorities advise on release or seizure.
- Dragon Money will fully cooperate with any ensuing investigation, providing additional data or testimony as needed.
- The customer in question will not be alerted to the suspicion beyond perhaps noticing that their account is locked; any inquiries by the customer will be handled carefully to avoid tipping off (e.g., they may be told the account is under a standard review).
- Internally, a post-incident review will occur to determine if any controls can be improved to detect similar cases earlier.

Through these steps, our program ensures that when confronted with actual money laundering attempts, we react swiftly, report to authorities, and protect the integrity of our operations.

6. Consequences of Non-Compliance

Failure to comply with the provisions of this AML/CFT Policy, whether by employees, contractors, or the organization as a whole, can result in severe consequences. Dragon Money N.V. is committed to enforcing this policy and understands the gravity of non-compliance:

- **Internal Disciplinary Action:** Employees of Dragon Money who neglect or willfully violate these AML/CFT procedures (for example, by skipping required verifications or ignoring unusual activity) will face disciplinary measures. This can include retraining, formal warnings, or up to termination of employment in cases of serious or willful non-compliance. The company has a code of conduct that makes AML adherence a condition of continued employment.
- **Regulatory and Legal Penalties:** Dragon Money N.V. operates under the license and oversight of the Curaçao gaming authorities. Non-compliance with AML/CFT obligations can lead to regulatory sanctions against the company, including substantial fines, the imposition of special measures (such as increased audits or mandatory independent monitors), suspension of our gaming license, or even revocation of the license, which would cease our operations. In addition, willful blindness or complicity in money laundering by any staff or the company can lead to criminal prosecution. Individuals (employees or officers) found guilty of facilitating money laundering can face criminal charges, potentially resulting in imprisonment and personal fines under Curaçao law and any other relevant jurisdiction's laws.
- **Reputational Damage:** Beyond formal penalties, failing to properly prevent money laundering can severely damage Dragon Money's reputation. News of involvement (even unwittingly) in money laundering or terrorist financing could erode customer trust, lead to negative media coverage, and harm relationships with business partners, banks, and payment processors. The long-term reputational risk could manifest in loss of customers, decreased revenue, and difficulty in obtaining banking or financial services (as banks may deem the company too risky). Thus, the cost of non-compliance far exceeds the investment in robust AML measures.
- **Impact on Business Continuity:** Regulators globally are increasingly intolerant of AML/CFT breaches in the gaming sector. Non-compliance could result in our inclusion on watchlists, greater scrutiny on all our transactions (slowing down business), and in worst cases, a shutdown of operations by authorities. Investors and stakeholders also may withdraw support if the company is seen as high-risk for regulatory non-compliance.

Dragon Money underscores that every member of the organization has a role in AML/CFT compliance, and thus shares responsibility for preventing these negative outcomes. We foster a compliance culture where raising concerns is encouraged, and adherence is rewarded. The company would much rather over-report or over-check a transaction than miss a potentially illicit one. In summary, non-compliance is not an option – the stakes are simply too high for our business, our staff, and the public trust.

7. References and Applicable Regulations

This AML/CFT Policy is designed to comply with, and is inspired by, the following laws, regulations, and guidelines (as updated to 2025):

- **Curaçao National Legislation:**
- **Regulations for the Combating of Money Laundering, the Financing of Terrorism, and Proliferation of Weapons of Mass Destruction** applicable to Curaçao Casinos and Providers of Other Online Games (January 2025). – Comprehensive regulations issued by the Curaçao Gaming Control Board (GCB) that outline casinos' obligations for AML/CFT. (This is a primary guiding document for our policy.)

- National Ordinance on the Identification of Clients when Rendering Services (N.G. 2017, no. 92) – Requires verifying customer identity for certain services (know-your-customer law in Curaçao).
- National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99) – Establishes the duty to report unusual transactions to the FIU and lists objective/subjective indicators (NORUT).
- Ministerial Decree of 11 November 2015 establishing Indicators of Unusual Transactions (N.G. 2015, no. 73) – Lists the specific transaction types/amounts that qualify as “unusual” under NORUT (e.g., the NAf 5000 threshold).
- Sanctions National Ordinance (N.G. 2014, no. 55) and Kingdom Sanctions Act (Kingdom Law of 2015, in force per N.G. 2017, no. 2) – These laws implement UN, EU, and other international sanctions within Curaçao’s jurisdiction.
- Various National Decrees for specific sanctions regimes: for example, decrees implementing UN Security Council resolutions concerning Al-Qaeda, the Taliban, ISIL (N.G. 2015, no. 29), sanctions concerning Libya (N.G. 2015, no. 28), and sanctions concerning North Korea (N.G. 2015, no. 30), as well as the National Ordinance extending validity of sanction decrees 2018 (N.G. 2018, no. 34). (These decrees detail particular lists and measures we must enforce in our sanctions screening.)
- Curaçao Penal Code (Wetboek van Strafrecht, N.G. 2011, no. 48) – Contains the criminal offenses for money laundering and financing of terrorism, which underlie our legal obligations (establishes that money laundering is a crime even if predicate offense occurred abroad, etc.).
- International Standards and EU Directives:
 - Financial Action Task Force (FATF) Recommendations – Although not listed explicitly above, our program is designed to meet FATF’s 40 Recommendations (the international AML/CFT standards), as reflected in local law.
 - EU 4th AML Directive (2015/849) and 5th AML Directive (2018/843) – While an EU directive is not directly binding in Curaçao, Dragon Money voluntarily aligns with the stricter elements of these directives as part of best practice (for instance, the risk-based approach, PEP handling, and beneficial ownership transparency requirements).
 - EU Regulation 2015/847 on Transfer of Funds – We ensure compliance with requirements to include originator and beneficiary information in fund transfers (relevant when moving funds to/from players via banks).
 - Basel Committee Guidelines & Wolfsberg Principles on AML for financial institutions – used as references for structuring our internal controls, where applicable to gaming.
- Related Internal Documents:
 - Dragon Money N.V. Anti-Fraud Policy – (if existing) Addresses detection of fraud and collusion, complementary to AML efforts.
 - Dragon Money Customer Privacy Policy – Outlines how customer data is handled and protected (mentioned in Section 5.8.5).

- Employee Code of Conduct & Handbook – Contains provisions requiring compliance with AML laws and outlines disciplinary procedures for non-compliance (see Section 6).
- Procedures Manual for Customer Verification – An internal document detailing step-by-step how staff should execute the verification procedures summarized in this policy (including which tools to use for ID verification, how to review documents, etc.).
- Incident Response Plan for AML – Internal guidelines on what to do when suspicious activity is identified (who to notify, how to secure evidence, etc.).

(All staff have access to the internal documents via our company intranet. External documents (laws and regulations) are maintained by the Compliance Officer and can be consulted as needed; key points are covered in training.)

Policy Availability: The latest version of this AML/CFT Policy is published on Dragon Money N.V.'s official website for transparency. It can typically be found in the “AML Policies” section (or via the user account settings page). Customers and other stakeholders can view the policy at any time, ensuring our commitments are public and clear.

8. Contact Information

For any questions, clarifications, or concerns regarding this AML/CFT Policy or its implementation, please contact our designated Compliance Officer:

- AML Compliance Officer: Veremiienko Kateryna
- Email: aml@drgn.casino

The Compliance Officer (or an authorized compliance team member) will be available to respond to regulatory inquiries, law enforcement requests, or internal questions related to this policy. Players or third parties who have feedback or need to report something suspicious about Dragon Money's operations may also use these contact details.

For general support unrelated to AML (e.g., account or gameplay issues), customers should continue to use the standard support contact: support@drgn.casino. However, if a customer has a specific complaint about an AML/KYC procedure (for instance, if they believe their account was unfairly suspended for verification), they can reach out to the Compliance Officer directly via the contact information above, or send the complaint through our support channels and it will be escalated to the Compliance team.

Revision History

- Version 1.0 – Effective 26 July 2024: Initial release of Dragon Money N.V.'s AML/CFT Policy.
- Version 2.0 – Effective 10 April 2025. This version was developed to meet the 2025 standards of the Curaçao Gaming Control Board and CGA template, consolidating prior drafts and incorporating all required sections (Audience, Approval/Review, Third-Party CDD, etc.). Approved by Dragon Money N.V. General Management and AML Compliance Officer.