
ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING (AML/CTF) POLICY

Humble Interactive Services N.V.

Effective Date: June 30, 2025

PREFACE:

This Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Policy has been developed in alignment with both Curaçao's legal framework and international standards aimed at combating financial crime.

On February 15, 2019, the Curaçao Gaming Control Board (GCB) was designated as the official AML/CTF supervisory authority for the gaming sector, with retroactive effect from January 1, 2016. The regulatory framework for AML/CTF compliance is grounded in the following key legal instruments:

- National Ordinance on the Reporting of Unusual Transactions (NORUT, N.G. 2017 no. 99)
- National Ordinance on the Identification when rendering Services (NOIS, N.G. 2017 no. 92)
- Sanctions National Ordinance (N.G. 2014 no. 55)
- Kingdom Sanctions Act (N.G. 2016 no. 54)

These laws are aligned with the 40 Recommendations of the Financial Action Task Force (FATF), the global standard for preventing money laundering and terrorist financing.

As a licensed business-to-consumer (B2C) gaming operator, Humble Interactive Services N.V. is committed to strict adherence to these obligations. This policy ensures the implementation of robust internal controls, comprehensive customer due diligence (CDD), real-time transaction monitoring, and prompt reporting of unusual or suspicious activity to the appropriate authorities, in full compliance with the requirements of the Curaçao Gaming Authority (CGA).

Moreover, as Curaçao is a member of the Caribbean Financial Action Task Force (CFATF), the jurisdiction is required to reflect FATF principles through its domestic AML/CTF measures. In this context, Humble Interactive Services N.V. reaffirms its unwavering commitment to safeguarding the integrity of its operations, maintaining the highest compliance standards, and contributing to the global fight against financial crime.

1. POLICY STATEMENT

Humble Interactive Services N.V. is committed to full compliance with Curaçao laws and regulations regarding Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF), including the National Ordinance on Games of Chance (NOGC), the National Ordinance on Identification in Service Provision (NOIS), the Ordinance on the Notification of Unusual Transactions (NORUT), and guidance from the Curaçao Gaming Authority (CGA). As a licensed B2C operator, the company acknowledges its elevated exposure to financial crime risks due to direct interaction with individual players. This policy sets out the principles and procedures to prevent misuse of the platform for ML/TF purposes.

2. PURPOSE

This policy outlines the framework adopted by Humble Interactive Services N.V. to detect, deter, and report suspected ML/TF activities. It provides operational guidance and compliance requirements for all employees and business partners, in line with CGA AML obligations and license conditions.

3. AUDIENCE

This policy applies to all employees, agents, affiliates, customer service providers, payment partners, and any third parties handling player registration, transactions, or compliance functions on behalf of Humble Interactive Services N.V.

4. DEFINITIONS

Key terms: Money Laundering (ML), Terrorist Financing (TF), Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), Suspicious Transaction Report (STR), Politically Exposed Person (PEP), Ultimate Beneficial Owner (UBO), Business Risk Assessment (BRA), Customer Risk Assessment (CRA), Compliance Officer (CO), and Curaçao Gaming Authority (CGA).

5. POLICY IMPLEMENTATION

5.1 BUSINESS RISK ASSESSMENT

Humble Interactive Services N.V. conducts an annual Business Risk Assessment (BRA) that evaluates products, services, target markets, delivery channels, and technology platforms for ML/TF vulnerabilities. The BRA is used to prioritize internal controls and resource allocation.

5.2 CUSTOMER RISK ASSESSMENT

At onboarding, each customer is assessed for risk using variables such as jurisdiction, payment method, gaming behavior, and device usage. High-risk profiles undergo EDD and ongoing review in accordance with CGA guidelines.

5.3 CUSTOMER ACCEPTANCE POLICY

Players must meet identity and age verification requirements. PEP and sanctions screening is conducted during onboarding. Players from sanctioned jurisdictions or who attempt to obscure identity are rejected. Ongoing re-verification occurs on thresholds or alerts.

5.4 CUSTOMER DUE DILIGENCE

Humble Interactive Services N.V. applies CDD measures prior to account activation or upon transactional triggers of NAF 4,000. Documentation includes proof of ID, proof of address, device fingerprinting, and source of funds where applicable. PEPs and individuals linked to suspicious networks are escalated to the MLRO.

5.5 ONGOING MONITORING

Automated and manual reviews are conducted daily. Alerts include:

- Large deposits with little gameplay;
- Multiple IP addresses or geolocation inconsistencies;
- Suspicious use of prepaid cards or virtual currencies;
- Frequent self-exclusion toggles or account resets.

5.6 RELIANCE ON THIRD PARTIES

When relying on PSPs or KYC vendors, Humble Interactive Services N.V. ensures that data is accessible, verifiable, and retained. Written agreements confirm that CDD responsibilities remain with the company, not the third party.

5.7 REPORTING OF UNUSUAL TRANSACTIONS

All staff must report suspected ML/TF activities to the Money Laundering Reporting Officer (MLRO). The MLRO assesses the need to file an .STR with the FIU Curaçao. Internal records are retained for a minimum of five years.

5.8 ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM

The AML program is updated annually and includes:

- Transaction monitoring protocols;
- Account freezing and blacklisting procedures;
- Audit schedules;
- KYC refresh procedures;
- Risk-based EDD playbooks.

6. COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE

Violations of this policy may result in internal disciplinary actions, contract termination, regulatory reporting, or legal proceedings. The company is committed to zero tolerance on ML/TF matters.

7. RELATED INFORMATION

CGA AML Policy (2025), NOIS, NORUT, Player Risk Matrix, KYC Templates, STR Filing Guide.

8. CONTACT INFORMATION

MLRO: support@spin.bet | Tel: +599 9 8432772

9. POLICY HISTORY

Initial issue – June 30, 2025.

10. POLICY URL

Only available offline

11. LEGAL AND REGULATORY FRAMEWORK

This policy implements and complies with the following legal instruments and regulatory frameworks:

- National Ordinance on Identification of Clients when Rendering Services (NOIS, N.G. 2017 no. 92)
- National Ordinance on the Reporting of Unusual Transactions (NORUT, N.G. 2017 no. 99)
- Ministerial Decree on Indicators (N.G. 2015 no. 73)
- Sanctions National Ordinance (N.G. 2014 no. 55)
- Kingdom Sanctions Act (N.G. 2016 no. 54)

These regulations form the basis for identification, verification, monitoring, and reporting processes implemented by Humble Interactive Services N.V.

12. INTERNATIONAL STANDARDS AND COOPERATION

Humble Interactive Services N.V. aligns its AML/CTF framework with the recommendations and standards issued by:

- Financial Action Task Force (FATF)
- Caribbean Financial Action Task Force (CFATF)

These frameworks promote cross-border cooperation in combating ML/TF and are critical to the continued licensing and credibility of Curaçao-licensed gaming operators.

ANNEXES

The following annexes support the implementation of this policy by providing practical tools and templates for compliance teams. They are to be used during customer onboarding, transaction monitoring, and internal reporting processes. Each annex aligns with Curaçao's AML regulatory requirements.

ANNEX A – CUSTOMER DUE DILIGENCE (CDD) CHECKLIST

The following checklist outlines the standard documentation and verification steps required during the Customer Due Diligence process:

- Valid government-issued ID (passport, national ID card, or driver's license)
- Proof of address (utility bill, bank statement, or government correspondence dated within last 3 months)
- Date of birth verification
- PEP screening and Sanctions list screening
- Selfie with ID (for biometric or liveness verification)
- Source of funds declaration (if required)
- Customer Risk Assessment form

ANNEX B – SUSPICIOUS TRANSACTION REPORT (STR) TEMPLATE

Reporting Officer: _____
Date of Report: _____
Player Username: _____
Full Name: _____
Date of Birth: _____
Country of Residence: _____
Nature of Suspicion: _____
Details of Transactions: _____
Supporting Documentation Attached: Yes / No
Recommended Action: _____
Filed to FIU: Yes / No – If yes, FIU Reference: _____

ANNEX C – CUSTOMER RISK ASSESSMENT (CRA) TEMPLATE

Customer ID: _____
Risk Rating: Low / Medium / High
Assessment Criteria:
- Jurisdiction Risk: _____
- Payment Method Risk: _____
- Behavior / Gameplay Risk: _____
- Source of Funds Risk: _____
- Device / IP Analysis: _____
EDD Required: Yes / No
Next Review Date: _____
Reviewer Name & Signature: _____