

Date: 4/11/2025

Version: 2.0

Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) Policy

Company: satfair.com/ Blue Sapphire N.V.

Introduction

Blue Sapphire N.V. a company incorporated in Curaçao, under registration number 0, with registration address Zuikertuintjeweg Z/N (Zuikertuin Tower) licensed and regulated by the Governor of Curaçao under the Remote Gaming Regulations, is steadfastly dedicated to preventing money laundering, terrorist financing, and other illicit activities within the online gaming industry. Operating under the stringent oversight of the Curaçao Gaming Authority (CGA), the company adheres to a robust legal framework that includes the Proceeds of Crime Act 2002 (Part 7), The Money Laundering, Terrorist Financing and Transfer of Funds Regulation no. 692 of June 26, 2017, the National Ordinance on Identification when Rendering Services (LID/NOIS), the National Ordinance on the Reporting of Unusual Transactions (LMOT/NORUT), the National Decree on Penalties and Administrative Fines for Service Providers, and the 2025 AML regulations issued by the CGA. Furthermore, satfair.com aligns its practices with international standards set by the Financial Action Task Force (FATF) and the Caribbean Financial Action Task Force (CFATF), including compliance with the FATF Travel Rule for cryptocurrency transactions. This commitment extends to safeguarding the integrity of the gaming industry by upholding the highest financial crime prevention standards across all financial transactions, gaming activities, customer interactions, and business relationships. By staying attuned to both national and international developments in AML/CFT initiatives, satfair.com ensures that its operations, reputation, and systems remain protected from exploitation for money laundering, terrorist financing, or other criminal purposes.

Objective of the Policy

- Maintain constant vigilance to minimize and manage reputational, legal, and regulatory risks.
- Uphold social duty to prevent serious crime and ensure systems are not abused for money laundering, terrorist financing, or other illicit activities.

Definitions and Abbreviations

- **AML:** Measures to prevent conversion of illicit funds into legitimate sources.
- **CFT:** Efforts to detect and prevent financial support for terrorist activities.

- **FIU:** Financial Intelligence Unit of Curaçao, responsible for analyzing suspicious transaction reports.
- **KYC:** Process of verifying customer identity and assessing risks.
- **MLRO:** Money Laundering Reporting Officer, responsible for monitoring and reporting suspicious activities.
- **PEP:** Politically Exposed Person, a customer in a prominent public position posing higher AML risks.

Regulatory Framework

- **National Regulations:**
 - Curaçao's Code of Criminal Law (Penal Code)
 - NORUT and NOIS
 - National and international sanction lists
- **International Regulations:**
 - FATF and CFATF guidelines
 - Alignment with global financial crime prevention measures

Obligations and Internal Controls

- **MLRO Responsibilities:**
 - Appoint a senior officer as the MLRO to oversee compliance with laws, regulations, and guidance notes.
 - Report all suspected money laundering attempts to the MLRO confidentially (no disclosure to customers).
 - MLRO submits Suspicious Activity Reports (SARs) to the FIU and liaises with relevant authorities.
 - Maintain registers for SARs, reporting actions, and trend analysis to strengthen controls.
- **Customer Due Diligence (CDD) and Know Your Customer (KYC):**
 - Implement a full KYC policy requiring identity verification (e.g., government-issued ID, proof of address, payment verification) before service access or large transactions (exceeding NAf. 4,000 or €2,130).
 - Apply enhanced due diligence (EDD) for high-risk customers (e.g., PEPs, high-risk jurisdictions, unusual transactions).

- Utilize online verification tools; request additional documents if criteria aren't met.
- Conduct biometric verification and digital identity authentication where applicable.
- **Risk-Based Approach (RBA):**
 - Conduct annual risk assessments (Business Risk Assessments and Customer Risk Assessments per CGA guidelines).
 - Categorize risks: customer, transaction, product/service, geographic.
 - Use automated transaction monitoring and AI-driven analytics for real-time fraud detection.
- **Record Keeping:**
 - Retain customer records, transaction logs, and risk assessments for at least five years in a secure, centralized compliance database.
 - Include timestamps, source of funds, and audit trails; available for regulatory audits.
- **Transaction Policies:**
 - No cash transactions; accept funds only via credit/debit cards, electronic/wire transfers, or approved methods.
 - Maintain a secure online list of registered players and their transaction histories.
 - Record all transactions; regularly check against fraud and social responsibility indicators.
 - Refund winnings/refunds to the original payment method where possible.
- **Staff Training:**
 - Provide initial and ongoing training on:
 - Personal responsibilities
 - Player identification and activity monitoring
 - Record-keeping and reporting suspicious transactions
 - Detecting unusual betting/deposit/withdrawal patterns, identity theft, and high-risk jurisdiction accounts

- Client due diligence (CDD), including enhanced requirements for PEPs
- **Suspicious Activity Reporting:**
 - Employees report suspicious activities (e.g., extreme player profiles, mismatched deposits) to the Risk Team/MLRO in handwritten form for confidentiality.
 - Prohibit tipping-off (disclosure to investigated parties); violators face legal penalties.
 - File SARs with the FIU for transactions exceeding NAf. 5,000 or showing structuring/layering signs.
 - Notify authorities within 24 hours of account suspension due to fraud, with evidence provided.
- **High-Risk Customers:**
 - Maintain a register of high-risk or PEP customers for increased scrutiny and frequent checks.
 - Terminate accounts with credible suspicion of fraudulent activity (e.g., forged documents, multiple accounts); retain funds pending investigation.
- **Cryptocurrency Compliance:**
 - Require enhanced KYC and source of funds verification for cryptocurrency transactions.
 - Accept only verified digital wallets/exchanges; comply with FATF Travel Rule.
 - Use blockchain analytics to monitor transaction flows.

Operational Policies

- **Account Restrictions:**
 - Prohibit anonymous/fictitious accounts, cash deposits, multi-account practices, and players under 18.
 - Limit payments exceeding €300 until identity, age, and residence are verified.
 - Close inactive accounts (30 months) and remit balances to players or the regulator if unlocatable.

- **Fraud and Disciplinary Measures:**

- Suspend accounts and immobilize funds if fraud is suspected (e.g., bank repudiation, third-party operation) until cleared by authorities.
- Investigate and discipline staff per employment law for illegal/inappropriate behavior (e.g., collusion with customers).

- **Withdrawal and Deposit Rules:**

- Process withdrawals via the original deposit method or bank transfer to a verified account.
- Minimum deposits: BRL 60, USD 10, EUR 10.
- Separate player funds legally from company funds; no loans or inter-player fund transfers allowed.
- Review deposit history, turnover, and gameplay before withdrawals to prevent money movement schemes.

Politically Exposed Persons (PEPs)

- Identify PEPs, their family members, and close associates per European and Curaçao guidelines:
 - **PEPs:** Individuals in prominent public roles (e.g., state officials, judges, ambassadors).
 - **Family Members:** Spouses, children, parents, siblings, etc.
 - **Close Associates:** Business partners or beneficial owners linked to PEPs.
- Collect data and apply EDD to minimize corruption and money laundering risks.

Forbidden Countries

- Restricted participation from:
 - United States and territories, Aruba, Bonaire, Curaçao, France, The Netherlands, Saba, Statia, St. Maarten, Singapore
 - Iran, North Korea, Albania, Barbados, Botswana, Cambodia, Jamaica, Haiti, Mauritius, Myanmar, Nicaragua, Pakistan, Panama, South Sudan, Syria, Yemen, Zimbabwe

Compliance and Enforcement

- Conduct independent third-party audits and internal reviews; address vulnerabilities with policy updates.

- Generate quarterly compliance reports; foster a compliance culture via risk awareness campaigns.
- Impose disciplinary actions (e.g., termination) for non-compliance; cooperate with regulatory investigations.
- Withhold funds and freeze/close accounts linked to illicit activity; terminate non-compliant third-party relationships.
- Review and update policy annually to reflect evolving CGA regulations and industry best practices.