

ANTI-MONEY LAUNDERING, COUNTERTERRORIST FINANCING, AND COUNTER-PROLIFERATION FINANCING POLICY

POLICY STATEMENT

Ecorpp Management N.V. ("Ecorpp") and its associated gaming operators are committed to conducting business with integrity, transparency, and strict adherence to all applicable AntiMoney Laundering (AML) and Counter-Terrorist Financing (CTF) and Counter Proliferation

Financing (CPF) regulations. As a licensed director and compliance service provider in Curaçao, Ecorpp upholds a zero-tolerance approach to money laundering, terrorist financing, and financial crimes that pose risks to the industry, the financial system, and national security.

To align with the National Ordinance on Games of Chance (LOK) 2024 and the Curaçao Gaming Authority (CGA) AML requirements, Ecorpp has implemented a comprehensive AML/CTF Compliance Program that incorporates a risk-based approach to identifying, mitigating, and managing financial crime risks. This program ensures that all operators under Ecorpp's management comply with:

- Regulatory requirements set forth by the Central Bank of Curacao and St. Maarten, Curaçao's Financial Intelligence Unit (FIU) and CGA.
- Know Your Customer (KYC) and Customer Due Diligence (CDD) obligations, including enhanced measures for high-risk transactions and customers.
- Mandatory reporting of unusual transactions, threshold-based reporting, and immediate escalation of suspicious activities.
- Strict internal and regulatory policies for transaction monitoring, record-keeping, and staff training.

The AML/CTF Compliance Program is Board-approved, continuously updated, and reinforced through stringent internal controls, governance structures, and independent audits.

Failure to comply with this Policy may result in disciplinary action, termination of business relationships, regulatory penalties, and criminal liability under Curaçao law.

Cover sheet

<u>Company name</u>	<u>version</u>
Spade and Scepter N.V.	1.4.2 including VASP risk policies
<u>License number CGA</u>	OGL/2024/1834/1057
<u>Domains related</u>	spadeandscepter.com
<u>Director</u>	<u>Ecorpp Management N.V.</u>
<u>Compliance Director</u>	<u>Derek Hendriks</u>
<u>Compliance Officer</u>	<u>Eliane Vazquez</u>
<u>MLRO</u>	
<u>Date:</u>	<u>19 September, 2025</u>

PURPOSE OF THIS POLICY

The purpose of this Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) Policy is to:

1. Establish Legal & Regulatory Compliance
 - o Ensure that Spade and Scepter N.V. and its gaming operators comply with all applicable AML/CTF laws, regulations, and directives under Curaçao's gaming framework.
 - o Adhere to the National Ordinance on Games of Chance (LOK) 2024, CGA's AML Guidelines (2025), and the Financial Intelligence Unit (FIU) of Curaçao's AML directives.
 - o Comply with the National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99 C.T.) ("NORUT"), The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92 C.T.)

- (“NOIS”), and o The National Ordinance on the Supervision of Trust Service Providers (N.G. 2019, no. 93 C.T) (“NOST”),
2. Define Responsibilities & Obligations o Outline the responsibilities of directors, officers, employees, and compliance personnel in preventing, detecting, and reporting money laundering and terrorist financing. o Set clear obligations for the Money Laundering Reporting Officer (MLRO) and Compliance Officers.
 3. Ensure Risk-Based AML Implementation o Implement a risk-based approach that aligns with FATF (Financial Action Task Force) international standards.
 - o Identify, assess, and mitigate customer, transaction, and jurisdictional risks associated with games of chance.
 4. Guide Personnel on AML Procedures o Provide a structured framework for recognizing and escalating suspicious activities and transactions.
 - o Offer step-by-step guidance on due diligence, transaction monitoring, and regulatory reporting.

This Policy applies to all directors, employees, agents, consultants, contractors, and thirdparty partners engaged in gaming operations under Ecorpp Management N.V.’s Management.

Any failure to adhere to this Policy will be subject to internal disciplinary actions and may lead to regulatory sanctions, legal consequences, and financial penalties in accordance with Curaçao’s AML legislation.

OVERSIGHT & COMPLIANCE MANAGEMENT

1. Compliance Governance & Responsibilities

Ecorpp Management N.V. is responsible for ensuring that all operators under its management implement robust AML/CTF measures in full compliance with the National Ordinance on Games of Chance (LOK) 2024 and the Curaçao Gaming Authority (CGA). Compliance is overseen at multiple levels, ensuring adherence to legal, regulatory, and ethical obligations.

1.1 Role of the Director (Ecorpp Management N.V.)

- The Director has ultimate responsibility for the AML/CTF Compliance Program, ensuring that policies, procedures, and internal controls effectively mitigate money laundering and terrorist financing risks.
- Senior management is required to:
 - o Ensure that all AML/CTF obligations are met, including KYC/CDD procedures, transaction monitoring, and regulatory reporting.
 - o Allocate adequate resources, training, and technology to support compliance efforts.

Approve and regularly review the risk assessment framework for identifying ML/TF vulnerabilities.

1.2 Appointment of the Money Laundering Reporting Officer (MLRO)

- The MLRO is the designated officer responsible for implementing and enforcing AML measures, ensuring regulatory reporting obligations are fulfilled.
- The MLRO's responsibilities include:
 - Receiving and assessing internal reports of suspicious transactions.
 - Submitting Unusual Transaction Reports (UTRs) to the Financial Intelligence Unit (FIU) via the goAML system.
 - Providing guidance and training to staff on AML/CTF compliance.
 - Conducting internal audits to assess the effectiveness of AML controls.
 - Liaising with regulatory bodies, law enforcement, and other stakeholders on AML matters.

1.3 Role of the Compliance Team & Risk Officers

- The Compliance Team supports the MLRO in executing the AML/CTF Compliance Program and ensuring alignment with CGA regulations.
- Responsibilities include:
 - Conducting enhanced due diligence (EDD) for high-risk transactions.
 - Overseeing politically exposed persons (PEP) screening and sanctions compliance.
 - Ensuring ongoing KYC/CDD verification and record-keeping compliance.

2. Regulatory Oversight & Reporting Requirements

2.1 Unusual Transaction Reporting (UTR) Requirements

- Any transaction deemed unusual or suspicious must be reported to the FIU of Curaçao via the goAML platform.
- Threshold-based reporting obligations:
 - Transactions of XCG. 5,000 or more must be flagged for review.
 - CDD is mandatory for transactions of XCG. 4,000 or higher.
 - Linked transactions exceeding XCG. 5,000 within a single gaming day require immediate escalation.
- Immediate reporting of transactions suspected to involve money laundering, terrorist financing, or fraud is mandatory.

2.2 Record-Keeping & Audit Obligations

- All AML-related records, including customer verification data, transaction reports, and internal reviews, must be retained for at least five (5) years after the end of the business relationship.

- Compliance audits must be conducted annually to assess adherence to Curaçao's AML/CTF framework and FATF guidelines.
- Any compliance deficiencies must be reported to senior management and corrective actions must be implemented.

1. MONEY LAUNDERING

1.1 Definition of Money Laundering

Money laundering (ML) is the process of disguising the proceeds of illegal activities to make them appear legitimate. Criminals use this process to integrate illicit funds into the economy, often exploiting vulnerable industries such as gaming and financial services.

Under the National Ordinance on Games of Chance (LOK) 2024) and Curaçao Gaming Authority (CGA), operators must actively detect, prevent, and report money laundering activities. Failure to do so can result in severe penalties, including license revocation, fines, and criminal liability.

Stages of Money Laundering

Money laundering typically occurs in three stages:

1. Placement – Illicit funds enter the financial system, often through deposits, purchases of gaming credits, or cash transactions.
2. Layering – Funds are moved through multiple transactions, making it difficult to trace their origin (e.g., repeated small deposits, quick withdrawals, or transfers between accounts).
3. Integration – Laundered funds re-enter the economy through investments, real estate, or gambling winnings.

Operators must monitor transactions at all stages and report suspicious activity to the Financial Intelligence Unit (FIU) via the goAML platform.

1.2 Examples of Money Laundering Risks in the Gaming Industry

B2C Risks (Business-to-Consumer)

Money laundering risks associated with individual players include:

- Deposit & Withdraw Without Gameplay – Players deposit large amounts, engage in minimal betting, and then withdraw funds to a different account.
- Use of Multiple Accounts – A single user creates multiple accounts to bypass transaction limits and detection systems.
- Anonymous Payment Methods – Customers use prepaid cards, cryptocurrency, or untraceable e-wallets to deposit and withdraw funds.
- Structuring Transactions – Customers break down large transactions into multiple smaller transactions (below XCG 5,000) to avoid detection.
- Chip Dumping & Collusion – Players deliberately lose bets to another player as a means of transferring illicit funds.

B2B Risks (Business-to-Business)

Operators must also be aware of money laundering risks in corporate relationships, including:

- Unverified or High-Risk Business Partners – A gaming operator receives funds from a company with unclear ownership or offshore ties.
- Frequent Changes in Ownership – A business undergoes multiple ownership changes within a short period, with no economic justification.
- Misuse of Affiliate or Agent Networks – Agents or affiliates use their position to process illicit funds through commission payments or bonuses.
- Cross-Border Transactions with Limited Documentation – Operators engage in financial transactions across multiple jurisdictions without clear business justifications.

Operators must apply enhanced due diligence (EDD) to high-risk business partners, ensuring UBO (Ultimate Beneficial Ownership) transparency.

1.3 Money Laundering Offences & Legal Consequences

Under Curaçao's AML regulations, the following constitute criminal money laundering offences:

- Concealing or disguising the source of illicit funds.
- Knowingly handling criminal property, including proceeds from fraud, drug trafficking, or corruption.
- Failing to report suspicious transactions to the FIU.
- Tipping off a customer that they are under investigation.

Penalties for Non-Compliance

- License revocation by the Curaçao Gaming Authority (CGA).
- Significant financial penalties (up to millions in XCG.).

- Criminal liability, including prison sentences for directors or compliance officers who fail to act.

Operators must ensure all transactions are monitored, and suspicious activities are reported without delay.

1.4 Knowledge or Suspicion of Money Laundering

AML laws require all personnel to report any suspicion of money laundering. Suspicion is defined as having reasonable grounds to believe that a transaction involves criminal activity.

- Operators should be particularly vigilant if a customer:
- Deposits large sums but refuses to provide source of funds documentation.
- Uses multiple accounts or frequently switches payment methods.
- Conducts high-value transactions from high-risk jurisdictions.
- Attempts to avoid KYC verification or provides false documents.

When suspicion arises, staff must immediately report to the MLRO, who will determine whether to file an Unusual Transaction Report (UTR) with the FIU.

1.5 Examples of Activities That May Lead to Knowledge or Suspicion

The following red flags may indicate potential money laundering:

B2C (Player-Related Red Flags)

- Unexplained Wealth – A customer with no clear income source wagers large amounts inconsistently.
- Rapid, Consecutive Transactions – Multiple deposits and withdrawals in a short period without gameplay.
- Third-Party Transactions – Funds are deposited from one account and withdrawn to another unrelated party.
- Sanctioned Entities or High-Risk Jurisdictions – Transactions involve countries flagged for money laundering risks.
- Refusal to Provide Information – Customers who resist KYC verification or provide misleading documentation.

B2B (Business Partner & Operator Red Flags)

- Frequent Ownership Changes – Unusual or unjustified shifts in business ownership.
- Unusual Transaction Flows – Large or irregular payments to unknown entities.
- Shell Companies & Offshore Accounts – Businesses with unclear ownership structures or offshore banking ties.
- Rapidly Changing Payment Methods – Operators that frequently switch financial institutions to avoid scrutiny.

If any of these red flags are detected, immediate reporting to the MLRO and FIU is required.

2. TERRORIST FINANCING

2.1 Definition of Terrorist Financing (TF)

Terrorist financing (TF) is the process of providing or collecting funds, by any means, with the intention or knowledge that they will be used for terrorist activities. Unlike money laundering, which aims to disguise the source of illicit funds, TF may involve both legitimate and illicit funds being used to finance acts of terrorism, recruit operatives, or sustain terrorist organizations.

Legal Framework & Operator Obligations

Under the National Ordinance on Games of Chance (LOK) 2024 and Curaçao Gaming Authority, all licensed operators must:

1. Implement strict due diligence to identify and prevent terrorist financing.
2. Report any suspicion of TF immediately to the Financial Intelligence Unit (FIU) via goAML.
3. Conduct ongoing monitoring to detect links to sanctioned individuals, high-risk jurisdictions, or known terrorist networks.

Failure to comply may result in criminal prosecution, regulatory fines, and license revocation.

2.2 Terrorist Financing Offences & Sanctions

Under Curaçao's AML/CTF laws, the following constitute terrorist financing offences:

- Knowingly providing financial support to a terrorist group, even if the funds originate from legal sources.
- Possessing or managing funds intended for terrorist activities.
- Engaging in transactions with designated terrorist organizations or individuals on global sanctions lists (e.g., UN, EU, OFAC).

- Failing to report known or suspected TF activity, making operators liable for negligence.

Penalties for Non-Compliance

- Severe criminal charges, including imprisonment.
- Regulatory fines and asset seizure.
- Permanent license revocation by the Curaçao Gaming Authority (CGA).

Operators must conduct real-time sanctions screening to prevent transactions involving individuals, businesses, or jurisdictions linked to terrorism.

2.3 Examples of Terrorist Financing Risks in the Gaming Industry

B2C (Player-Related TF Risks)

- Frequent Small Deposits Below Reporting Thresholds – Players structure transactions to evade detection (e.g., multiple deposits under XCG. 5,000).
- Unusual Payment Methods – Use of anonymous e-wallets, prepaid cards, or cryptocurrencies that enable untraceable transactions.
- Irregular Betting & Withdrawals – Customers deposit funds, engage in minimal gaming, and quickly withdraw funds to unrelated accounts.
- Connections to High-Risk Countries – Transactions involving regions flagged for terrorist activity or weak AML controls.

B2B (Business Partner TF Risks)

- Shell Companies & Complex Corporate Structures – Operators unknowingly receive funds from front companies linked to terrorism.
- Use of Agents or Third Parties to Move Funds – Affiliates or payment processors facilitate transactions on behalf of undisclosed entities.
- Frequent Cross-Border Transfers with Limited Justification – Businesses send or receive funds between multiple jurisdictions without clear business purpose.
- Business Partners with Sanctions Exposure – Engaging with vendors, suppliers, or partners that appear on sanctions watchlists.

Red Flags Indicating Potential Terrorist Financing

- Players reluctant to provide identity verification or source of funds.
- Businesses or individuals associated with known terrorist-linked charities or organizations.
- Transactions inconsistent with the customer's usual gaming behavior.
- Large donations or financial transfers made through gaming accounts with no legitimate purpose.

Operators must apply Enhanced Due Diligence (EDD) for any high-risk customers, businesses, or transactions suspected of TF.

2.4 CPF Offences & Legal Obligations

Operators must integrate sanctions screening tools capable of detecting:

- Individuals or entities listed under UN, EU, OFAC, and CBCS sanctions
- Transactions involving jurisdictions subject to CPF-related trade restrictions or arms embargoes
- Transfers potentially linked to dual-use goods or front companies operating in proliferation-sensitive industries

Screening systems must:

- Operate in real time
- Log all match evaluations
- Escalate matches to the MLRO for review and potential reporting to FIU

Operators must ensure staff are trained to recognize CPF-specific red flags and typologies.

Offences related to proliferation financing under Curaçao law and international conventions include:

- Providing, collecting, or processing funds knowing they are intended for use in nuclear, biological, or chemical weapons programs
- Facilitating transactions for entities on proliferation-related watchlists
- Failing to implement screening or to escalate suspicious CPF-linked activity
- Engaging in economic activities that support sanctioned weapons programs or jurisdictions

Penalties include:

- License revocation
- Criminal prosecution
- Unlimited fines

- Asset seizure

3. OPERATOR OBLIGATIONS UNDER THIS AML POLICY

3.1 Obligations of Spade and Scepter N.V

As a licensed operator under Curaçao's National Ordinance on Games of Chance (LOK) 2024, Spade and Scepter N.V. is required to implement a risk-based approach to prevent money laundering and terrorist financing. This means that AML/CTF measures must be proportionate to the risks posed by customers, transactions, and jurisdictions.

To comply with Curaçao Gaming Authority (CGA) AML Policy 2025, Spade and Scepter N.V. and its operations must:

- Conduct risk-based customer due diligence (CDD) and enhanced due diligence (EDD) for high-risk clients.
- Monitor transactions in real-time to detect unusual or suspicious activity.
- Report Unusual Transaction Reports (UTRs) and Suspicious Activity Reports (SARs) to the Financial Intelligence Unit (FIU).
- Screen customers, partners, and transactions against global sanctions lists (e.g., UN, EU, OFAC).
- Implement internal AML controls, including regular staff training and independent audits.
-

Non-compliance may result in license revocation, financial penalties, or criminal prosecution.

Incorporate Counter-Proliferation Financing (CPF) detection measures into the compliance program, including the identification of transaction types, counterparties, and jurisdictions associated with weapons of mass destruction financing.

Evaluate and respond to proliferation financing typologies published by FATF, FIU Curaçao, and international regulatory bodies.

3.2 Risk Assessment & Ongoing Monitoring

3.2.1 Risk-Based Approach

Spade and Scepter N.V. must conduct annual risk assessments to evaluate:

- Customer risk – Based on player profiles, transaction behaviour, and source of funds.
- Jurisdictional risk – Exposure to high-risk countries with weak AML enforcement.
- Product risk – Gaming services that may facilitate money laundering, such as peer-to-peer betting.
- Payment risk – Use of anonymous payment methods like cryptocurrency or prepaid cards.
- **Proliferation risk** – Business relationships or transactions involving countries subject to UN arms embargoes, dual-use goods, or parties listed in proliferation financing guidance.

3.2.2 Ongoing Monitoring & Red Flags

Spade and Scepter N.V. must continuously monitor all and any transactions to identify ML/TF red flags, including:

- Customers who frequently deposit and withdraw funds without gaming activity.
- Rapid, large, or structured transactions below reporting thresholds.
- Accounts linked to sanctioned individuals or politically exposed persons (PEPs).
- B2B partners engaged in unusual cross-border transactions.

All high-risk transactions must be escalated to the MLRO for review. If necessary, a UTR/SAR must be filed with the FIU.

Additional CPF-specific red flags may include:

- Transactions involving entities in jurisdictions under UN Security Council Resolutions related to non-proliferation (e.g., DPRK, Iran).
- Use of shell or front companies without verifiable business purpose.
- Transfers involving dual-use goods or suppliers operating in weapons-related industries.
- Affiliates or agents structuring payments to mask the true origin of funds.

All CPF red flags must be reported internally and reviewed by the MLRO.

4. POLICIES & PROCEDURES

4.1 Training & Awareness

4.1.1 AML/CTF Training Requirements Under LOK & NORUT

Under the National Ordinance on Games of Chance (LOK) 2024 and the National Ordinance Reporting Unusual Transactions (NORUT), all employees and relevant stakeholders involved in gaming operations must receive ongoing AML/CTF training. The goal is to ensure that all personnel understand:

- Their legal obligations under LOK & NORUT, including reporting responsibilities.
- How to identify money laundering and terrorist financing risks in gaming transactions.
- Steps to take when encountering suspicious activity.

Failure to comply with training requirements can result in regulatory fines, disciplinary actions, or criminal liability under Curaçao's AML laws.

Training must also cover CPF-related risks, including typologies of proliferation financing, screening procedures for CPF watchlists, and escalation steps when such risks are identified. This includes specific training on FATF Recommendation 7 and proliferation-related sanctions regimes (e.g., UN DPRK/Iran designations).

4.1.2 Training Frequency & Mandatory Topics

Initial Training – All employees must complete AML/CTF training within 30 days of starting their role.

Annual Refresher Courses – Ongoing training ensures employees stay updated on new AML threats, LOK amendments, and NORUT obligations. **Job-Specific AML Modules:**

- For Customer-Facing Staff: Identifying suspicious gaming patterns.
- For Compliance Teams: Filing UTRs/SARs under NORUT guidelines.
- For Senior Management: Overseeing AML/CTF risk management strategies.

4.1.3 Competency Assessment & Record-Keeping

Employees must pass AML knowledge assessments after training.

Training records must be maintained for at least five (5) years and made available for CGA or FIU audits.

4.2 Money Laundering Reporting Officers (MLRO) & Compliance Oversight

4.2.1 Appointment of MLRO & Responsibilities

Under LOK 2024, every licensed operator must appoint a Money Laundering Reporting Officer (MLRO) who is responsible for:

- Receiving and analysing internal reports of suspicious transactions.
- Filing Unusual Transaction Reports (UTRs) with the Financial Intelligence Unit (FIU) via NORUT requirements.
- Ensuring compliance with Curaçao's AML/CFT regulations.
- Providing guidance and training to employees on AML policies.
- Liaising with regulatory authorities (CGA, FIU, law enforcement) on AML/CTF matters.
- Coordinating the operator's CPF compliance efforts, including sanctions list screening, review of cross-border transfers, and escalation of red flags to appropriate authorities.

4.2.2 Deputy MLRO & Compliance Officers

A Deputy MLRO (DMLRO) can be designated to support the MLRO and act as a backup in their absence.

A dedicated Compliance Team must oversee:

- Real-time transaction monitoring & risk assessments.
- Review of NORUT reporting obligations.
- Ensuring customer due diligence (CDD) and enhanced due diligence (EDD) procedures are followed.

4.2.3 Compliance Committee & Internal Audits

Quarterly compliance committee meetings must be held to review AML effectiveness. Independent audits must be conducted annually to assess:

- Effectiveness of AML controls & procedures.
- Compliance with NORUT reporting requirements.
- Any identified AML risks & remediation efforts.
- CPF controls must also be reviewed to ensure compliance with FATF R7 and UN sanctions enforcement

5. PERSONNEL OBLIGATIONS

5.1 Primary Obligations Under LOK & NORUT

All personnel working for Spade and Scepter N.V., including employees, contractors, agents, and third-party service providers, must comply with the National Ordinance on Games of Chance (LOK) 2024 and the National Ordinance Reporting Unusual Transactions (NORUT). These laws impose strict anti-money laundering (AML) and counter-terrorist financing (CTF) obligations, requiring personnel to:

- Adhere to AML/CTF policies and procedures as defined by Spade and Scepter N.V. and Curaçao regulatory authorities.
- Identify and report suspicious transactions following NORUT reporting requirements.
- Ensure customer due diligence (CDD) and enhanced due diligence (EDD) measures are applied properly.
- Protect confidential AML-related information and avoid unauthorized disclosures ("tipping off").
- The institution conducts an annual SIRA in accordance with LOK Art. 25 and CGA risk-based guidance. The SIRA identifies integrity risks by customer type, product, geography, and delivery channel, resulting in risk ratings and tailored controls

Personnel must also be trained in CPF detection protocols, particularly when handling crossborder transactions, corporate clients, or jurisdictions flagged for proliferation risk.

Failure to comply with these obligations may result in disciplinary action, regulatory penalties, criminal liability, and potential revocation of gaming licenses.

5.2 Reporting Obligations: Suspicious Transactions & Unusual Activity

Under NORUT, all personnel must report any transaction or activity that appears suspicious. These reports must be submitted to the Money Laundering Reporting Officer (MLRO) and, when necessary, escalated to the Financial Intelligence Unit (FIU) via goAML.

5.2.1 Internal Reporting Procedures

If an employee detects suspicious activity, they must:

1. Immediately notify the MLRO using the designated reporting forms.
2. Refrain from alerting the customer or third party (to avoid tipping off).
3. Provide supporting documentation (e.g., transaction logs, customer profiles).

The MLRO must then:

1. Assess the report and determine if an Unusual Transaction Report (UTR) is required.
2. File the UTR with the FIU through the goAML system, if necessary.
3. Maintain records of all reports for a minimum of five (5) years.

5.3 MLRO/DMLRO Reporting Responsibilities Under NORUT

The MLRO and Deputy MLRO (DMLRO) are responsible for ensuring compliance with mandatory reporting obligations under NORUT. Their key responsibilities include:

- Filing Unusual Transaction Reports (UTRs) within the required timeframes.
- Escalating Suspicious Activity Reports (SARs) when necessary to law enforcement.
- Monitoring transactions for red flags and implementing preventive measures.
- Ensuring all employees understand their AML/CTF reporting duties.

Failure to report suspicious or unusual transactions may result in legal consequences for both individuals and Spade and Scepter N.V..

6. INTERNAL CONTROLS

6.1 Customer Due Diligence (CDD) Obligations Under LOK & NORUT

Customer Due Diligence (CDD) is a mandatory process under the National Ordinance on Games of Chance (LOK) 2024 and the National Ordinance Reporting Unusual Transactions (NORUT). It requires gaming operators under Spade and Scepter N.V. to verify the identity of customers and assess their risk of involvement in money laundering (ML) and terrorist financing (TF).

Operators must apply CDD in the following situations:

- When establishing a new business relationship with a customer.
- When a customer conducts transactions equal to or exceeding XCG. 4,000 (whether in a single transaction or through linked transactions).
- When there is suspicion of ML/TF activity, regardless of the transaction amount.
- When the veracity of previously obtained customer information is in doubt.

CDD includes:

Identity verification – Obtaining and verifying official identification (passport, national ID, utility bills).

Source of funds checks – Ensuring the customer's funds originate from legitimate sources.

Ongoing monitoring – Continuously reviewing customer activity for red flags or unusual behaviour.

6.1.1 Requirement to Carry Out CDD

Operators must not process transactions or establish business relationships unless CDD is successfully completed.

If a customer fails to provide the required information:

The relationship must be terminated immediately.

A Suspicious Activity Report (SAR) must be filed with the FIU if money laundering is suspected.

6.1.2 Enhanced Due Diligence (EDD) for High-Risk Customers

Certain customers pose a higher risk and require Enhanced Due Diligence (EDD) under LOK and NORUT. This applies to:

- Politically Exposed Persons (PEPs) – Individuals who hold prominent public positions (or their relatives/close associates).
- Customers from high-risk jurisdictions – Countries with weak AML controls or international sanctions.
- Customers engaging in complex or unusually large transactions.

EDD measures include:

Obtaining additional verification documents (e.g., proof of income, financial statements).

Conducting deeper investigations into the customer's financial background.

Requiring senior management approval before processing transactions. Applying stricter transaction monitoring.

6.1.3 Simplified Due Diligence (SDD) for Low-Risk Customers

In limited cases, Simplified Due Diligence (SDD) may apply when a low ML/TF risk is determined. This typically applies to:

Customers using low-risk financial institutions that have strong AML measures.

Even under SDD, transaction monitoring must still be conducted, and operators must reassess risks periodically.

6.1.4 CDD Measures Include

CDD must follow a structured process:

- Identifying & verifying the customer – Obtaining and validating personal identification documents.
 - Determining the Ultimate Beneficial Owner (UBO) – Identifying individuals who control or benefit from corporate accounts.
 - Assessing the source of wealth & funds – Confirming that money used for gaming is from legitimate sources.
 - Ongoing monitoring – Ensuring the customer’s transactions remain consistent with their profile.
-

6.1.5 Enhanced Due Diligence (EDD) Measures

When EDD is required, operators must:

- Obtain additional documentation proving the legitimacy of funds.
- Monitor high-risk accounts more frequently for suspicious activity.
- Implement transaction limits for PEPs or high-risk jurisdictions.
- Conduct periodic reviews to reassess risk levels.

Failure to apply EDD where required can lead to regulatory penalties and possible license revocation by the Curaçao Gaming Authority (CGA).

When CPF risks are identified, operators must apply EDD equivalent to or greater than that required for PEPs. This includes enhanced scrutiny of UBOs, source of funds, and business purpose behind transactions potentially linked to sanctioned weapons programs or jurisdictions.

6.1.6 Beneficial Ownership Requirements

Operators must ensure they identify the Ultimate Beneficial Owner (UBO) for any corporate customer. This means determining:

- Who ultimately owns or controls 10% or more of a company's shares or voting rights.
- Whether any beneficial owners are linked to high-risk entities or jurisdictions.
- If a UBO is a PEP, additional EDD measures must be applied.

If the UBO cannot be determined, operators must file a report with the FIU.

6.1.7 Identification & Verification Process

Operators must collect and verify:

For Individuals:

- Full name, date of birth, and nationality.
- Government-issued identification (passport, national ID, driver's license).
- Residential address verification (utility bill, bank statement).

For Corporate Clients:

- Company registration documents.
 - Shareholder structure and UBO details.
 - Proof of business activity (financial records, tax filings).
-

6.1.8 Timing of Verification

CDD/EDD must be completed before any gaming transactions take place. However, in limited cases where immediate verification is not possible, operators may:

Temporarily allow transactions while verification is pending, but only if ML/TF risk is low. Set strict transaction limits until full verification is complete. Terminate the relationship immediately if verification fails.

6.1.9 Ongoing Monitoring & Transaction Review

Operators must continuously review customer activity to detect suspicious behaviour.

- Regular checks on customer risk levels.
- Automated alerts for suspicious deposit and withdrawal patterns.
- Special scrutiny for large or complex transactions.

6.1.10 Record-Keeping Obligations

Under LOK 2024 and NORUT, operators must retain AML-related records for at least five (5) years, including:

- Customer identification data & transaction records.
- Risk assessments & due diligence reports.
- UTRs/SARs filed with the FIU.
- Internal AML compliance audits & staff training records.

Failure to maintain proper AML records can result in regulatory sanctions, financial penalties, and criminal liability.

6.2 Politically Exposed Persons (PEPs) & Sanctions Screening

Operators must:

Identification of the ultimate beneficial owner (UBO) and determination of PEP status shall be mandatory at onboarding and during ongoing monitoring.

Screen all customers against global PEP & sanctions lists (UN, EU, OFAC).

Apply enhanced due diligence to all identified PEPs.

Prohibit transactions with individuals or entities under international sanctions.

Extend sanctions screening to include CPF-related designations (e.g., UN Security Council Resolutions 1540, 1718, 2231)

During player onboarding, the UBO must be identified, and screening for Politically Exposed Persons (PEPs) is mandatory. Results must be documented and reviewed by the AMLCO

Recommendations is to use automated, real-time systems that log alerts and record escalation decisions.

6.3 Personnel Measures & Employee Screening

All employees in sensitive AML roles must undergo:

1. Background checks before hiring.
 2. AML/CTF training to recognize ML/TF threats.
 3. Ongoing compliance monitoring.
-

6.4 Independent Audit & AML Controls

Operators must conduct annual independent AML audits to review:

1. Effectiveness of internal AML policies.
 2. Compliance with LOK/NORUT & FIU requirements.
 3. Gaps or deficiencies in AML enforcement.
-

6.5 Contractual Language & AML Clauses

All business agreements must include AML compliance clauses, requiring:

Third-party affiliates, agents, and partners to comply with Curaçao AML laws.
Termination rights if AML violations occur.

6.6 Record-Keeping & Data Protection

All AML records must be stored securely and made available for regulatory inspections.
Customer data must be protected under data privacy laws, preventing unauthorized access.

6.7 Counter-Proliferation Financing (CPF) Controls

Operators must implement formal controls to detect and prevent CPF risks:

- Screen customers and transactions against CPF-related watchlists (UN, EU, OFAC, CBCS).
- Flag and escalate all transactions involving dual-use goods, high-risk jurisdictions, or shell companies.
- Apply EDD to any customer, agent, affiliate, or partner linked to possible proliferation concerns.
- Conduct regular risk assessments to identify exposure to CPF risks in products, jurisdictions, or partnerships.



Red Flags may include:

- Cross-border payments with no logical business purpose
- Corporate clients with opaque ownership from sanctioned jurisdictions
- Affiliates that change bank accounts or jurisdictions frequently
- Transactions with vague or incomplete descriptions from restricted countries

All red flags must be escalated to the MLRO. Reports must be filed with the FIU as required.

6.8 Virtual Asset Transactions (see appendix D)

Customers using virtual assets (cryptocurrencies) are automatically classified as high risk. Enhanced Due Diligence is triggered for crypto deposits above €2,000 (or 4,000 XCG equivalent).

Wallet ownership must be verified via signed message or test transaction. Transactions are screened through blockchain analysis tools for exposure to mixers, darknet markets, and sanctioned addresses. Use of privacy coins or anonymous exchanges is prohibited. All crypto transactions are flagged for review by the AMLCO.

For the Virtual Assets Policy, please refer appendix D

6.7 Reliance on Third Parties

Spade and Scepter N.V. may rely on regulated third parties for certain KYC elements only where a formal agreement exists and the third party is located in a jurisdiction applying equivalent AML/CFT standards. The third party must make all documentation available immediately upon request. The ultimate responsibility for compliance remains with Spade and Scepter N.V..

APPENDICES

APPENDIX A – APPLICABLE LEGISLATION, REGULATIONS & GUIDANCE

Operators under Spade and Scepter N.V.'s management must comply with all Curaçao AML/CTF regulations, as well as relevant international standards. Below is an overview of the key legislation governing AML compliance:

A.1 Curaçao Legislation

CBCS AML/CTF/CPF Circulars and Guidance Notes (2023–2025)

National Ordinance on Games of Chance (LOK) 2024

- Establishes the legal framework for gaming operators in Curaçao.
- Defines AML/CTF compliance obligations, including customer due diligence, reporting, and risk assessments.
- Mandates internal controls and governance measures to prevent financial crime.

National Ordinance Reporting Unusual Transactions (NORUT)

- Requires operators to identify and report Unusual Transaction Reports (UTRs) to the Financial Intelligence Unit (FIU).
- Establishes legal requirements for record-keeping, sanctions screening, and MLRO responsibilities.

National Ordinance on Identification when Rendering Services (NOIS)

- Mandates strict identity verification procedures for gaming operators.
- Outlines requirements for CDD, EDD, and beneficial ownership transparency.

Financial Intelligence Unit (FIU) Directives

- Specifies the format and procedures for submitting UTRs/SARs via the goAML platform.
- Requires enhanced monitoring and reporting for transactions linked to high-risk jurisdictions.

A.2 International Regulations & Standards

Financial Action Task Force (FATF) Recommendations

- Establishes global AML/CTF best practices for identifying and mitigating financial crime risks.
- Requires a risk-based approach to compliance, sanctions screening, and transaction monitoring.

United Nations & European Union Sanctions

- Prohibits transactions with sanctioned individuals, countries, or organizations linked to ML/TF.
- UN Security Council Resolutions 1540, 1718, 2231 (proliferation-related)
- FATF Recommendation 7 – Proliferation Financing
- EU Dual-Use Regulation (for reference in corporate assessments)
-

Egmont Group Guidelines for FIUs

- Defines the international framework for suspicious transaction reporting and FIU cooperation.

APPENDIX B – RELATED DOCUMENTS & AML POLICY REFERENCES

1. Blocked geographies

- Aruba
- Australia
- Austria
- Belgium
- Bonaire
- Bulgaria
- Canada
- Christmas Island
- Curaçao
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Greenland
- Guadeloupe
- Hungary
- Ireland
- Italy
- Kazakhstan
- Latvia
- Liechtenstein
- Lithuania
- Luxembourg
- Malta
- Martinique
- Netherlands
- Norway
- Poland
- Portugal
- Puerto Rico
- Romania
- Saba
- Saint Barthélemy
- Saint Martin
- Sint Eustatius



- Sint Maarten
- Saudi Arabia
- Singapore
- Slovakia
- Slovenia
- Spain
- Sweden
- Switzerland
- United Arab Emirates
- United States
- Ukraine

APPENDIX C – DETERMINING A HIGH RISK OF MONEY LAUNDERING

Operators must assess ML/TF risks using a risk-based approach, considering the following high-risk indicators:

C.1 Customer-Related Risk Factors

- Politically Exposed Persons (PEPs) – Individuals in government, judiciary, military, or public office.
- Unverified or false identities – Customers providing incomplete or forged documents.
- Use of multiple accounts – Customers controlling numerous accounts to obscure fund flows.
- High-risk nationalities – Customers from jurisdictions flagged for AML deficiencies by the FATF.

C.2 Transaction-Related Risk Factors

- Large cash deposits or structured transactions – Multiple smaller transactions below XCG. 5,000 to evade detection.
- Deposit & withdrawal without gameplay – Customers funding accounts with large amounts but engaging in minimal or no gambling.
- Use of anonymous payment methods – Transactions involving prepaid cards, cryptocurrencies, or third-party accounts.
- Frequent cross-border transfers – Gaming funds moving across multiple jurisdictions without business justification.

C.3 Business Partner & Operator Risks (B2B)

- Unusual or unexplained ownership structures – Corporate clients with complex or opaque shareholding arrangements.
- Frequent changes in company directors or UBOs – Businesses that repeatedly modify ownership or directorship.
- High-risk agent or affiliate relationships – Third parties processing gaming funds with limited oversight or accountability.
- Operators engaging in excessive offshore transactions – Funds moving between multiple entities without clear economic purpose.

Operators must apply enhanced due diligence (EDD) to any customer, business partner, or transaction that meets these high-risk criteria.

APPENDIX D – VIRTUAL ASSET RISK MANAGEMENT POLICY

Spade and Scepter N.V.

1. PURPOSE AND SCOPE

This Virtual Asset Risk Management Policy establishes the framework for identifying, assessing, mitigating, and monitoring risks associated with the use of virtual assets (cryptocurrencies) within the operations of Spade and Scepter N.V.

This policy forms part of the overall AML/CTF/CPF compliance program and must be read in conjunction with the AML Policy (v1.4).

This policy applies to:

- All customers using virtual assets
- All transactions involving virtual assets
- All employees and third parties involved in crypto processing

2. LEGAL AND REGULATORY FRAMEWORK

This policy is based on:

- National Ordinance on Games of Chance (LOK, 2024) – Article 15
- National Ordinance on Identification when Rendering Services (NOIS, PB 2017, no. 92)
- National Ordinance on the Reporting of Unusual Transactions (NORUT, PB 2017, no. 99)
- CGA AML/CFT Policy (2025)
- FIU Curaçao reporting requirements (goAML)

- FATF Recommendations (including Recommendation 15 and 16)

All virtual asset activities must comply with the above laws.

3. RISK-BASED APPROACH TO VIRTUAL ASSETS

3.1 Risk Classification

All customers using virtual assets are classified as high risk by default.

This classification is based on:

- Pseudonymity of blockchain transactions
- Cross-border nature of virtual assets
- Increased exposure to money laundering typologies

3.2 Inherent Risks

The following risks are identified:

- Anonymity risk
- Layering risk through multiple wallets and exchanges
- Velocity risk (rapid movement of funds)
- Obfuscation risk (mixers, tumblers)
- Jurisdictional risk (high-risk or sanctioned countries)

3.3 Risk Mitigation

Risk is mitigated through:

- Enhanced Due Diligence (EDD)

- Blockchain analytics tools
- Wallet verification
- Ongoing monitoring

Residual risk is accepted only where controls are effective and documented.

4. CUSTOMER DUE DILIGENCE (CDD)

4.1 Mandatory KYC

Customers are not permitted to use virtual assets unless:

- Full KYC/CDD has been completed

This is required under NOIS and LOK Article 15.

4.2 Enhanced Due Diligence (EDD)

EDD applies to:

- All crypto users
- Transactions $\geq$ EUR 2,000 / 4,000 XCG equivalent
- High-risk jurisdictions
- PEPs
- Suspicious activity

EDD measures include:

- Source of funds verification
- Additional documentation
- Senior management approval

5. WALLET VERIFICATION

All wallets must be verified prior to use via:

- Signed message, or
- Test transaction

Unverified wallets are not permitted.

6. PROHIBITED ACTIVITIES

The following are prohibited:

- Privacy coins (e.g. Monero)
- Anonymous or unverified wallets
- Mixers and tumblers
- Sanctioned wallet addresses
- Darknet-related transactions

Detection results in:

- Immediate restriction
- MLRO escalation
- Possible FIU reporting

7. TRANSACTION MONITORING

7.1 Blockchain Monitoring

All transactions are monitored using blockchain analytics tools, including:

- Wallet risk scoring
 - Sanctions exposure
 - Darknet links
 - Mixer usage
 - Cross-chain activity

7.2 Red Flags

Indicators include:

- Rapid deposits and withdrawals without gameplay
- Frequent wallet changes
- Structuring below thresholds
- Multiple wallets per user
- High-risk jurisdiction exposure
- Chain hopping or layering

8. REPORTING OBLIGATIONS

8.1 FIU Reporting (NORUT)

Transactions must be reported where:

- XCG 5,000 threshold is met, or
- Suspicion exists

Crypto-specific triggers:

- Sanctioned wallet exposure
 - Mixer usage
 - Inconsistent behaviour
 - Refusal to provide source of funds
-

8.2 Tipping-Off Prohibition

Employees must not disclose:

- That a report has been filed
- That an investigation is ongoing

9. TRAVEL RULE CONSIDERATIONS

Where applicable:

- Originator and beneficiary data must be obtained
- Incomplete data must be escalated

Aligned with FATF Recommendation 16.

10. GOVERNANCE

10.1 MLRO

Responsible for:

- Oversight of crypto monitoring
- Review of alerts
- FIU reporting
- Record keeping

10.2 Compliance Function

Responsible for:

- Daily monitoring
- Risk assessment updates
- Policy enforcement

10.3 Audit

Crypto controls are subject to:

- Annual independent audit
- Internal control review

11. RECORD KEEPING

Records retained for minimum five (5) years:

- Wallet verification
- Transactions
- Blockchain analysis
- FIU reports
- Internal investigations

12. TRAINING

Staff must receive training on:

- Crypto AML risks
- Monitoring tools
- Red flags
- Reporting obligations

At onboarding and annually.

13. POLICY REVIEW

This policy must be:

- Reviewed annually
- Updated for regulatory changes
- Board approved

APPENDIX E – AML/CFT/CPF COMPLIANCE POLICY OF VEGAS GAMES INC (NEVADA, USA)

1. POLICY STATEMENT

Vegas Games Inc., incorporated in the State of Nevada, United States, is committed to upholding the highest standards of Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) compliance. As a gaming company operating under U.S. jurisdiction and with global affiliations, we maintain a zerotolerance approach toward the misuse of our platforms for money laundering, terrorist financing, or illicit financial activities.

This policy ensures compliance with:

- The Bank Secrecy Act (BSA)
- The USA PATRIOT Act
- U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) requirements
- Office of Foreign Assets Control (OFAC) sanctions regulations
- FATF Recommendations applicable to private sector entities

2. LEGAL FRAMEWORK & SCOPE



This AML/CFT/CPF policy is developed in accordance with the legal framework governing U.S.-based financial institutions and casinos, including:

- **Bank Secrecy Act (BSA)**
- **Title 31 CFR Chapter X** – FinCEN regulations for casinos and gaming entities
- **USA PATRIOT Act** – Sections relevant to due diligence and reporting obligations
- **OFAC Regulations** – Blocking and prohibition of transactions involving designated parties
- **FATF Recommendations** – International compliance alignment
- **Nevada Gaming Control Board (NGCB)** – Regulatory expectations for gaming licensees

This policy applies to all directors, officers, employees, and third parties associated with Vegas Games Inc., both at corporate and operational levels.

3. GOVERNANCE & COMPLIANCE RESPONSIBILITIES

3.1 Board Oversight

The Board of Directors is responsible for the approval, oversight, and periodic review of this policy, ensuring that adequate resources are allocated for AML/CFT/CPF compliance.

3.2 AML Compliance Officer (AMLCO)

An AML Compliance Officer has been designated and vested with the following responsibilities:

- Implementing and maintaining the AML Program
- Filing Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTRs) with FinCEN
- Conducting internal investigations and liaising with FinCEN, OFAC, and the NGCB
- Maintaining internal records of all AML-relevant documents
- Ensuring risk assessments and policy updates occur at least annually



3.3 Training and Awareness

All employees must undergo:

- Mandatory AML training at onboarding
- Annual refresher training
- Role-specific training for high-risk functions (e.g., compliance, finance, and customer-facing staff)

Training covers identification of suspicious activity, OFAC compliance, SAR/CTR procedures, and CPF typologies.



4. CUSTOMER DUE DILIGENCE (CDD) AND RISK CLASSIFICATION

4.1 Know Your Customer (KYC)

Vegas Games Inc. employs a risk-based approach to CDD, applying varying levels of scrutiny based on customer profile. Required elements include:

- Verification of identity using government-issued ID
- Proof of address
- Collection of SSN or ITIN for U.S. residents
- Beneficial ownership disclosure for corporate clients (25% threshold) • Source of funds declarations for high-value players

4.2 Enhanced Due Diligence (EDD)

EDD is mandatory for:

- Politically Exposed Persons (PEPs)
- Customers from FATF-listed high-risk jurisdictions
- Cryptocurrency users with high-volume transactions
- High-net-worth individuals depositing or withdrawing $\geq$ USD 10,000/month

EDD measures include deeper background checks, open-source intelligence reviews, and mandatory source of wealth verification.

4.3 Ongoing Monitoring

Transactions are continuously monitored using automated tools and manual oversight. Highrisk behaviors triggering alerts include:

- Rapid, repeated deposits/withdrawals without gameplay
- Use of third-party funding sources

- IP geolocation inconsistencies
- Repeated near-threshold transactions (structuring)

5. TRANSACTION MONITORING & REPORTING

5.1 Suspicious Activity Reports (SARs)

Suspicious activities must be reported internally and escalated to the AMLCO. The AMLCO is responsible for evaluating and, where appropriate, submitting a SAR to FinCEN within 30 days.

Examples of reportable conduct:

- Unexplained large transactions
- Altered or falsified KYC documentation
- Attempted circumvention of AML controls
- Refusal to provide source of funds

5.2 Currency Transaction Reports (CTRs)

Cash transactions exceeding USD 10,000 in a single day (by one or multiple related transactions) trigger a CTR, filed within 15 days per FinCEN requirements.

5.3 Record-Keeping Obligations

All AML-related records must be retained for a minimum of five (5) years. This includes:

- KYC files
- SAR/CTR submissions
- Internal alerts and investigations
- Training logs

- Audit results
-

6. COUNTER-TERRORIST FINANCING (CTF)

Vegas Games Inc. actively screens all customer and transaction data against OFAC's SDN List and other relevant watchlists. Any positive or potential matches are escalated to the AMLCO for further evaluation.

CTF obligations include:

- Blocking property of designated terrorists and organizations
 - Prohibiting any service provision to entities identified under the Global Magnitsky Act or similar U.S. sanctions regimes
 - Maintaining real-time sanctions screening and logging all match dispositions
-

7. COUNTER-PROLIFERATION FINANCING (CPF)

In alignment with FATF Recommendation 7 and U.S. sanctions enforcement (OFAC and UN), the company has adopted the following CPF measures:

- Screening of all transactions for CPF watchlist indicators
- Identifying dual-use goods or front company indicators
- Blocking and reporting transactions related to Iran, DPRK, and other designated jurisdictions

Employees are trained to recognize CPF typologies, including:

- Unusual fund flows from sanctioned regions
- Customers engaged in industries linked to weapons development or dual-use technologies

8. VIRTUAL ASSET CONTROLS

Where permitted by law, Vegas Games Inc. may accept virtual assets under enhanced controls. Requirements include:

- Full wallet attribution (KYT)
 - Blockchain forensics using certified vendors (e.g., Chainalysis, Elliptic)
 - Prohibition on privacy coins or anonymous wallet addresses
 - EDD for any crypto transaction $\geq$ USD 2,000
-

9. THIRD-PARTY DUE DILIGENCE & CORRESPONDENT RISK

Vegas Games Inc. screens all vendors, payment processors, affiliates, and third-party agents for:

- Sanctions compliance
- UBO identification and EDD
- Past regulatory infractions
- Jurisdictional risk exposure

No business is conducted with counterparties in sanctioned jurisdictions or with insufficient AML frameworks.

10. INTERNAL CONTROLS & AUDIT

Vegas Games Inc. conducts:

- Annual independent AML audits
- Quarterly internal control assessments
- Continuous improvement reviews of the AML Program



All deficiencies are documented, addressed, and reported to senior management.

11. DISCIPLINARY ACTIONS & ENFORCEMENT

Failure to comply with this policy may result in:

- Employee disciplinary measures, including termination
 - Termination of client or partner relationships
 - Voluntary or mandatory reporting to the NGCB, FinCEN, or law enforcement
-

12. Risk Matrix

Spade and Scepter N.V. – AML Risk Matrix (2025)

This Risk Matrix forms part of the Business Risk Assessment (BRA) as outlined in the Spade and Scepter N.V. Anti-Money Laundering Compliance Program (2025). It is aligned with the requirements under the National Ordinance on Games of Chance (LOK), NOIS, NORUT, and the Curaçao Gaming Authority (CGA) AML/CFT Policy (2025).

Company Risk Matrix (BRA Summary)

Risk Category	Sub-Categories	Inherent Risk Level	Mitigating Controls	Residual Risk
Customer Risk	Natural Persons Legal Entities PEPs High-risk jurisdictions	High	KYC/CDD/EDD procedures PEP screening Jurisdictional exclusion Automated identity verification	Medium
Product/Service Risk	Casino Games Sportsbook Bonuses/Promotions Crypto acceptance	Medium	Transaction limits Bonus abuse monitoring Crypto wallet ownership verification	Low
Geographic Risk	Accepted countries Excluded countries (e.g. US, Iran, North Korea) FATF grey/black lists	High	Country risk scoring IP and payment geolocation checks Real-time access blocking	Medium
Delivery Channel Risk	Online (web/mobile) Affiliates 3rd-party payment processors	High	Risk scoring per channel Affiliate due diligence PSP risk controls	Medium

Scoring Definitions

Risk Level	Description
Low	Minimal exposure, well-controlled, minimal regulatory attention
Medium	Moderate exposure, mitigated by controls, requires monitoring
High	Significant exposure, requires enhanced controls, continuous review

Methodology Notes

- Inherent Risk: Identified without considering mitigation.
- Residual Risk: Risk remaining after applying controls.
- Risk matrix is reviewed annually as part of the SIRA/SARA process.
- Aligned with FATF recommendations, CGA AML/CFT Policy (2025), and FIU typologies.

Alignment with EU AML Directives

The following elements of the Spade and Scepter N.V. Risk Matrix and broader AML Compliance Program reflect compliance with the core provisions of the European Union's AML regulatory framework, including the 4th, 5th, and 6th AML Directives (EU) 2015/849, (EU) 2018/843, and (EU) 2018/1673 respectively:

- Risk-Based Approach (Article 8 of EU Directive 2015/849): Spade and Scepter N.V. applies a documented and ongoing risk-based methodology across customers, products, jurisdictions, and delivery channels.
- Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) (Articles 13–15): The policy enforces tiered identity verification, UBO verification, PEP screening, and high-risk jurisdiction exclusions.
- Record Retention (Article 40): All CDD and transactional data is retained for a minimum of 5 years, in accordance with Curaçao laws and EU AML standards.
- Suspicious Activity Reporting (Articles 33–34): Unusual and suspicious transaction reporting procedures are aligned with NORUT and are functionally equivalent to STR obligations under the EU framework.
- Beneficial Ownership Transparency (Articles 30–31): KYB and corporate client checks include verification of beneficial ownership and risk assessment of legal structures.
- Cooperation with FIU and Supervisory Authorities (Articles 32–35): The company's compliance team cooperates with the Curaçao FIU and CGA, fulfilling equivalent obligations to FIU cooperation under EU directives.
- Criminalisation of Money Laundering and Liability (EU Directive 2018/1673): Internal policies reflect zero tolerance for facilitation of predicate offences and establish internal reporting duties and staff accountability.

For internal reporting or external inquiries:



AML Compliance Officer

Derek Hendriks

**approved by Director Ecorpp
Management N.V.
Boy Hendriks**