

ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING POLICY

R Bostock Enterprises B.V.

Curacao Gaming Authority License Number OGL/2024/1067/0640

Approving Official(s):	Pulkit Totla
Responsible Office:	Compliance Department
Effective Date:	February 3, 2026
Next Review Date:	February 3, 2027

TABLE OF CONTENTS

1. 1. Policy Statement
2. 2. Purpose
3. 3. Audience
4. 4. Definitions
5. 5. Policy Implementation
6. 5.1 Business Risk Assessment
7. 5.2 Customer Risk Assessment
8. 5.3 Customer Acceptance Policy
9. 5.4 Customer Due Diligence
10. 5.5 Ongoing Monitoring
11. 5.6 Reliance on Third Parties
12. 5.7 Reporting of Unusual Transactions
13. 5.8 AML Compliance Program
14. 6. Compliance and Consequences of Non-Compliance
15. 7. Related Information
16. 8. Contact Information
17. 9. Policy History

1. POLICY STATEMENT

R Bostock Enterprises B.V. ('the Company') is firmly committed to preventing and combating money laundering (ML), terrorist financing (TF), and proliferation financing (PF) in all its operations. Operating as a licensed gaming operator under the Curacao Gaming Authority (CGA), the Company recognizes the critical importance of maintaining the highest standards of Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) controls and compliance.

The Company's commitment to AML/CTF compliance extends across all business lines, including casino gaming, sports betting, virtual gaming, and related financial services. This Policy establishes a comprehensive framework designed to prevent our products, services, and platform from being exploited for money laundering, terrorist financing, or proliferation financing activities.

The Company operates in strict compliance with the following legal and regulatory frameworks:

- Curacao National Ordinance for Games of Chance (LOK)
- National Ordinance on the Reporting of Unusual Transactions (NORUT)
- Curacao Gaming Authority (CGA) Regulations and Guidelines
- Financial Action Task Force (FATF) Forty Recommendations and FATF Guidance on Virtual Assets
- European Union AML Directives (as reference standards for international best practices)
- United Nations Sanctions Regimes and Terrorism Financing Conventions

Non-compliance with this Policy may result in serious consequences, including disciplinary action against employees, significant regulatory penalties, criminal liability, and potential license revocation. All employees, contractors, agents, and service providers are required to adhere strictly to the provisions of this Policy.

2. PURPOSE

The primary purpose of this Policy is to establish a robust and comprehensive framework that enables R Bostock Enterprises B.V. to effectively identify, manage, and mitigate the risks of money laundering, terrorist financing, and proliferation financing. This Policy aims to:

- Establish clear procedures and controls to prevent the Company's services from being used for ML/TF/PF activities
- Ensure compliance with all applicable Curacao laws, regulations, and CGA requirements
- Implement effective customer due diligence and ongoing transaction monitoring mechanisms
- Detect and report suspicious or unusual transactions to competent authorities in a timely manner
- Maintain accurate records of all customer information and transactions for regulatory inspection and audit purposes
- Promote a culture of compliance throughout the organization
- Provide clear guidance to all personnel regarding their AML/CTF obligations and responsibilities

- Protect the Company's reputation and operational integrity in the gaming and financial services industry

3. AUDIENCE

This Policy applies to all individuals and entities involved in the operation of R Bostock Enterprises B.V., including but not limited to:

- All employees, whether full-time, part-time, or temporary, across all departments
- Contractors and consultants engaged by the Company
- Board members and senior management
- Third-party service providers and suppliers (including payment processors, identity verification vendors, and screening providers)
- Affiliated entities and subsidiaries operating under the Company's brand
- Any person involved in the provision or administration of the Company's gaming services

Additionally, this Policy communicates expectations to our customers regarding the information they must provide and the conditions under which we can maintain their accounts. Customers are notified of key elements of this Policy through our Terms of Service, responsible gaming materials, and account registration processes.

4. DEFINITIONS

The following terms and definitions are essential to understanding this Policy:

Money Laundering (ML): The process of converting illegally obtained proceeds into seemingly legitimate assets or funds to disguise their criminal origin, typically involving placement, layering, and integration stages.

Terrorist Financing (TF): The provision or collection of funds or financial assets with the intention that they will be used, or in the knowledge that they are to be used, to carry out terrorist acts or to support terrorist organizations.

Proliferation Financing (PF): The provision, collection, or provision of funds or services with the intention or knowledge that such funds or services will be used for the development, production, acquisition, stockpiling, retention, transfer, or use of weapons of mass destruction.

Know Your Customer (KYC): The process of verifying and confirming the identity of a customer, understanding the nature of their business activities, and assessing the risks associated with doing business with them.

Customer Due Diligence (CDD): The comprehensive process of verifying customer identity, understanding the source of their funds, and assessing customer risk, with the depth adjusted based on risk profile.

Enhanced Due Diligence (EDD): Heightened customer verification and ongoing monitoring procedures applied to customers presenting elevated ML/TF/PF risks, including high-net-worth individuals, politically exposed persons, and customers in high-risk jurisdictions.

Politically Exposed Person (PEP): An individual who holds or has held prominent public positions (such as heads of state, senior government officials, judicial or military officers, and senior executives of state-owned enterprises) or their immediate family members or close associates.

Suspicious Activity Report (SAR) / Unusual Transaction Report (UTR): A formal report filed with the Financial Intelligence Unit (FIU) when a transaction or pattern of activity is suspected to involve or facilitate money laundering, terrorist financing, or other illegal activity.

Financial Intelligence Unit (FIU): In Curacao's context, the centralized unit responsible for receiving, analyzing, and disseminating information regarding suspected money laundering and terrorist financing; reports are submitted to Curacao FIU.

Money Laundering Reporting Officer (MLRO): The senior management official responsible for overseeing AML/CTF compliance, receiving internal reports of suspicious activity, and ensuring timely and accurate reporting to authorities.

Business Risk Assessment (BRA): A comprehensive evaluation of the ML/TF/PF risks inherent to the Company's business model, products, delivery channels, customer base, and geographic footprint.

Customer Risk Assessment (CRA): An ongoing evaluation of individual customers based on factors such as jurisdiction, transaction patterns, PEP status, source of funds, and risk profile classification.

Beneficial Owner: The natural person or persons who ultimately owns or controls a legal entity or arrangement, or on whose behalf a transaction is being conducted.

Shell Bank: A bank with no physical presence in the country where it is licensed and no significant presence in any country, with no meaningful management and staff.

Correspondent Banking: Relationships established between financial institutions to provide services across borders, requiring appropriate due diligence and controls.

Virtual Assets: Cryptographic assets and digital representations of value that can be digitally transferred, stored, or traded, including cryptocurrencies and digital tokens.

Sanctions List: Official lists of individuals and entities subject to financial sanctions or restrictions, including UN, EU, OFAC, and local Curacao government lists.

Adverse Media: Public information suggesting that a customer or beneficial owner is involved in criminal activity, financial crime, or other illegal conduct.

5. POLICY IMPLEMENTATION

5.1 Business Risk Assessment

R Bostock Enterprises B.V. maintains a comprehensive Business Risk Assessment (BRA) that identifies and evaluates the money laundering, terrorist financing, and proliferation financing risks inherent to our operations. This assessment forms the foundation for our risk-based approach to AML/CTF compliance.

5.1.1 Risk Assessment Scope

The Business Risk Assessment covers the following dimensions:

Product Risk: Casino gaming, sports betting, virtual/live gaming, in-play betting, esports wagering, and payment processing services

Delivery Channel Risk: Web-based platform, mobile applications, desktop clients, application programming interfaces (APIs) for third-party operators

Customer Type Risk: Retail players, high-value players (VIPs), corporate customers, affiliate partners, payment processors

Geographic Risk: Jurisdictions of customer residence, incorporation of business entities, server locations, payment routing jurisdictions

Payment Method Risk: Credit/debit cards, e-wallets (Skrill, Neteller, ecoPayz), bank transfers, cryptocurrency payments, prepaid cards

5.1.2 Risk Matrix Approach

The Company employs a risk matrix methodology that evaluates each risk factor on two dimensions:

Likelihood (Probability): Assessed on a scale of Very Low, Low, Medium, High, and Very High

Impact: Assessed on a scale of Minimal, Low, Medium, High, and Critical

Risk scores are calculated by multiplying likelihood and impact ratings, resulting in an overall risk classification (Very Low, Low, Medium, High, Very High) for each product, channel, customer type, and geographic combination. Higher-risk combinations trigger enhanced monitoring and stronger controls.

5.1.3 High-Risk Scenarios Identified

- New customers from high-risk jurisdictions (FATF Grey List, FATF Black List, or jurisdictions with weak AML/CTF frameworks)
- High-value transactions exceeding monitoring thresholds with unclear economic justification
- Rapid succession of deposits followed by immediate large withdrawals
- Customers claiming to be politically exposed persons or family members of PEPs

- Transactions involving virtual assets or cryptocurrency, particularly unregulated or privacy-coin transactions
- Customers unable or unwilling to provide satisfactory source of funds documentation for deposits
- Structuring or 'smurfing' patterns, where multiple transactions just below reporting thresholds are detected
- Customers with adverse media or negative news reports linked to financial crime, sanctions violations, or terrorism

5.1.4 Annual Review and Update

The Business Risk Assessment is reviewed and updated on an annual basis, or more frequently if significant changes occur in the business, regulatory environment, or threat landscape. Updates are documented and approved by the Money Laundering Reporting Officer and senior management. Material changes to the BRA trigger communication to relevant staff and potential adjustments to customer monitoring procedures.

5.2 Customer Risk Assessment

R Bostock Enterprises B.V. implements a comprehensive Customer Risk Assessment (CRA) system that evaluates each customer's individual risk profile and applies appropriate controls and monitoring levels. This system uses a color-coded classification framework to facilitate communication and decision-making.

5.2.1 Risk Classification System

BLACK (Unverified/Refused): Customers who cannot be verified through satisfactory CDD procedures, or customers for whom adequate information cannot be obtained. BLACK-classified accounts have a maximum deposit limit of EUR 200 and are subject to immediate closure if the customer fails to complete enhanced verification within 30 days of account opening.

GREEN (Low Risk - Verified): Customers successfully verified through standard CDD procedures with clear source of funds documentation, from jurisdictions with robust AML/CTF frameworks, with no PEP status, adverse media, or red flags. GREEN-classified customers are eligible for standard monitoring levels.

BLUE (Low Risk - High Confidence): Customers verified through enhanced procedures with additional documentation, from low-risk jurisdictions, with full economic profile clarity, no adverse media, and long tenure with the Company without incidents. BLUE-classified customers represent the lowest monitoring burden.

ORANGE (Medium Risk - Enhanced Monitoring): Customers from medium-risk jurisdictions, with moderate transaction volumes, or presenting minor inconsistencies in provided documentation. ORANGE-classified customers trigger automated transaction monitoring with alerts for significant deposits, withdrawal pattern changes, or source of funds queries.

RED (High Risk - Heightened Scrutiny): Customers from high-risk jurisdictions, claiming PEP status, with adverse media, large transaction volumes, or presenting multiple red flags. RED-classified accounts trigger enhanced due diligence, intensive transaction monitoring, and potential mandatory account closure if risks cannot be adequately mitigated.

5.2.2 Risk Assessment Factors

Customer risk classification is determined through evaluation of the following factors:

- **Jurisdiction of Residence/Incorporation:** Customers from jurisdictions identified on FATF grey/black lists, with weak AML/CTF frameworks, or subject to international sanctions are classified as higher risk.
- **Transaction Patterns:** Rapid accumulation of deposits, frequent large transactions, unusual timing patterns, or transactions inconsistent with stated business activities increase risk classification.
- **PEP Status:** Customers identified as politically exposed persons or close associates/family members of PEPs trigger automatic ORANGE or RED classification and enhanced due diligence.
- **Source of Funds:** Clear documentation of legitimate source of funds reduces risk classification. Inability to explain source of funds or evidence of potentially illicit origins increases risk.
- **Adverse Media:** Online searches, news monitoring, and adverse media screening results showing links to criminal activity, sanctions violations, or financial crime trigger RED classification.
- **Payment Methods:** Virtual assets and cryptocurrency payments trigger elevated risk classifications. Multiple payment method changes or routing through high-risk jurisdictions increase risk.
- **Account Activity Duration:** Established customers with lengthy activity histories and consistent patterns are lower risk than new customers.
- **Communication Consistency:** Customers providing inconsistent information or unable to explain their activities are classified as higher risk.
- **Previous Compliance Issues:** Customers previously flagged for suspicious activity or who have violated account terms are automatically elevated to ORANGE or RED classification.

5.2.3 Risk Reclassification

Customer risk classifications are reviewed and updated when:

- Significant transactions or deposits are detected
- Adverse media or sanctions matching occurs
- Customers change account information or activity patterns
- Changes occur in the regulatory or geopolitical environment affecting customer jurisdiction
- Periodic reviews are conducted (minimum semi-annually)

Reclassifications are documented in the customer's AML file, with justification for the change recorded.

5.3 Customer Acceptance Policy

R Bostock Enterprises B.V. implements a risk-based customer acceptance policy aligned with our overall Customer Risk Assessment framework. The Company reserves the right to accept or refuse business relationships based on our ability to conduct adequate due diligence and manage inherent risks.

5.3.1 General Acceptance Requirements

- Customer must be at least 21 years of age (verified through documentary evidence)
- Customer must not be identified on any applicable sanctions list (UN, EU, OFAC, Curacao government lists)
- Customer must not be from jurisdictions subject to comprehensive international sanctions (as determined by the Company)
- Customer must not be identified as a shell company or established for the purpose of money laundering or tax evasion
- Customer must not refuse to complete required customer due diligence procedures
- Customer must not provide false or misleading information during registration or due diligence
- Customer must consent to ongoing monitoring of account activities and transactions

5.3.2 Restricted Jurisdictions

R Bostock Enterprises B.V. maintains a Restricted Jurisdictions List, updated regularly, which identifies countries and territories from which we do not accept customers or with which we severely limit business relationships due to sanctions, weak AML/CTF frameworks, or high ML/TF risk. Customers cannot create accounts or access our services from these restricted jurisdictions.

The Restricted Jurisdictions List is reviewed quarterly and updated based on changes to international sanctions regimes, FATF guidance, and regulatory requirements. The list is maintained by the Compliance Department and communicated to all relevant staff.

5.3.3 PEP Screening and Enhanced Acceptance Procedures

All customers are screened against PEP databases during account registration and on an ongoing basis. Customers identified as politically exposed persons or immediate family members/close associates of PEPs cannot be accepted without explicit approval from the Money Laundering Reporting Officer and the completion of enhanced due diligence procedures.

For PEP customers, the following additional procedures apply:

- Documented investigation of source of wealth and source of funds
- Senior management approval of business relationship establishment
- Enhanced transaction monitoring with lower thresholds for suspicious activity
- Quarterly risk reassessment
- Enhanced record keeping of all supporting documentation

5.3.4 Sanctions Screening

All customers are screened against comprehensive sanctions lists during account opening and on an ongoing basis:

United Nations Consolidated List - Individuals and entities designated by the UN Security Council

European Union Consolidated List - EU designated individuals and entities

OFAC Specially Designated Nationals List - US designated individuals and entities

Curacao Government Lists - Local government designations (where applicable)

If a customer matches or potentially matches a sanctions list entry (even partially), the account is immediately suspended and escalated to the Money Laundering Reporting Officer for investigation. The Company will not process any transactions for sanctioned individuals or entities, and funds may be frozen pending legal review and regulatory notification.

5.3.5 Refusal of Service

The Company reserves the right to refuse service to any customer if:

- Adequate customer due diligence cannot be completed
- Customer fails to provide required identification or documentation
- Customer provides false or misleading information
- Customer is identified on a sanctions list or as a politically exposed person without satisfactory justification
- Customer is from a restricted jurisdiction
- Customer engages in activities suspected to involve money laundering or terrorist financing
- The Company's risk assessment procedures suggest unacceptable risks

When service is refused, customers are notified in writing, if possible. The Company retains documentation of refusals for regulatory inspection.

5.4 Customer Due Diligence

Customer Due Diligence (CDD) is the cornerstone of R Bostock Enterprises B.V.'s AML/CTF program. CDD involves verifying customer identity, understanding the nature and purpose of customer relationships, and assessing ML/TF risk. The Company applies a risk-based approach to CDD, with the depth and intensity of CDD procedures adjusted based on individual customer risk profiles.

5.4.1 Three-Tier CDD Framework

Simplified CDD: Applied to low-risk customers and relationships where the ML/TF risk is demonstrably minimal. Simplified CDD includes basic identity verification and confirmation that the customer is not on sanctions lists. Simplified CDD is not applied to customers from high-risk jurisdictions or claiming PEP status.

Standard CDD: The baseline due diligence applied to all customers before allowing transactions to exceed EUR 2,150 in rolling 30-day deposits. Standard CDD includes: (1) Collection of full name,

date of birth, nationality, and residential address; (2) Identity verification through government-issued ID (passport, national ID card, or driver's license); (3) Proof of address (utility bill, bank statement, government correspondence); (4) Sanctions and PEP screening; (5) Basic source of funds inquiry for deposits exceeding ANG 4,000.

Enhanced CDD: Applied to customers classified as high risk, claiming PEP status, conducting high-value transactions, or from jurisdictions with weak AML/CTF frameworks. Enhanced CDD includes: (1) All Standard CDD requirements plus; (2) Detailed source of funds/wealth documentation; (3) Investigation of beneficial owners for business customers; (4) Senior management approval; (5) More intensive transaction monitoring with lower alert thresholds; (6) Quarterly risk reassessment.

5.4.2 KYC Process and Third-Party Verification

R Bostock Enterprises B.V. utilizes third-party identity verification and screening providers to support our KYC and CDD procedures:

Primary Provider - Sumsub: Provides automated and manual identity verification services, including document scanning, liveness checks, and comprehensive identity verification. Sumsub is integrated with our customer registration platform to provide real-time verification results.

Screening Provider - ComplyAdvantage: Provides continuous sanctions screening, PEP screening, and adverse media monitoring. ComplyAdvantage database is queried at customer registration and on ongoing periodic basis (minimum monthly screening for all active accounts).

Integration Process:

1. During account registration, customers upload identification documents through Sumsub interface
2. Sumsub performs real-time verification against government databases and performs liveness checks
3. Customer data is simultaneously submitted to ComplyAdvantage for sanctions and PEP screening
4. Results are automatically returned within minutes
5. If verification is successful and no sanctions matches are found, account is provisionally activated pending address verification
6. Customer submits proof of address documentation within 30 days
7. Once address verification is completed, account is fully activated and unrestricted

5.4.3 Required Documentation

Standard CDD Documentation Required:

Government-Issued Identification:

- Passport, national identity card, or driver's license
- Must be valid or expired no more than 5 years
- Must clearly display customer name, date of birth, photograph, and signature
- Both sides of document must be provided (if two-sided)

Proof of Address:

- Utility bill (electricity, water, gas, internet) dated within 90 days
- Bank statement or credit card statement dated within 90 days
- Government correspondence (tax notice, official letter)
- Lease agreement or property deed
- Must clearly display customer name and current address

Enhanced CDD Documentation (if applicable):

Source of Funds Documentation:

- Employment verification letter or recent payslips
- Business ownership documentation and financial statements
- Investment account statements showing source of trading profits
- Inheritance documentation or gift letters
- Pension statements or retirement account documentation

Beneficial Owner Documentation (for business customers):

- Corporate registry extracts and articles of incorporation
- List of shareholders holding >25% ownership with supporting identification
- Identification documents for beneficial owners
- Proof of beneficial owner address

PEP Documentation (if applicable):

- Documented explanation of PEP status
- Source of wealth investigation documentation
- Family relationship documentation if claiming as family member
- Assets and liabilities declaration

5.4.4 PEP and Sanctions Screening Procedures

Politically Exposed Person Screening:

All customers are screened against PEP databases during account registration and quarterly thereafter.

Customers identified as:

- Heads of state or government
- Senior government officials
- Senior judicial or military officers
- Senior executives of state-owned enterprises
- International organization officials
- Family members of any of the above
- Close associates of any of the above

...are flagged for enhanced due diligence and require Money Laundering Reporting Officer approval before account activation.

Sanctions List Screening:

All customers are screened against UN, EU, OFAC, and Curacao government sanctions lists. Matching is performed using:

- Exact name matching
- Fuzzy matching to account for spelling variations and aliases
- Date of birth matching (when available)
- Nationality matching

If a match is found or a potential match identified, the account is immediately suspended and escalated to Money Laundering Reporting Officer. False positives are documented, and customers are contacted to provide additional information to clear the match.

5.4.5 Customer Due Diligence File

All customer due diligence documentation is maintained in a Customer AML File, which includes:

- Copy of government-issued identification
- Proof of address documentation
- Customer Risk Assessment documentation and risk classification rationale
- Source of funds documentation (where applicable)
- Beneficial owner identification (for business customers)
- Sanctions and PEP screening results
- Adverse media screening results
- Notes on CDD procedures completed and dates
- Approvals (including enhanced due diligence approvals)
- Any exceptions or deviations from standard procedures
- Ongoing monitoring notes and any suspicious activity investigations

Customer AML files are maintained for a minimum of 5 years after account closure and are made available for regulatory inspection.

5.5 Ongoing Monitoring

R Bostock Enterprises B.V. maintains comprehensive ongoing monitoring of all customer accounts and transactions. Ongoing monitoring is essential to detect unusual or suspicious activities that may indicate money laundering, terrorist financing, or other illegal purposes. The Company employs both automated systems and manual review procedures to identify suspicious patterns.

5.5.1 Automated Transaction Monitoring System

All transactions are processed through an automated transaction monitoring system that evaluates each transaction against predefined risk rules and alerts. The monitoring system continuously evaluates transaction data and customer activity patterns, generating alerts when rules are triggered. Alerts are

reviewed by the Player Risk Team and escalated to the Money Laundering Reporting Officer when suspicious activity is identified.

5.5.2 AML Monitoring Triggers and Rules

The automated monitoring system triggers alerts based on the following activity patterns and thresholds:

- Single Deposit Threshold Exceeded: Deposits exceeding EUR 5,000 (or local currency equivalent) trigger standard review. Deposits exceeding EUR 20,000 trigger intensive review.
- Rolling Deposit Threshold: Total deposits exceeding EUR 8,000 in a rolling 30-day period trigger review for accounts classified as GREEN or BLUE.
- Deposit Method Change: Customers changing payment method from their initially verified method without explanation trigger review.
- Cross-Method Withdrawal: Customers withdrawing via different payment method than used for deposits trigger review (potential financial structuring).
- Cashier as Currency Exchange: Attempts to use the gaming platform as a currency exchange service (e.g., depositing via one payment method, withdrawing via another with minimal/no wagering) trigger alerts.
- Withdrawal Without Wagering: Withdrawal requests within 24 hours of deposit without meaningful wagering activity trigger review.
- Source of Funds Unexplained: Customers unable to provide satisfactory explanation for source of deposits trigger escalation.
- Deposit Velocity Increase: Increase in deposit frequency or amounts exceeding 10% above customer's 4-week rolling average triggers review.
- Adverse Media Match: Customers matching adverse media screening results trigger immediate escalation.
- High/Medium Risk Verification Returns: Verification service returning high-risk or medium-risk designations trigger enhanced monitoring.
- Inconsistent Communications: Customers providing inconsistent information or unable to explain stated activities trigger review.
- Bank/E-Wallet Transaction Constants: Constant monitoring of customer's bank and e-wallet transaction velocity; rapid in/out movements trigger review.
- High-Value Withdrawals: Withdrawal requests exceeding EUR 300 trigger standard review; requests exceeding EUR 2,000 trigger intensive review.
- Transaction Velocity: More than 50 transactions (deposits + withdrawals) in a single calendar day triggers review.
- Structuring Pattern: Multiple transactions just below monitoring thresholds within short time period trigger review.
- Geographic Inconsistency: Transactions inconsistent with customer's stated residence or business location trigger review.
- Time-Zone Anomaly: Account activity at unusual hours for customer's stated time zone trigger review (potential account compromise).

- **Rapid Account Creation and High Activity:** New accounts immediately engaging in high-value transactions trigger review.

5.5.3 Player Risk Team Review Process

All alerts generated by the automated monitoring system are reviewed by the Player Risk Team, comprising:

- Head of Compliance
- AML Compliance Analyst (dedicated resources)
- Payments Manager

The Player Risk Team reviews each alert within 24 hours of generation. Review procedures include:

1. Assessment of alert context and transaction details
2. Review of customer's complete transaction history
3. Analysis of customer's stated business activities versus actual activities
4. Source of funds verification
5. Determination of whether activity is suspicious or can be adequately explained

Weekly Summary Reports: The Player Risk Team prepares a comprehensive weekly report summarizing all alerts generated, reviewed, and investigated. The report is submitted to the Money Laundering Reporting Officer and includes:

- Total alerts generated
- Alerts by category/trigger type
- Alerts requiring escalation to suspicious activity investigation
- Customer risk classification changes
- Accounts flagged for closure due to AML concerns
- Any potential unusual transactions requiring reporting to authorities

5.5.4 Suspicious Activity Investigation and Escalation

When Player Risk Team review determines that activity may involve money laundering, terrorist financing, or other illegal purposes, the matter is escalated to the Money Laundering Reporting Officer for formal investigation.

Suspicious Activity Investigation Procedure:

1. MLRO receives escalation and initiates formal investigation
2. AML investigation file is created documenting the investigation timeline and findings
3. Detailed analysis is conducted of:
 - Customer background and stated business activities
 - Complete transaction history
 - Source of funds documentation and verification
 - Communications with customer (if any)
 - Customer risk profile and classification rationale
 - Comparison to known ML/TF typologies

4. Additional information is requested from customer if needed
5. Account activity monitoring is intensified pending investigation completion
6. Account may be frozen if imminent risk of funds being used for illegal purposes is identified
7. Investigation is documented with findings and conclusion
8. If suspicious activity is confirmed, Unusual Transaction Report is prepared for filing with Curacao FIU
9. Customer account may be closed if risks cannot be adequately mitigated

5.5.5 Color-Coded Risk Escalation System

The Company employs a color-coded escalation system to facilitate rapid communication regarding customer risk levels:

GREEN - Low Risk: Standard monitoring applies. Weekly reporting to MLRO in summary format.

ORANGE - Medium Risk: Enhanced monitoring applied. Daily review by Player Risk Team. Alert thresholds are more sensitive (lower deposit/withdrawal amounts trigger review). Daily reporting to MLRO.

RED - High Risk: Intensive monitoring applied. Real-time review of transactions. Multiple alert thresholds are more sensitive. Escalation to MLRO within 2 hours of alert generation. Consideration of account closure within 30 days if risks cannot be mitigated.

BLACK - Unverified/Refused: Restricted account status. Maximum EUR 200 deposit limit. 30-day deadline for CDD completion or account closure. Daily monitoring for compliance deadline.

5.6 Reliance on Third Parties

R Bostock Enterprises B.V. utilizes third-party service providers for critical AML/CTF functions, including identity verification, sanctions screening, and adverse media monitoring. While the Company may rely on third parties for certain operational functions, R Bostock Enterprises B.V. retains ultimate responsibility for AML/CTF compliance and cannot delegate its obligations to third parties.

5.6.1 Third-Party Service Providers

Sumsub (Identity Verification Provider): Provides automated identity verification services including document scanning, data extraction, liveness verification, and government database matching. Sumsub is integrated into our customer registration platform.

ComplyAdvantage (Screening Provider): Provides sanctions list screening, PEP database screening, and adverse media monitoring. ComplyAdvantage is integrated for both real-time account registration screening and ongoing periodic screening.

5.6.2 Due Diligence on Third-Party Providers

R Bostock Enterprises B.V. conducts comprehensive due diligence on all third-party AML/CTF service providers prior to engagement:

Regulatory Authorization: Verification that providers are appropriately licensed and regulated for the services they provide.

Compliance Framework: Review of provider's AML/CTF policies, procedures, and compliance program.

Data Security: Assessment of provider's information security practices, including encryption, access controls, and data protection compliance.

Financial Stability: Assessment of provider's financial position to ensure continuity of service.

Reference Checks: Contact with other clients using the provider's services.

Service Level Agreements: Negotiation of service agreements defining accuracy, response times, uptime, and liability.

5.6.3 Contractual Requirements

All contracts with third-party AML/CTF service providers include the following requirements:

- Obligation to maintain confidentiality and protect customer data
- Data protection compliance with applicable regulations
- Right to audit third party's controls and compliance procedures
- Notification requirements for security breaches or service failures
- Minimum availability/uptime requirements
- Data retention and deletion procedures upon contract termination
- Compliance with Curacao law and CGA requirements
- Prohibition on sub-contracting without R Bostock's written approval
- Liability limitations and insurance requirements

5.6.4 Ongoing Third-Party Monitoring

R Bostock Enterprises B.V. monitors third-party service providers on an ongoing basis:

- Quarterly review of service level agreement compliance and uptime metrics
- Annual compliance questionnaires requesting updates on provider's AML/CTF program
- Semi-annual review of provider's regulatory status and any enforcement actions
- Immediate notification requirement if provider experiences security breaches, regulatory sanctions, or material service failures
- Right to conduct on-site audits of provider's operations and controls

If a third-party provider fails to meet contractual obligations or compliance requirements, R Bostock Enterprises B.V. has the right to terminate the relationship and transition to an alternative provider.

5.6.5 Retention of Ultimate Responsibility

While R Bostock Enterprises B.V. relies on third parties for operational support, the Company retains ultimate responsibility for:

- All customer due diligence decisions
- Customer risk assessments and classifications
- Decisions to accept or refuse customers
- Suspicious activity investigation and reporting
- Compliance with all applicable laws and regulations
- Regulatory reporting and audit compliance
- Employee training on AML/CTF obligations

The Company cannot use reliance on third parties as a defense for AML/CTF compliance failures or regulatory violations.

5.7 Reporting of Unusual Transactions

R Bostock Enterprises B.V. is obligated under Curacao's National Ordinance on the Reporting of Unusual Transactions (NORUT) to identify and report transactions suspected to involve or facilitate money laundering, terrorist financing, proliferation financing, or other illegal activities. The Company maintains comprehensive procedures for recognizing, investigating, and reporting unusual transactions.

5.7.1 Definition of Unusual Transaction

An unusual transaction (also referred to as a Suspicious Activity Report or SAR) is any transaction or pattern of transactions that:

- Appears to involve funds derived from criminal activity
- Is structured to evade reporting requirements
- Is inconsistent with the customer's known business or stated activities
- Involves large sums with no apparent economic purpose
- Involves attempts to obscure the origin, source, or destination of funds
- Involves transactions with high-risk jurisdictions or sanctioned entities
- Involves politically exposed persons or terrorist-related entities
- Shows patterns consistent with known money laundering or terrorist financing typologies
- Involves virtual assets or cryptocurrency with unclear purpose
- Raises other reasonable suspicion of illegal activity

5.7.2 Internal Reporting Chain

Unusual transaction reports are processed through the following internal chain:

STEP 1 - Initial Detection

Staff members, Payment Team, Player Risk Team, or automated systems detect a transaction or pattern

potentially involving suspicious activity.

STEP 2 - Internal Reporting

The detecting party documents the suspicious transaction with details and reports to the Player Risk Team or directly to the Money Laundering Reporting Officer.

STEP 3 - Preliminary Investigation

Player Risk Team conducts preliminary review of the transaction:

- Review of customer's complete transaction history
- Assessment of transaction against known typologies
- Verification of customer information and source of funds
- Determination of whether investigation should be escalated

STEP 4 - Escalation to MLRO

If preliminary investigation confirms reasonable suspicion of unusual transaction, matter is escalated to Money Laundering Reporting Officer with detailed findings.

STEP 5 - Formal Investigation

MLRO conducts formal investigation of potentially unusual transaction, documenting:

- Investigation timeline and procedures performed
- Relevant transaction and customer data
- Supporting documentation and analysis
- Conclusion regarding whether reasonable suspicion of illegal activity exists

STEP 6 - Reporting Decision

MLRO determines whether filing Unusual Transaction Report (UTR) with Curacao FIU is required. If reasonable suspicion of illegal activity exists, UTR is prepared and filed.

STEP 7 - Filing with FIU

Unusual Transaction Report is filed with Curacao Financial Intelligence Unit (FIU) in accordance with NORUT requirements.

5.7.3 Unusual Transaction Report (UTR) Contents

Unusual Transaction Reports filed with Curacao FIU include the following information:

- Customer identification and account information
- Date(s) of transaction(s) being reported
- Transaction amounts, currency, and details
- Payment methods involved
- Source and destination of funds
- Reason for suspicion of unusual nature
- Relevant customer risk factors
- Summary of investigation findings

- Date of report submission
- Reporting officer identification

UTRs are prepared with professional completeness and accuracy, as they form the basis for law enforcement and intelligence investigation.

5.7.4 Reporting Timelines

Unusual transactions are reported to Curacao FIU in accordance with NORUT requirements:

- Suspicious transactions should be reported as soon as practicable, but no later than 10 business days from when reasonable suspicion is identified
- Imminent threats to public safety or national security may require expedited reporting
- Ongoing investigations may result in supplementary reports if additional information becomes available

If an unusual transaction involves imminent risk of funds being used for terrorist financing or terrorism, the Company may freeze customer funds and notify Curacao FIU on an emergency basis within 24 hours.

5.7.5 Record Keeping

R Bostock Enterprises B.V. maintains comprehensive records of all unusual transaction reports:

- Copy of submitted UTR to FIU
- Investigation file documentation
- Supporting transaction and customer data
- Investigator notes and conclusions
- Date submitted to FIU
- FIU acknowledgment/receipt (if provided)
- Any follow-up communications with FIU

All UTR records are retained for a minimum of 5 years and are made available for regulatory inspection by CGA.

5.7.6 Tipping-Off Prohibition

Staff members must strictly adhere to tipping-off prohibitions:

- Customer must not be informed that an Unusual Transaction Report is being filed or has been filed concerning their account or transactions
- Customer must not be informed that their account is under investigation
- Customer must not be provided information that would indicate we suspect money laundering or terrorist financing

Violation of tipping-off prohibitions is grounds for immediate disciplinary action up to and including termination of employment. The Company will cooperate with law enforcement to prevent obstructing investigations through improper customer notification.

5.8 AML Compliance Program

R Bostock Enterprises B.V. maintains a comprehensive Anti-Money Laundering and Counter-Terrorist Financing Compliance Program designed to ensure effective implementation of all AML/CTF controls and procedures. The program is risk-based and is reviewed and updated regularly to reflect changes in the regulatory environment and the Company's business operations.

5.8.1 Organizational Structure and Responsibilities

The AML/CTF Compliance Program operates within the following organizational structure:

General Manager (GM) Overall responsibility for AML/CTF compliance, including regulatory reporting and regulatory relationship management. The CEO ensures adequate resources and senior management commitment to AML/CTF program.

Money Laundering Reporting Officer (MLRO): Senior manager directly accountable to CEO for AML/CTF compliance program effectiveness. MLRO is responsible for: (1) Policy development and updates, (2) Suspicious activity investigation and reporting, (3) Regulatory correspondence, (4) Staff training and oversight, (5) Independent audit coordination, (6) Escalation of compliance issues.

Head of Compliance: Reports to MLRO and oversees day-to-day compliance operations. Responsibilities include: (1) Customer due diligence oversight, (2) Transaction monitoring program administration, (3) Third-party provider management, (4) Compliance documentation and record-keeping.

Finance Manager: Manages financial transaction processing and payment reconciliation. Coordinates with AML team on large transaction review and unusual transaction investigation.

Player Risk Team: Dedicated team reviewing transaction monitoring alerts and conducting preliminary suspicious activity investigation. Prepares weekly risk reports for MLRO.

Payments Team: Processes customer deposits and withdrawals, applies transaction monitoring rules, and flags transactions meeting alert criteria.

5.8.2 Staff Training and Awareness

R Bostock Enterprises B.V. is committed to ensuring all staff understand their AML/CTF obligations and responsibilities. The Company maintains a comprehensive training program:

Mandatory Initial Training: All employees receive comprehensive AML/CTF training upon hire, covering:

- Overview of money laundering and terrorist financing threats
- Applicable Curacao laws and CGA requirements
- Company's AML/CTF policies and procedures
- Red flags and suspicious activity indicators
- Reporting procedures and obligations
- Disciplinary consequences of non-compliance

- Confidentiality obligations

Annual Refresher Training: All staff complete annual AML/CTF refresher training covering policy updates, regulatory changes, and emerging threats.

Role-Specific Training: Staff involved in compliance-critical functions (payments, customer service, account management) receive additional specialized training covering their specific obligations and responsibilities.

Compliance Induction: New employees in compliance-related roles receive extended training on investigation procedures, reporting requirements, and third-party provider management.

Training Records: The Company maintains records of all training completed by staff, including dates, content covered, and employee acknowledgment. Training records are retained for regulatory inspection.

5.8.3 Record Retention

R Bostock Enterprises B.V. maintains the following records for a minimum of 5 years:

- Customer identification and due diligence documentation
- Customer risk assessment files
- Transaction records (amounts, dates, payment methods, parties involved)
- Correspondence with customers
- Customer account opening and closing documentation
- Suspicious activity investigation files
- Unusual Transaction Reports filed with FIU
- Staff training records
- Compliance committee meeting minutes
- Internal audit reports
- Third-party service provider contracts and audit results

Records are retained for 5 years from the date of the transaction or account closure, whichever is later. Where legal proceedings are pending, records may be retained longer as required by law.

5.8.4 Account Blocking and Fund Freezing

R Bostock Enterprises B.V. has procedures to block customer accounts and freeze funds upon reasonable suspicion of money laundering or terrorist financing:

Account Blocking Procedures:

1. When reasonable suspicion of ML/TF/PF is identified, Money Laundering Reporting Officer may authorize account blocking
2. Account blocking restricts customer's ability to withdraw funds or place new bets
3. Customer is not informed of the reason for account blocking (tipping-off prohibition)

4. Account remains blocked pending investigation completion

Fund Freezing:

If investigation confirms reasonable suspicion that funds are derived from illegal activity or are intended for illegal purposes, funds are frozen and cannot be accessed or transferred by customer. Frozen funds are separately maintained pending law enforcement instructions or account closure.

Regulatory Notification:

If customer funds are frozen due to suspected ML/TF/PF activity, Unusual Transaction Report is filed with Curacao FIU notifying authorities of the frozen funds and basis for freezing.

5.8.5 Independent Audit and Compliance Review

R Bostock Enterprises B.V. undergoes periodic independent audit of its AML/CTF compliance program:

Annual Independent Audit: At minimum annually, an independent external auditor reviews:

- Completeness and effectiveness of AML/CTF policies and procedures
- Compliance with policies by staff
- Adequacy of customer due diligence
- Transaction monitoring system functionality
- Suspicious activity investigation procedures
- Record retention and documentation
- Training program effectiveness

Audit Report: The independent auditor provides a detailed report with findings, recommendations, and compliance assessment to senior management and the MLRO.

Corrective Action: Management develops and implements corrective action plans to address any audit findings, with completion timelines and responsible parties documented.

Regulatory Sharing: The independent audit report is made available to Curacao Gaming Authority upon request as evidence of compliance program effectiveness.

5.8.6 Whistleblowing Procedures

R Bostock Enterprises B.V. maintains confidential whistleblowing procedures enabling staff to report suspected AML/CTF violations, compliance failures, or regulatory violations:

Reporting Channels:

- Direct reporting to Money Laundering Reporting Officer
- Anonymous reporting through dedicated compliance email (compliance@rbostock.ky)
- Reporting to external compliance hotline (if engaged)

Confidentiality: All whistleblower reports are treated confidentially. Reporter identity is protected to the

maximum extent possible.

Non-Retaliation: The Company strictly prohibits retaliation against staff making good-faith compliance or legal violation reports. Retaliation is grounds for disciplinary action.

Investigation: All whistleblower reports are investigated promptly and thoroughly, with findings documented.

Protection: Staff making good-faith reports are provided protection from any adverse employment action based on the report.

6. COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE

Strict adherence to this Policy and applicable AML/CTF laws is mandatory for all employees, contractors, and service providers. Non-compliance can result in severe consequences at both individual and organizational levels.

6.1 Employee Disciplinary Actions

Employees who violate this Policy or applicable AML/CTF laws may face disciplinary actions including:

- Written warning
- Suspension without pay
- Demotion to lower-level positions
- Termination of employment for cause
- Referral to law enforcement for criminal prosecution

The severity of disciplinary action depends on the nature and severity of the violation, including whether it was intentional or negligent, the impact on the Company, and any prior violations by the employee.

7. RELATED INFORMATION

This Policy is complementary to and should be read in conjunction with the following related policies, procedures, and regulatory requirements:

Curacao National Ordinance for Games of Chance (LOK): The primary gaming regulation governing licensed gaming operators in Curacao, establishing licensing requirements, operational standards, and AML/CTF obligations.

National Ordinance on the Reporting of Unusual Transactions (NORUT): Curacao's AML reporting law establishing obligations to identify and report unusual transactions to the Financial Intelligence Unit.

Curacao Gaming Authority (CGA) Regulations and Guidelines: CGA's regulatory guidance for licensed operators, including detailed AML/CTF compliance requirements, customer due diligence standards, and transaction monitoring expectations.

Financial Action Task Force (FATF) Forty Recommendations: International AML/CTF standards developed by FATF and widely adopted by countries worldwide, providing the foundation for Curacao's AML/CTF regulatory framework.

FATF Guidance on Virtual Assets: FATF's specific guidance on applying AML/CTF standards to cryptocurrency and virtual asset transactions, providing best practices for virtual asset monitoring and reporting.

European Union AML Directives: EU's comprehensive AML/CTF regulatory framework (5th AML Directive and subsequent guidance), established as reference standards for international best practices in AML/CTF compliance.

United Nations Sanctions Regimes: UN Security Council designations and sanctions programs related to terrorism and WMD proliferation, which Curacao incorporates into its sanctions screening obligations.

R Bostock Enterprises B.V. Know Your Customer (KYC) Policy: Detailed procedures for customer identification and verification, establishing minimum standards for customer due diligence.

R Bostock Enterprises B.V. Responsible Gaming Policy: Policy establishing player protection measures and responsible gaming controls, which complement AML/CTF controls in identifying problematic account activities.

R Bostock Enterprises B.V. Information Security Policy: Policy establishing information security controls protecting customer data and AML documentation from unauthorized access or disclosure.

8. CONTACT INFORMATION

For questions regarding this Policy or AML/CTF compliance matters, please contact:

Compliance Department:

R Bostock Enterprises B.V.:

Email: support@bet-40.vip, support@elitebet.io, support@rocketbet.com, support@ukingbet.com

Money Laundering Reporting Officer: Marios Loukas Charalampous

9. POLICY HISTORY

Version	Date Effective	Date Approved	Type of Change	Approving Authority
3.0	February 3, 2026	February 3, 2026	Updated Policy	Pulkit Totla

APPROVALS AND SIGNATURE

This Anti-Money Laundering and Counter-Terrorist Financing Policy is hereby approved and authorized by the undersigned:



Pulkit Totla

R Bostock Enterprises B.V.

Date: February 3, 2026