

LUCKYROO N.V.

Risk Policy for Cryptocurrency Usage



Abraham de Veerstraat 1,

Willemstad, Curaçao

Last review: November 2024

Document Owner: Christos Polyviou, Compliance Officer

Version No:	Date:	Version Author:	Approved By:	Approval Date:	Signature
1	December 2024	Christos Polyviou Compliance Officer	The Board	December 2024	

I. Purpose and business description

This policy details how the Company will manage the risks posed by money laundering and terrorist financing for Cryptocurrency usage and will ensure a consistency of approach within the Company. Luckyroo N.V is a limited liability company registered in Curaçao with company registration number 163606, license number OGL/2024/1371/0694 is owning and operating online gambling brand Betwinner. The Company is required to follow the law on Prevention of Money Laundering and Terrorist Financing. The supervised body of the Company is GCB (Curaçao Gaming Control Board) that supervise gaming industry for compliance with legislation and regulation regarding anti-money laundering and countering the financing of terrorism (AML/ CFT).

This policy outlines the framework for identifying, managing, and mitigating risks associated with cryptocurrency usage by Luckyroo N.V. Risk Policy is established in compliance with applicable laws and regulations as required by the Gaming Board Curaçao, relevant international AML standards, and other regulatory bodies overseeing financial technology and cryptocurrency use.

This policy applies to all employees, contractors, subsidiaries, and third-party partners associated with the Company who engage in the handling, transaction, or storage of cryptocurrency in any form within business operations.

II. Relevant legislation and guidance

The Company is required to comply with the following legislation relating to anti-money laundering and counter-terrorist financing (CTF):

Curaçao Gambling and AML Regulations: Compliance with the Gaming Board Curaçao's mandates for the use of cryptocurrency within licensed gaming operations.

Curaçao National Ordinance on Reporting Unusual Transactions (NORUT) and National Ordinance on Identification of Clients for Services (NOIS): Ensuring identification, monitoring, and reporting of unusual or suspicious transactions as stipulated by Curaçao's Financial Intelligence Unit (FIU).

Financial Action Task Force (FATF) Recommendations: Following the FATF guidelines on Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs), specifically FATF Recommendation 15 and the FATF Guidance on a Risk-Based Approach to Virtual Assets.

European Union's 5th and 6th Anti-Money Laundering Directives (AMLD5 and AMLD6): Although Curaçao is outside the EU, these directives provide critical guidance for best practices in crypto-related AML, including KYC measures, recordkeeping, and transaction reporting.

The Basel Committee on Banking Supervision's Principles for handling cryptocurrency risk in financial institutions, providing global standards for mitigating volatility and operational risk.

III. Responsibilities and governance

Board and senior management collectively have responsibility for setting the Company's objectives, defining strategies to achieve them, and establishing the necessary governance risk management and control frameworks to manage the risks to their achievement.

Board of Directors The Board and Senior Management

The Board is responsible for assessing money laundering risk, ensuring the implementation of this policy to minimize the risk, that the appropriate employee training is provided, and that performance review for all employees across the Company takes account of compliance with this manual.

The Board will satisfy themselves that there are appropriate systems and controls in place for any outsourced arrangements to monitor and mitigate the risks posed by money laundering.

The Board is required to provide Compliance Officer with adequate resources and full independence to ensure the Companies' compliance with Money Laundering Regulations.

Compliance Officer: The Compliance Officer is responsible for implementing AML controls, liaising with FIU Curaçao, and coordinating audits. They monitor adherence to both internal and external regulations, managing cryptocurrency compliance documentation.

The Company has appointed Christos Polyviou as the Compliance Officer with overall responsibility for the establishment and maintenance of effective financial crime and anti- money laundering systems and controls.

The Company will ensure that the Compliance Officer has a level of authority and independence within the Company and that he has access to sufficient resources, staff, and information to carry out his/her responsibilities, as well as access to the right members of the senior management team. The Compliance Officer will be subject to the Company's performance management process to ensure ongoing competence in the role of Compliance Officer. Compliance Officer reports directly to the Board.

Responsibilities of the Compliance Officer include:

- On an annual basis prepare and provide the Board with the Compliance Officer Annual Report. The Board will review the Compliance Officer Report on AML provided to them to enable them to appropriately manage the money laundering risks and will take any necessary actions.
- In addition to the annual Compliance Officer Report, on a quarterly basis the Compliance Officer will provide management information to the Board regarding compliance with the policies, operation, and effectiveness of the systems and controls in place to combat money laundering, and recommendations or enhancements required. The Compliance Officer will also escalate AML issues to the Board as considered necessary.
- The Compliance Officer and/or the Board are required to provide the necessary authorities with the required access or information in the case of an AML investigation.
- The Compliance Officer has responsibility for oversight of the Company's compliance with the relevant laws and regulations on systems and controls against money laundering.
- The Compliance Officer will act as a focal point within the Company for all activity relating to anti-money laundering.
- The Compliance Officer is responsible for keeping up to date with changes in laws and regulations in relation to anti-money laundering and making use of findings from national and

international bodies tasked with combating financial crime in order to update the Company's systems and controls where necessary.

- The Compliance Officer responsible for oversight of the Company's compliance with its requirements in respect of staff training.
- The Compliance Officer is the point of contact/escalation for all employees to raise any reports or concerns relating to any suspected or actual money laundering and is responsible for recording, investigating, and reporting this to the relevant authorities, such as the Financial Intelligence Unit (FIU), as necessary. Where reporting to the authorities is not deemed necessary the Compliance Officer will document the reason for this course of action and will, where appropriate, inform senior management and the Board of such decisions.
- The Compliance Officer is responsible for open communication and coordination liaison with the law enforcement authorities dealing with AML/CTF as required.
- This policy will be communicated to all staff during their induction to the Company and any updates will be communicated via email from the Compliance Officer

Risk Management Committee: The Risk Management Committee, comprising senior management and experts in digital assets, oversees risk assessments specific to cryptocurrency. This committee convenes quarterly to evaluate transaction activity, analyse risk exposure, and review control effectiveness.

The responsibilities of the Committee include:

- to drive the implementation of regulatory framework
- to act as an escalation, point for internal breaches, suspicious activities, and any other urgent matters
- to oversee the relationship between the Company and any regulatory bodies in case of any inquiries, audits, or investigations
- to review the effectiveness of the Company's regulatory risk management and compliance framework, in relation to the Company's risk appetite
- to review information which enables the Committee to consider the process established by the company for risk identification and management, assess the risks involved in the company's business and how they are controlled and monitored
- to consider the money laundering and financial crime risks associated with proposed strategies, including any product development and distribution/process changes which could impact the customer experience/outcome
- to review any material breaches of AML policies and procedures
- to have oversight and review the Company's procedures concerning the prevention and detection of fraud and financial crime
- to review the Company's arrangements for regulatory compliance, via its monitoring activities
- to perform other oversight functions, as required

Internal Audit Function: The audit team conducts quarterly evaluations of the cryptocurrency management process, providing independent assessments to the Board and ensuring compliance with both the policy and regulatory standards. The audit team will review the adequacy and effectiveness of the AML framework including policies, procedures, systems, and controls. Furthermore, the audit team will measure compliance with the AML framework and make recommendations for improvements. The Compliance Officer and the Board will be responsible for implementing their recommendations and documenting such implementation.

IV. Cryptocurrency-Specific Risk Identification

Volatility and Market Risk

Cryptocurrency values can fluctuate significantly, posing a financial risk in gaming operations where deposits, bets, and winnings are transacted in cryptocurrency. Company mitigates these risks by:

Stablecoin Usage for High-Value Winnings: Where feasible, the Company uses stablecoins (e.g., USDC or USDT) for larger payouts to provide stability and minimize exposure to price fluctuations.

Payout Limits and Frequency Controls: Payouts over specific thresholds are reviewed for volatility impact. All payouts are segmented across predefined time intervals to prevent large financial losses during extreme price swings.

Procedure: The Financial Department monitors cryptocurrency markets and adjusts payout values to reflect real-time prices. Daily checks are conducted to confirm that all cryptocurrency payouts adhere to the established thresholds, and any adjustments are logged in the transaction ledger.

Regulatory and Compliance Risk

Cryptocurrency regulation varies across jurisdictions and can shift rapidly, especially in the gaming sector. To address regulatory risk:

Ongoing Compliance Monitoring: The Compliance Officer tracks regulatory developments affecting cryptocurrency in online gaming, particularly those imposed by the Gaming Board Curaçao.

Documentation and Record-Keeping: Comprehensive records of all transactions, including KYC documentation, are maintained for a minimum of five years, as mandated by the AMLD5 and Curaçao FIU standards.

Procedure: Regular audits are conducted on documentation and records related to cryptocurrency transactions. The Compliance Team issues monthly reports to the Risk Management Committee and immediately flags any regulatory deviations for corrective action.

AML/CFT and Fraud Risk

Due to the pseudo-anonymous nature of cryptocurrencies, the Company is committed to strong AML and CFT controls to prevent fraud and money laundering. These include:

KYC Procedures: All customers engaging in cryptocurrency transactions undergo rigorous verification, including government-issued ID checks and proof of address verification.

Enhanced Due Diligence (EDD) for High-Risk Transactions: For transactions above certain thresholds or involving high-risk jurisdictions, additional due diligence measures are applied, such as gathering source of funds documentation.

Procedure Flow for High-Risk Transactions: When a transaction exceeds the high-risk threshold, it is flagged by the monitoring system and forwarded to the Compliance Officer. The Compliance Team reviews additional documentation and performs blockchain tracing on the funds' origins. If further investigation is warranted, the transaction is suspended and pending clearance.

Cybersecurity and Asset Protection Risk

Cryptocurrencies, being digital assets, are susceptible to cybersecurity threats such as hacking, phishing, and unauthorized access. The Company employs comprehensive security protocols to protect crypto holdings and transactional integrity.

- **Cold Storage for Long-Term Holdings:** All non-transactional crypto reserves are stored in cold storage wallets, with multi-signature protection.
- **Hot Wallet Security Measures:** Operational wallets used for transactions are secured with two-factor authentication (2FA), real-time monitoring, and transaction limits to minimize exposure.

Procedure: Each day, cryptocurrency holdings in hot wallets are reconciled against the transaction ledger, with any discrepancies flagged for immediate investigation. Access to wallets requires multiple signoffs by authorized personnel, and transaction attempts outside of standard hours trigger automated alerts.

V. AML/CFT Due Diligence and Reporting

Company follows a robust AML/CFT framework tailored to cryptocurrency's unique risks:

- **Customer Due Diligence (CDD):** All users are required to complete CDD checks, including identity verification, address confirmation, and source of funds.
- **Ongoing Monitoring:** Real-time transaction monitoring systems analyse patterns and flag unusual behaviour, such as high-frequency deposits and withdrawals that indicate potential layering or structuring.
- **Suspicious Activity Reporting (SAR):** Any flagged transactions are reported to FIU Curaçao as per NORUT requirements.

Flow of Reporting Suspicious Activity: Upon detecting a suspicious transaction, the system automatically notifies the Compliance Team. The Compliance Officer reviews the transaction and compiles a SAR report. If confirmed, the report is submitted to FIU Curaçao within 24 hours. Documentation of the transaction and SAR report is retained for five years, accessible for audit purposes.

VI. Security Protocols for Cryptocurrency Transactions

Cold Wallet and Hot Wallet Segregation

To enhance security and limit risk, Company distinguishes between hot and cold wallets:

- **Cold Wallets:** Hold 90% of the company's crypto assets in offline, secure storage.

- **Hot Wallets:** Retain only necessary operational funds for daily transactions, with 24-hour limits on maximum value thresholds.

Procedure: Each transfer from cold to hot storage requires multi-level authorization from senior management. Monthly reconciliations validate balances against transaction records, ensuring accuracy and preventing unauthorized transfers.

Access Control and Authentication

Only authorized personnel have access to cryptocurrency wallets, secured by multi-factor authentication and hardware security modules (HSMs).

VII. Operational Controls and Transaction Monitoring

Transaction Monitoring System

The company uses a blockchain analytics system to monitor all incoming and outgoing cryptocurrency transactions. The system flags irregular activity, such as rapid transactions or large withdrawals, prompting further investigation.

Examples of high risk/red flags transactions include:

- Any transaction which shows a different behaviour than expected from the customer either based on the customer's betting history or compared to other customers within the same category
- Any transactions that show one account making one payment using lots of small coins
- Any transaction that shows lots of payments made with one coin
- Any transactions detected as spam on the network
- Any transactions from a high-risk customer as categorized by the Luckyroo N.V (e.g: PEP)
- Any wallet addresses flagged as high risk by blockchain analytics system
- Crypto funds are deposited soon after a customer opens an account and withdrawn again shortly afterward without making use of any of the services and/or products provided by the Company
- Customer deposits fiat funds or crypto assets in an account but leaves the account dormant without any activities
- Withdrawals within 2 months after deposit without placing any bets.
- Funds have been reported as stolen or otherwise reported to have been obtained illegally.
- Transactions are conducted in large volume/amounts or at a high velocity that is inconsistent with peer-group or customer-specific transaction patterns.
- Account is funded through funds held with institutions located in jurisdictions that are either unstable or considered to be high-risk.
- Transactions are carried out in a manner that is inconsistent with reasonable trading patterns/ strategies or at specific times and amounts not congruent with normal industry practices.
- The transaction's script or reference suggests an illicit activity
- Customer involved in crypto asset mining operations (either directly or indirectly through relationships with third parties) that take place in a high-risk jurisdiction, relate to higher-risk crypto assets (such as privacy coins), or where its organization gives rise to higher risk
- Customer who is unable to produce the required KYC information and documentation
- Customer who uses VPN, TOR, encrypted, anonymous, or randomly generated email or a temporary email service

- Customer who requests an exchange to or from cash, privacy coins, or anonymous electronic money
- Customer who sends crypto assets to a newly created address
- Customer who persistently avoids KYC thresholds through smaller transactions
- Customer who requests an exchange to or from a state-sponsored virtual currency that may be used to avoid sanctions
- Customer who exploits technological glitches or failures to his advantage

Procedure Flow for Monitoring: When a transaction is flagged, it enters the compliance review process, where the Compliance Team assesses whether it aligns with known customer activity. Transactions deemed suspicious undergo enhanced scrutiny, while legitimate activity is cleared and documented.

Quarterly and Annual Audits

The Compliance Officer and Internal Audit conduct quarterly reviews on cryptocurrency processes, validating transaction records and confirming adherence to AML protocols. An annual audit includes third-party verification to assess operational controls and cybersecurity standards.

Training and Employee Awareness

The Company is committed to ensuring that all relevant members of staff receive training that is appropriately comprehensive for them to fulfil their roles. All staff is to receive training upon the beginning of employment at the Company and annually. Following training, a test will be given of the material covered to test knowledge and understanding of the materials. The content of the training will revolve around the AML and CTF obligations set out in the relevant legislation.

This policy is reviewed at least annually or whenever deemed necessary. Any amendments, whether driven by regulatory changes or operational requirements, are approved by the Board and communicated to all relevant personnel.