

Cryptocurrency Usage in Payment Processing

Policy date: 15 May, 2025

Version: 1.0

Purpose

The purpose of this policy is to define risk management practices and compliance requirements associated with the indirect use of cryptocurrency in player transactions. While 418Services B.V. (hereinafter referred to as the “operator”) does not directly accept cryptocurrency, the associated risks via the Payment Agent and Payment Service Providers (PSPs) must be managed to ensure regulatory compliance, operational security, and financial integrity.

Scope

This policy applies to:

1. All operator departments involved in payments, compliance, risk management, and audits.
2. The Payment Agent acting on behalf of the operator to process player transactions in fiat currency.
3. Any Payment Service Providers engaged by the Payment Agent that accept cryptocurrency from players.

Policy Statement

The operator commits to mitigating risks related to cryptocurrency transactions by enforcing stringent controls, conducting periodic due diligence, and ensuring compliance with relevant laws and regulations.

Risk Management Principles

1. Governance and Oversight

The Compliance Department will work closely with the Payment Agent to ensure that cryptocurrency risks are systematically identified, assessed, and mitigated.

2. KYC and AML Compliance

2.1. Enhanced KYC Protocols

The Payment Agent must ensure that PSPs implement enhanced KYC measures for all players transacting with cryptocurrency:

- Verified government-issued identification.
- Proof of address (no older than 3 months).
- Source-of-funds declaration if crypto deposits exceed a predefined threshold.

2.2. AML Screening

- All PSPs must conduct comprehensive AML screening of cryptocurrency transactions.
- The Payment Agent must ensure PSPs use blockchain analytics tools to trace cryptocurrency transactions back to their source.

3. Cryptocurrency Transaction Monitoring

3.1. Automated Monitoring Systems

- PSPs must monitor crypto-fiat transactions for anomalies such as:
- High transaction volumes.
- Transactions linked to flagged wallets or jurisdictions.
- Structuring to avoid reporting thresholds.

3.2. Threshold Alerts

- PSPs must notify the Compliance Team of any cryptocurrency transactions exceeding a predetermined threshold, U\$10,000 in fiat.

4. Third-Party Risk Management

4.1. Payment Agent Due Diligence

- The operator will annually evaluate the Payment Agent's risk framework.
- Evaluation criteria include:
- KYC/AML adherence.
- Use of blockchain tools.

4.2. PSP Onboarding

- The Payment Agent must verify PSPs have:
- Financial licenses or registration.
- FATF Travel Rule compliance.
- Anti-fraud systems.

5. Regulatory and Legal Compliance

- The operator will monitor regulatory developments and update the policy as needed.
- An annual Compliance Impact Assessment will be conducted.

6. Volatility and Conversion Risks

6.1. Conversion Timelines

- Crypto accepted by PSPs must be converted to fiat within 24 hours.
- Exceptions must be documented.

6.2. Liquidity Management

- Payment Agent must maintain liquidity to cover conversion delays.

Incident Management

1. Detection: Flag by PSP or Payment Agent.
2. Escalation: Notify Compliance within 24 hours.
3. Investigation: Review transaction data and KYC.
4. Reporting: Notify authorities as required.
5. Remediation: Update controls and processes.

Enforcement and Consequences

- Breaches by PSPs or Payment Agents may lead to:
- Contract termination.
- Regulatory reporting.
- Internal disciplinary action.

Training and Awareness

- Annual training on:
- Cryptocurrency risk management.
- Regulatory changes.
- Blockchain analytics.

Review and Updates

- Reviewed upon regulatory changes.
- Updates require senior management approval.

Attachments

1. Crypto Risk Assessment Template
2. Incident Reporting Form
3. Regulatory Reference Guide

Attachment 1: Crypto Risk Assessment Template

Assessment Area	Risk Description	Likelihood (High/Med/Low)	Impact (High/Med/Low)	Mitigation Measures	Responsible Party
Customer Identity Risk	Insufficient KYC checks on crypto-originating funds	High	High	Require robust KYC/AML standards from PSPs	Payment Agent
Illicit Source of Funds	Funds originating from sanctioned jurisdictions	Medium	High	Use blockchain analytics to flag high-risk wallets	PSPs & Payment Agent
Conversion Delays	Delayed fiat conversion leading to volatility risk	Low	Medium	Mandate immediate conversion policies	Payment Agent
Regulatory Non-Compliance	PSP failure to comply with evolving crypto laws	High	High	Conduct regular PSP compliance audits	Compliance Team
Transaction Fraud	Suspicious transaction patterns or anomalies	Medium	High	Implement automated monitoring tools	Payment Agent

Attachment 2: Incident Reporting Form

Incident Details

1. **Date of Incident:** [Enter Date]
2. **Time of Incident:** [Enter Time]
3. **Reported By:** [Name/Role]
4. **Incident Description:** [Provide a brief summary of the suspicious activity]

Involved Parties

1. **Player ID/Account:** [Enter Details]
2. **PSP Name:** [Enter Name]
3. **Cryptocurrency Involved:** [Specify, e.g., Bitcoin, Ethereum]
4. **Transaction Amount (Fiat/Equivalent Crypto):** [Enter Amount]

Preliminary Investigation

1. **Source Wallet Address:** [Enter Address]
2. **Blockchain Analytics Results:** [Summarize Findings]
3. **Risk Level Assessment:** [High/Medium/Low]
4. **Immediate Action Taken:** [Freeze Funds, Notify Authorities, etc.]

Next Steps

1. **Further Investigation Required (Yes/No):** [Specify]
 2. **Date for Follow-Up:** [Enter Date]
 3. **Responsible Team/Individual:** [Enter Details]
-