

Cryptocurrency Usage in Payment Processing

Sky Interactive B.V.

30 April 2025

[version #1.0]

Purpose

The purpose of this policy is to establish a framework for managing the risks and ensuring compliance obligations associated with the indirect involvement of cryptocurrency in player payment transactions. Although Sky Interactive B.V. (hereinafter referred to as the “Operator”) does not directly accept or process cryptocurrency, the Operator acknowledges the potential exposure to cryptocurrency-related risks through its relationships with the appointed Payment Agent and any affiliated Payment Service Providers (PSPs). This policy is designed to proactively address those risks in order to uphold regulatory compliance, safeguard operational integrity, and maintain the transparency and traceability of all financial transactions.

This policy also serves to align internal processes with applicable anti-money laundering (AML), counter-terrorism financing (CTF), and financial crime prevention standards, while ensuring that all payment channels involving the indirect flow of cryptocurrency are subject to rigorous oversight and governance.

Scope

This policy applies to:

1. Internal Stakeholders: All operator departments that are involved in or have oversight of payment processing, risk management, regulatory compliance, finance, and internal or external audits..
2. Payment Agent: The entity authorized to act on behalf of the operator to facilitate and process player transactions denominated in fiat currency.
3. Payment Service Providers: Third-party PSPs engaged by the Payment Agent that accept cryptocurrency as a form of payment from players.

Policy Statement

The operator is committed to maintaining the highest standards of integrity and transparency in all aspects of its payment processing operations by enforcing stringent controls, conducting periodic due diligence, and ensuring compliance with relevant laws and regulations. Through the adoption of this policy, the operator reinforces its commitment to responsible financial conduct and to minimizing the legal, reputational, and operational risks that may arise from indirect cryptocurrency exposure.

Risk Management Principles

1. Governance and Oversight

The operator's Compliance Department shall maintain continuous oversight of payment activities conducted by the Payment Agent and its affiliated PSPs. This includes, but is not limited to:

- Collaborating with the Payment Agent to develop and implement risk mitigation strategies to limit exposure.
- Ensuring that governance structures support the identification, assessment, monitoring, and reporting of cryptocurrency-related risks.
- Integrating crypto-related risk management into the broader enterprise risk management framework.

2. Know Your Customer (KYC) and Anti-Money Laundering (AML) Compliance

2.1. Enhanced KYC Protocols

The Payment Agent must ensure that all PSPs engaging in cryptocurrency transactions enforce robust, risk-based KYC procedures, including, at minimum:

- Verification of government-issued photo identification.
- Proof of residential address, dated within the last three (3) months.
- Declaration of the source of funds, required for any cryptocurrency transaction that exceeds pre-established thresholds.

2.2. AML Screening

- All PSPs are required to conduct comprehensive AML screening of users and transactions, using risk indicators and sanction lists in accordance with applicable regulations.
- Suspicious activity must be escalated for immediate internal review and, where necessary, reported to competent authorities.
- The Payment Agent must ensure PSPs use blockchain analytics tools securing cryptocurrency transactions' traceability to legitimate sources.

3. Cryptocurrency Transaction Monitoring

3.1. Automated Monitoring Systems

PSPs must implement automated surveillance systems capable of detecting and flagging unusual activity related to crypto-fiat conversions. These systems should include, but are not limited to:

- Detection of atypical transaction volumes or patterns inconsistent with historical player behavior.

- Identification of transactions linked to flagged wallet addresses, entities under sanction or high-risk jurisdictions.
- Monitoring of transaction structuring, including payment splitting to avoid reporting thresholds.

3.2. Threshold Alerts

- PSPs must generate real-time alerts for any cryptocurrency transaction exceeding a predefined fiat-equivalent threshold (e.g., € 5,000).
- Such alerts must be escalated immediately to both the Payment Agent and the operator's Compliance Department, with supporting documentation and a preliminary risk assessment.

4. Third-Party Risk Management

4.1. Payment Agent Oversight

The operator shall evaluate the Payment Agent's risk management and compliance control framework annually to ensure alignment with contractual obligations.

Evaluation criteria include:

- Assessment of the Payment Agent's ongoing due diligence of PSPs and their adherence to KYC/AML regulations.
- Review of technical solutions used for blockchain forensics and transaction monitoring.
- Examination of adherence to contractual and regulatory obligations.

4.2. PSP Onboarding

The Payment Agent must perform rigorous due diligence before onboarding any PSPs that handle cryptocurrency. This includes verification of:

- Licensing or registration with relevant financial regulatory authorities.
- Compliance with the FATF Travel Rule, jurisdiction-specific crypto regulations, and financial crime prevention frameworks.
- Implemented anti-fraud controls and blockchain tracing tooling.

5. Regulatory and Legal Compliance

- The operator shall actively monitor global regulatory developments in the cryptocurrency space to ensure continuous compliance.
- Legal and regulatory changes affecting cryptocurrency transactions shall be reflected in updates to this policy.

- A Compliance Impact Assessment will be conducted annually to identify gaps and areas for improvement.

6. Cryptocurrency Volatility and Conversion Risk

6.1. Timely Conversion of Cryptocurrency

To minimize financial exposure to market fluctuations:

- PSPs must convert all cryptocurrency received from players into fiat currency within twenty-four (24) hours of receipt .
- Exceptions to this timeline may only be granted on a case-by-case basis and must be formally documented, with rationale provided to the Payment Agent and communicated to the operator.

6.2. Liquidity Management

- The Payment Agent shall maintain adequate liquidity reserves to secure fiat settlements and ensure minimized delays in cryptocurrency conversion during periods of elevated market volatility.

Incident Management

The operator maintains a structured and timely incident management framework to address suspicious activity arising from cryptocurrency-related transactions:

1. **Detection:** Any unusual or potentially suspicious transaction involving cryptocurrency is identified and flagged by the relevant PSP or the Payment Agent, based on predefined risk and transaction monitoring indicators.
2. **Escalation:** Upon detection, the Payment Agent shall to escalate the incident to the operator within twenty-four (24) hours, providing all relevant details and supporting data.
3. **Investigation:** A joint investigation involving the operator, payment agent and relevant PSP shall be initiated, this review includes, but is not limited to:
 - Review of transaction monitoring data from the PSP.
 - Blockchain analytics findings related to wallet addresses, transaction flows or other data points deemed relevant.
 - Collection of additional KYC items if necessary.
4. **Reporting:** If the investigation concludes that a transaction is suspicious, a Suspicious Transaction Report (STR) shall be submitted to the financial intelligence unit (FIU), in accordance with the jurisdictional reporting requirements and statutory timeframes.
5. **Remediation:** Recommendations for remedial actions and control enhancements will be proposed and submitted to senior management. These may include updates to internal procedures, escalation protocols, or third-party oversight measures among others.

Enforcement and Consequences

Strict adherence to this policy is mandatory. Failure to comply may lead to legal, financial, and reputational consequences for the breaching party. The following enforcement measures apply:

- Immediate termination of contracts or service agreements where non-compliance is material or persistent.
- Referral to relevant regulatory or enforcement authorities where breaches involve financial crime or statutory violations.
- Financial penalties or indemnification obligations, in accordance with existing contractual clauses.
- A breach of this policy by operator internal staff, shall result in disciplinary actions, up to and including termination of employment, consistent with the operator's internal disciplinary procedures.

Training and Awareness

To support effective implementation and continuous compliance with this policy, the operator shall deliver annual training for all personnel whose roles intersect with cryptocurrency-related activities. Training will include:

- Identification and mitigation of cryptocurrency-specific risks in payment channels.
- Regulatory developments impacting cryptocurrency and associated providers.
- Practical training on the use of blockchain analytics and monitoring tools.
- Incident handling procedures and reporting obligations.
- Ad hoc training.

Policy Review and Updates

This policy shall be reviewed and/or updated:

- Upon any material change in applicable laws or regulations related to cryptocurrency, payment processing, or AML/CTF obligations.
- In response to significant incidents, enforcement actions, or findings indicating control weaknesses.
- Annually, to ensure ongoing relevance and effectiveness.

Incident Reporting Form

Incident Details

Date of Incident:

Time of Incident:

Reported By (Name/Role):

Incident Description:

Involved Parties

Player ID / Account:

Payment Service Provider (PSP) Name:

Cryptocurrency Involved:

Transaction Amount (Fiat / Crypto Equivalent):

Preliminary Investigation

Source Wallet Address:

Blockchain Analytics Results:

Risk Level Assessment:

- ☐ High
- ☐ Medium
- ☐ Low

Immediate Action Taken:

- ☐ Funds Frozen
- ☐ Authorities Notified
- ☐ Other (specify): _____

Next Steps

Further Investigation Required:

- ☐ Yes
- ☐ No

Date for Follow-Up:

Responsible Team / Individual:
