

CRYPTOCURRENCY USAGE IN PAYMENT PROCESSING

METASPINS NV

10.03.2025

V 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 Metaspins NV (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 and the PSP to ensure that cryptocurrency risks are systematically identified, assessed, and mitigated.

2. KYC and AML Compliance

2.1. Enhanced KYC Protocols

The Operator must ensure to implement KYC measures for all players transacting with cryptocurrency at the specified thresholds.

2.2. AML Screening

- PSPs must conduct comprehensive AML screening of cryptocurrency transactions, flagging suspicious activity for immediate review.
 - PSPs may use blockchain analytics tools to trace cryptocurrency transactions back to their source.
-

3. Cryptocurrency Transaction Monitoring

3.1. Automated Monitoring Systems

PSPs must deploy automated systems to monitor crypto-fiat transactions for anomalies, including:

- High transaction volumes inconsistent with typical player behavior.
- Transactions linked to flagged wallet addresses or high-risk jurisdictions.
- Structuring of transactions to avoid reporting thresholds.

3.2. Threshold Alerts

- PSPs must notify the Operator's compliance team of any cryptocurrency transactions exceeding transactions in the amount of XCG 5,000 or more, regardless whether the transaction is made in cash, by check or other form of payment, or through electronic or other non- physical means.
-

4. Third-Party Risk Management

4.1. Payment agent Due Diligence

The Operator will evaluate the PSP's risk management framework annually to ensure compliance with contractual obligations.

Evaluation criteria include:

- Evaluation of PSPs' adherence to KYC/AML regulations.
- Review of blockchain monitoring and risk management tools.

4.2. PSP Onboarding

- The Operator must perform rigorous due diligence before onboarding any PSPs that handle cryptocurrency. This includes verifying:
 - Licenses or registrations with financial regulators.
 - Evidence of compliance with FATF Travel Rule and other jurisdictional requirements.
 - Implementation of anti-fraud and blockchain tracing technologies.

5. Regulatory and Legal Compliance

- The Operator will actively monitor global regulatory developments in cryptocurrency to ensure continuous compliance.
 - Any new or amended laws affecting cryptocurrency transactions must be reflected in updates to this policy.
 - A Compliance Impact Assessment will be performed annually to identify gaps and areas for improvement.
-

6. Incident Management

In the event of suspicious cryptocurrency-related activity:

1. **Detection:** The PSP or payment agent flags the transaction as suspicious.
 2. **Escalation:** The payment agent notifies the Operator Compliance Team within 24 hours of the flagged activity.
 3. **Investigation:** A joint investigation is conducted involving:
 - PSP's transaction monitoring data.
 - Blockchain analytics results.
 - Additional KYC documents if required.
 4. **Reporting:** Suspicious transactions must be reported to relevant authorities within the legally mandated timeframes.
 5. **Remediation:** Recommendations for process improvements and updated controls are submitted.
-

Enforcement and Consequences

Non-compliance with this policy by the payment agent or PSPs may result in:

- Termination of contracts.
 - Reporting to regulatory authorities.
 - Financial penalties, as per contractual agreements.
 - Internal violations by Operator staff will lead to disciplinary actions, up to and including termination of employment.
-

Training and Awareness

The Operator will provide annual training for all relevant personnel on:

- Cryptocurrency risk management.
 - Updated regulatory requirements.
 - Use of blockchain analytics tools for risk monitoring.
-

Review and Updates

- This policy will be reviewed if regulatory changes occur.
- All updates must be approved by the senior management.

Attachments

1. Crypto Risk Assessment Template
2. Incident Reporting Form

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	Operator
Illicit Source of Funds	Funds originating from sanctioned jurisdictions	Medium	High	Use blockchain analytics to flag high-risk wallets	PSPs & payment agent
Regulatory Non-Compliance	PSP failure to comply with evolving crypto laws	High	High	Conduct regular PSP compliance audits	Operator
Transaction Fraud	Suspicious transaction patterns or anomalies	Medium	High	Implement automated monitoring tools	PSPs & 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]
-