

Policy on Direct Cryptocurrency Transactions for Players Accounts without Intermediated Payment Processing

Gareton B.V.

11.11.2025

1. Purpose

The purpose of this policy is to define risk management practices and compliance requirements to prevent AML/CFT/CFP and other illicit activities through the direct use of cryptocurrency payments in player transactions, where the Payment Agent is involved only in fiat transactions and not in crypto processing.

This policy outlines the responsibilities of Gareton B.V. (hereinafter referred to as the “Operator”) to ensure regulatory compliance, detect and report suspicious activities, mitigate risk from direct cryptocurrency transactions, and establish a framework for customer due diligence (CDD) and record keeping.

2. Scope

This policy applies to:

1. All Operator departments involved in payments, compliance, risk management, and audits.
2. The Payment Agent, solely responsible for fiat currency processing, is excluded from any crypto transaction operations.
3. Any internal or third-party services facilitating direct wallet interactions.

3. 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.

4. Risk Management Principles

4.1. Governance and Oversight

The Operator’s Compliance Department shall ensure that risks associated with cryptocurrency are systematically identified, assessed, and mitigated. The Payment Agent’s role is limited exclusively to fiat operations and does not encompass any part of the crypto transaction’s workflow. The PSPs still have the obligation to consider sanctions jurisdictions and high-risk jurisdictions when conducting fiat operations. All governance responsibilities related to cryptocurrency transactions lie solely with the Operator.

4.2. Risk Assessment

Ongoing risk assessments will evaluate:

- The nature of cryptocurrencies used
- Jurisdictional risks
- Customer and transaction behavior
- Technological vulnerabilities

4.3. Customer Due Diligence (CDD)

4.3.1 Identity Verification (KYC)

All customers making crypto deposits or withdrawals exceeding EUR2000,-- or equivalent, are required to:

- Submit a verified government-issued identification.
- Submit a recent proof of address (not older than 3 months).

- Provide the source-of- cryptocurrency funds

4.3.2 Enhanced Due Diligence (EDD)

EDD will be applied when:

- Customers are from high-risk jurisdictions
- Activities are inconsistent with typical gaming behavior
- Transactions are linked to flagged wallets or unusual patterns

4.4. Transaction and Ongoing Monitoring

The Operator will use both automated and manual tools to:

- Screen wallet addresses using blockchain analytics
- Flag transactions linked to sanctioned entities/jurisdictions
- Detect structuring of transactions
-

Transactions exceeding EUR2000, -- (or equivalent) must trigger an alert to the Compliance Department, and be recorded in the Transaction Monitoring Register.

4.5. Consistent Crypto Flow Requirement

To ensure consistency, traceability, and the mitigation of financial crime risks, the Company enforces a strict policy whereby all incoming cryptocurrency transactions must be returned in the same cryptocurrency and to the originating wallet address. The designated Payment Agent is only involved in fiat transactions, and is not responsible for or involved in the processing, custody, or flow of cryptocurrency funds.

4.5 Regulatory and Legal Compliance

- Actively monitor global regulatory developments in cryptocurrency to ensure continuous compliance.
- Reflect any new or amended laws affecting cryptocurrency transactions in policy updates.
- Conduct a Compliance Impact Assessment annually to identify gaps and areas for improvement.

5. Incident Management

In the event of suspicious cryptocurrency-related activity, employees must escalate suspicious activity to the AML Compliance Officer or MLRO, who will:

1. Investigate the alerts
 2. File Suspicious Transaction Reports with the FIU
 3. Recommend improvements to processes and controls
-

6. Enforcement and Consequences

Non-compliance will result in disciplinary actions, up to and including termination of employment.

7. Training and Awareness

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

- Cryptocurrency risk management.
- AML Compliance
- Updated regulatory requirements.
- Use of blockchain analytics tools

8. Record Keeping

All KYC documentation, transaction records, and monitoring logs will be retained for a minimum of 5 years in compliance with applicable AML requirements.

9. Review and Updates

- This policy will be reviewed if regulatory changes occur.
- Operational restructuring

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/inadequate KYC checks on crypto-originating funds	High	High	Adhere to internal KYC/AML standards. Require robust documentation and validation	Operator Compliance Team
Illicit Source of Funds	Use of wallets linked to sanctioned jurisdictions or jurisdictions with a regulatory concern	Medium	High	Use blockchain analytics to flag high-risk wallets	Operator
Transaction Fraud	Suspicious transaction patterns or anomalies	Medium	High	Implement automated (real time) monitoring tools and alert systems	Risk & Compliance Team

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]
-