Transaction Monitoring & Fraud Detection Policy

Version	1.0
Effective Date	01 June 2025
Approved By	Compliance & Risk Committee
Next Review Date	01 June 2026

bayarcash

1. Purpose

The purpose of this policy is to establish clear guidelines and procedures for monitoring financial transactions and detecting fraudulent activity at Bayarcash Sdn. Bhd. (Registration Number: 202201040365 (1486062-H)) ("**Bayarcash**"). This ensures the integrity of the company's operations, protects customer assets, and mitigates financial and reputational risk.

2. Scope

This policy applies to:

- All financial transactions processed by Bayarcash, including deposits, withdrawals, transfers, and payments.
- All Bayarcash employees, contractors, and third-party service providers involved in transaction processing, monitoring, or investigation.
- All systems, databases, and software used for transaction management operated by Bayarcash.

3. Policy Statement

Bayarcash is committed to:

- Identifying and preventing fraudulent or suspicious activities in real-time.
- Complying with applicable laws, regulations, and industry standards (e.g., AML, KYC, PCI DSS).
- Maintaining transparency, accuracy, and accountability in transaction monitoring processes.
- Protecting customer information and assets from unauthorized access or misuse.

4. Roles & Responsibilities

4.1 Fraud Detection & Risk Management Team

- Monitor transactions continuously for suspicious patterns or anomalies.
- Investigate alerts and escalated cases of potential fraud.
- Maintain records of investigations and findings.

4.2 IT & Security Team

- Ensure transaction monitoring systems are secure, reliable, and up-to-date.
- Implement automated tools for anomaly detection, reporting, and alerting.

4.3 Compliance & Legal Team

- Ensure procedures comply with regulatory requirements.
- Coordinate with law enforcement or regulatory authorities when necessary.

4.4 Employees

- Report any suspicious activity observed during transaction processing.
- Adhere to internal controls and fraud prevention protocols.

5. Transaction Monitoring Procedures

5.1 Automated Monitoring

All transactions are subject to real-time automated monitoring for:

- Unusual transaction amounts or frequency.
- Transactions to high-risk regions or entities.
- Rapid account activity inconsistent with historical patterns.

5.2 Manual Review

- Alerts generated by automated systems are reviewed by the **Fraud Detection Team**.
- High-risk transactions are escalated for detailed investigation.

5.3 Risk Scoring

Each transaction is assigned a risk score based on factors such as:

- Amount, frequency, and location.
- Account history and behavior patterns.
- External threat intelligence or known fraud trends.

6. Fraud Detection & Response

- Investigate suspected fraud immediately.
- Freeze accounts, payments, or transactions if necessary to prevent loss.
- Document findings, actions taken, and outcomes in a secure incident log.
- Notify affected customers and relevant authorities in accordance with regulatory requirements.
- Review and update fraud detection rules based on lessons learned.

7. Reporting & Escalation

- **Suspicious Activity Reports (SARs)** are submitted to regulatory authorities as required.
- Internal escalation follows a defined hierarchy:
    - Fraud Detection Analyst
    - Fraud Detection Manager
    - Head of Risk & Compliance
- Reports include: account details, transaction history, risk assessment, and actions taken.

8. Data Security & Confidentiality

- Customer and transaction data must be protected according to Bayarcash's **Access Control & User Management Policy** and applicable data protection regulations.
- Unauthorized disclosure of customer information during monitoring or investigation is strictly prohibited.

9. Employee Training & Awareness

- All relevant employees undergo annual training on fraud detection, transaction monitoring procedures, and regulatory compliance.
- Employees are educated on common fraud schemes, social engineering, and internal reporting mechanisms.

10. Review & Continuous Improvement

- Fraud detection rules, systems, and processes are reviewed at least quarterly or after significant incidents.
- Feedback from investigations and audits informs updates to monitoring tools and procedures.

11. Review & Continuous Improvement

- Regular audits are conducted to ensure adherence to this policy and applicable regulatory requirements.
- Non-compliance may result in disciplinary action, up to and including termination.

12. Policy Review

- This policy will be reviewed annually or following major regulatory, operational, or technological changes.
- Updates require approval from the Compliance & Risk Committee and executive management.

13. Bayarcash Transaction Monitoring & Fraud Detection Flowchart

13.1 Transaction Initiation

The customer performs a transaction (deposit, withdrawal, transfer, payment).

13.2 Automated Monitoring

System checks transaction in real-time against:

- Transaction amount limits.
- Frequency of transactions.
- Account history & behavior patterns.
- High-risk countries/entities.

13.3 Risk Scoring

Assign a risk score based on:

- Amount & frequency.
- Geolocation & IP analysis.
- Historical activity patterns.
- Known fraud trends.

13.4 Risk Assessment Decision

- **Low Risk**: Transaction approved automatically.
- **Medium Risk**: Transaction flagged for review.
- **High Risk**: Transaction temporarily blocked and escalated.

13.5 Manual Review by Fraud Detection Team

- For flagged and high-risk transactions.
- Analyst reviews transaction details.
- Validates if it's legitimate or potentially fraudulent.

13.6 Investigation & Action

If fraud confirmed:

- Freeze account/payment.
- Notify customers.
- Report to authorities/regulators.

If fraud not confirmed:

- Approve transaction.
- Document findings.

13.7 Record Keeping & Continuous Improvement

- Log all alerts, reviews, and actions.
- Update automated monitoring rules based on lessons learned.
- Conduct periodic audits.