Fraud Prevention Policy

Paymit Limited

1. Introduction

At Paymit, we are committed to detecting, deterring, and preventing fraudulent activities that could compromise the integrity of our payment services. Fraud remains a significant challenge within the financial services sector, and as a regulated entity, Paymit implements robust measures to mitigate risks and safeguard customers, employees, and partners.

Fraud can occur in multiple ways, including deceptive schemes targeting consumers or attempts to exploit Paymit's systems for illicit gains. This policy outlines the common fraud typologies that Paymit encounters and the security measures implemented to prevent fraudulent transactions.

2. Statement of Intent

Paymit Ltd adopts a zero-tolerance policy towards fraud. All employees, customers, and partners must uphold honesty, transparency, and accountability. This policy ensures that:
- Fraudulent activities are identified and mitigated proactively.
- Customers are protected from financial crime.
- Internal processes are aligned with UK regulatory obligations.

3. Responsibilities in Fraud Prevention

At **Paymit Ltd**, fraud prevention is a collective responsibility that involves senior management, the Money Laundering Reporting Officer (MLRO), and all employees. Each level of the organization plays a crucial role in ensuring fraud risks are mitigated effectively.

Below are the designated responsibilities:

a. Senior Management Responsibilities

The **Board of Directors and Senior Management** are responsible for overseeing the strategic direction of fraud prevention efforts, ensuring compliance with regulatory requirements, and promoting a culture of integrity and accountability.

Key Responsibilities:

- Establish and uphold a **zero-tolerance policy** towards fraud.
- Ensure **adequate resources** and budget allocation for fraud prevention technologies, training, and compliance monitoring.
- Approve and **review fraud risk assessments** at least annually, making necessary updates to the fraud prevention framework.
- Oversee the **implementation of fraud prevention controls**, ensuring alignment with the **Fraud Act 2006, Bribery Act 2010, and Money Laundering Regulations 2017**.
- Regularly review fraud risk indicators and **approve reports submitted by the MLRO** regarding suspicious activities or fraudulent transactions.

- Ensure that **internal controls and governance policies** are in place to deter fraud at all levels of the organization.
- Authorize **escalation of fraud cases** to external authorities such as **Action Fraud, the National Crime Agency (NCA), and the Financial Conduct Authority (FCA)** where necessary.

b. Money Laundering Reporting Officer (MLRO) Responsibilities

The **MLRO** is responsible for fraud detection, investigation, and regulatory compliance. The MLRO ensures that fraud risks are continuously assessed and mitigated through appropriate control measures.

Key Responsibilities:

- Serve as the **primary point of contact for fraud-related concerns** within Paymit and liaise with external regulators and law enforcement agencies.
- Implement **fraud detection mechanisms**, including **real-time transaction monitoring, suspicious activity reporting, and enhanced due diligence (EDD)** for high-risk customers.
- Ensure that fraud prevention policies are **regularly reviewed and updated** in line with emerging threats and regulatory changes.
- Review **high-risk transactions and customer profiles**, approving or rejecting them based on fraud indicators.
- Conduct **internal fraud investigations** and escalate confirmed fraud cases to the **NCA, FCA, and Action Fraud** where applicable.
- Ensure employees receive **regular training on fraud prevention, social engineering risks, and transaction monitoring**.
- Oversee **automated fraud detection tools** such as **ACURIS RISK INTELLIGENCE and EMLO TECHNOLOGIES**, ensuring they operate efficiently.
- Provide **quarterly fraud risk assessments** to senior management and the board of directors.
- Maintain **a record of fraud cases**, including internal and external fraud incidents, ensuring appropriate follow-up actions.

c. Employee Responsibilities

Every Paymit employee, regardless of their role, has a duty to be vigilant against fraud. Employees must understand their responsibilities in preventing, detecting, and reporting fraudulent activities.

Key Responsibilities:

- Adhere to Paymit's **fraud prevention and AML policies** at all times.
- Identify **red flags** that indicate potential fraud, including **suspicious transactions, inconsistent customer behavior, and fraudulent documentation**.

- Report any suspected fraud to the **MLRO or compliance team** using the internal fraud reporting mechanism.
- Undergo **mandatory fraud prevention training**, ensuring they remain aware of the latest fraud typologies and best practices.

d. Legislative Framework

This policy adheres to the following laws and regulations governing financial crime and fraud prevention:
- Fraud Act 2006
- Bribery Act 2010
- Money Laundering Regulations (MLR) 2017
- Proceeds of Crime Act 2002
- General Data Protection Regulation (GDPR) and Data Protection Act 2018
- FCA and HMRC Regulatory Framework

4. Fraud Definition and Categories

Fraud is defined as an intentional act of deception to secure an unfair or unlawful financial gain. It includes:

- Theft: Unauthorized appropriation of funds or assets.
- Identity Theft: Using stolen personal information for fraudulent transactions.
- False Accounting: Manipulating financial records for deceitful purposes.
- Bribery & Corruption: Unlawful financial incentives to influence decisions.
- Conspiracy to Defraud: Coordinated fraudulent activities by multiple parties.

5. Types of Fraud and Prevention Measures

a. Consumer Fraud

Consumer fraud occurs when fraudsters manipulate individuals into transferring money through deceptive schemes. Fraudsters use social engineering tactics to persuade victims that they are making legitimate payments.

i. Identity Theft

Fraudsters may attempt to use stolen or synthetic identities to gain unauthorized access to financial services.

Mitigation Measures:

- **Electronic Verification (e-KYC):** Paymit employs real-time ID verification through GBG Onfido to validate customer identities.
- **Document Authenticity Checks:** Customers must provide proof of identity and address when required, which are cross-referenced with official databases (Electronic Verification).

- **Two-Factor Authentication (2FA):** Users must authenticate transactions using an additional security layer.

ii. Lottery and Prize Scams

Fraudsters inform victims that they have won a lottery or prize but must first pay a fee to claim their winnings.

Mitigation Measures:

Enhanced Fraud Warnings: Paymit includes fraud alerts at key transaction stages, warning users of potential scams.

Suspicious Payee Monitoring: Unusual beneficiaries or repeated requests from unverified sources are flagged.

Customer Support Checks: Customer service representatives are trained to identify victims and intervene where necessary.

iii. Family Emergency Scams

Fraudsters impersonate a relative or friend of the victim, claiming they are in an emergency and urgently need money.

Mitigation Measures:

- **Verification Prompts:** Paymit advises customers to confirm such requests by directly contacting their relative or friend before making any payment.
- **Automated Fraud Alerts:** Transactions flagged as high-risk may be paused for additional verification. Transactions that deviate from usual remittance pattern/ expected flow of funds and flagged.
- **Customer Education:** Users are regularly informed about common scams via emails and in-app notifications.

b. Account Takeover and Unauthorized Access

Cybercriminals may attempt to gain unauthorized access to a customer's account through phishing, credential stuffing, or malware.

Mitigation Measures:

- **Two-Step Verification:** Customers are required to verify their identity via OTP (One-Time Password) when logging in and making transactions.
- **Transaction Approval via 3D Secure:** Every transaction is verified through 3D Secure authentication.
- **Automated Monitoring:** Paymit's real-time transaction monitoring system flags suspicious activities for review.

c. Online Purchase Scams

Fraudsters may lure victims into sending money for non-existent goods or services.

Mitigation Measures:

- **Strict Verification of Payees:** Paymit does not allow third-party transactions without verification.
- **Real-Time Monitoring Alerts:** The system flags unusual spending patterns that could indicate a scam.
- **Customer Awareness:** Paymit provides fraud prevention education to customers through emails and notifications.

d. Card Fraud

This includes various schemes such as lost or stolen cards, card cloning (skimming), and Card Not Present (CNP) fraud.

Mitigation Measures:

- **Only Cardholder Transactions Allowed:** Paymit ensures that payments can only be made using cards belonging to the registered account holder.
- **3D Secure Authentication:** A mandatory step for all card-based transactions.
- **Real-Time Monitoring:** Transactions undergo automated monitoring for anomaly detection.

e. Money Laundering via Paymit Platform

Fraudsters may use stolen funds or engage in layering techniques to disguise illicit financial activities.

Mitigation Measures:

- **Automated AML Screening:** Paymit integrates ACURIS RISK INTELLIGENCE to screen all transactions and parties against sanction lists.
- **Transaction Monitoring via EMLO TECHNOLOGIES:** A sophisticated system that uses 50+ AML rules to detect unusual transaction patterns.
- **Enhanced Due Diligence (EDD):** High-risk customers undergo additional verification and must submit proof of source of funds.
- **Transaction Limits:** Paymit enforces periodic transaction limits to mitigate abuse.

f. Internal Fraud

Employees may misuse their access to engage in fraudulent activities, such as processing unauthorized transactions.

Mitigation Measures:

- **Role-Based Access Control (RBAC):** Employees only have access to information necessary for their role.
- **Multi-Level Approval System:** Large transactions require MLRO approval.
- **Audit Trail:** All activities are logged and periodically reviewed for suspicious behavior.
- **Regular Employee Training:** Staff undergoes mandatory fraud prevention training to recognize and report fraudulent activities.

g. Chargeback Fraud

Some users may initiate chargebacks falsely, claiming they did not authorize a transaction.

Mitigation Measures:

- **Clear Transaction Descriptions: We will make sure that** customers can easily recognize transactions on their bank statements with clear company name, as many customers claim chargeback when they do not recognize a charge clearly.
- **Automated Customer Alerts:** Customers receive instant notifications for every transaction.
- **Dispute Resolution Mechanism:** Paymit promptly investigates chargeback requests to identify fraudulent claims.
- Clarity and transparency in our refund policy are paramount. We ensure customers have a thorough understanding of these policies before engaging in transactions with Levantine Express.

h. Phishing and Social Engineering Attacks

Fraudsters may impersonate Paymit or trick customers into revealing personal information.

Mitigation Measures:

- **Security Awareness Campaigns:** Paymit educates users on recognizing phishing attempts.
- **Official Communication Policy:** Customers are advised to verify emails and never share login credentials.
- **Fraud Reporting Channel:** Users can report suspected fraud directly to Paymit.

6. Fraud Reporting and Response

Customers and employees are encouraged to report any suspicious activity via Paymit's fraud reporting channels. Paymit will:

1. **Investigate and Block Fraudulent Transactions:** Suspicious transactions are reviewed by the compliance team and blocked if necessary.
2. **Report Fraud to Authorities:** Any fraud involving criminal activity is reported to the action fraud: https://reporting.actionfraud.police.uk/login For vulnerable consumers or where there is a suspicion that a fraudster may be collecting funds in the UK, this will also be reported to the NCA.National Crime Agency (NCA).
3. **Take Legal Action:** Paymit reserves the right to take legal action against fraudsters, including terminating accounts found engaging in fraud.