PAYPORT UK

Anti-Fraud policy and procedure

Table of Contents

Document Control

Approver(s)	Board of Directors
Policy Owner	MLRO – Alexander Kostiaev
Version	1.0
Status	Operational
Last Reviewed Date	June 2020
Date of Next Scheduled Review	June 2021

1. Introduction

PAYPORT UK (SimplePay London Ltd) has been providing Electronic Money Services since 01/04/2019. As a e-money service provider, PAYPORT UK will face the threat of fraud (both internal and external) which will need to be addressed.

Purpose of this Document

This document specifies PAYPORT UK's approach in identifying the fraud risks that it faces, when delivering its payment service, and implementing the necessary controls to mitigate them.

2. Risk Assessment

All Fraud risks have been identified using a fraud risk assessment, which has been appended to this document.

The risk assessment has provided details of the following:

- Details of Internal and External Fraud risks PAYPORT UK faces
- The controls in place to mitigate those risks
- The policies that have been developed to implement the controls
- Details of how the policies are monitored

3. Fraud Risks

PAYPORT UK has identified the following risks relating to fraud:

3.1 Internal Fraud

- Falsification of records
- Forging of signatures
- Involvement with bribes
- Breaches of anti-money laundering procedures
- Any financial crime
- Misleading representations
- Improper verification of KYC information during account registration

3.2 External Fraud

- External fraud by suppliers includes:

  - Payment for services and goods not supplied
  - Kickbacks for biased selection of suppliers
  - Payments to bogus vendors for false claims
  - Cheques written for cash only or not property authorised
  - Purchase of goods for private use

- Social Engineering
- Application fraud
- Identity theft
- Facility takeover fraud

4. Controls to mitigate the risks

PAYPORT UK has implemented the following controls, which will mitigate the risks identified in section 3.

4.1 Controls for Internal Fraud

PAYPORT UK has implemented the following controls:

PAYPORT UK has clear policies that cover:

- Serving or processing transactions for family and friends
- Personal purchases/transactions
- Personal use of equipment such as telephones, laptop computers, etc
- Authorised delegations

Have clear transaction procedures, including:

- Daily banking – by two people at all times
- Dual signatures on cheques
- Provision of receipts and acknowledgment of transactions
- Segregated purchasing, receipting and paying

PAYPORT UK provides strong, consistent supervision of staff: monitoring delegations, supervising employee compliance with procedures, challenge suspicious or unusual transactions.

PAYPORT UK maintains security of information: limiting access to confidential information, enforcing the use of employee ID, regularly changing passwords for computers, alarms etc, reviewing and investigating all security violations, cancelling access promptly when people transfer or leave.

PAYPORT UK has established strong human resource management procedures: undertaking pre-employment screening, implementing equitable remuneration system, providing adequate training and education and communicating policies, expectation of compliance, audit regime and consequences of non-compliance.

PAYPORT UK has specific and multi-layered on-boarding policy and procedure in place.

Regular training and awareness courses are being run to educate staff on fraud, bribery, money laundering and financial crime.

4.2 Specific Policies to implement the controls

The following policies have been implemented by PAYPORT UK, which will enable these controls to be implemented:

- Anti-Bribery Policy
- Anti-Fraud Policy
- Financial Crime Policy and Procedure
- HR on-boarding policy
- IT InfoSecurity Policy
- Data and Privacy Policy

4.3 Controls for External Fraud

PAYPORT UK has implemented the following controls in relation to the external fraud risks

- Fraud by suppliers can be prevented by:
    - Ensuring staff are appropriately trained in accounts payable and stores functions
    - Ensure that supervision occurs over processing receipts and payments for expenditure
    - Ensure that purchasing, receipting and payment functions are segregated so that no single person performs all three duties
    - Ensuring there are guidelines for relationships between your business members and suppliers to avoid bias and inducements from suppliers (gifts)
    - Ensuring audits are conducted on all areas of purchasing including:
        - petty cash, non-receipted items and all invoices

- PAYPORT has deployed an appropriate transaction filtering and monitoring systems in place and we use customer profiling (based on risk scores) to detect suspicious payment transactions
- PAYPORT UK has implemented awareness raising campaigns for staff, contractors, introducing brokers and staff.
- PAYPORT UK IT department has implemented the following technical measures:

    - Sender Policy Framework
    - DomainKeys Identified Mail
    - Domain-based Message Authentication, Reporting and Conformance

4.4 Specific Policies to implement the controls

The following policies have been implemented by PAYPORT UK, which will enable these controls to be implemented:

- Anti-Bribery Policy
- Anti-Fraud Policy
- Financial Crime Policy and Procedure
- HR Screening policy
- IT InfoSecurity Policy
- Data and Privacy Policy

5. Issue Monitoring and Resolution

The controls outlined in this policy have been designed to prevent a fraud related issue from occurring. Where an issue does occur, details of how it will be monitored and resolved are outlined in the Financial Crime Policy and Procedure.

6. Compliance Monitoring

This policy will be monitored through the compliance monitoring plan.

PAYPORT UK

Appendix 1
PAYPORT UK Risk Assessment

Factor	Area	Details of focal point	Risks	Controls	Policy	Monitor
Fraud	Internal Fraud	Employees Introducing Brokers	Falsification of records Forging of signatures Involvement with bribes Breaches of anti-money laundering procedures Any financial crime Misleading representations	PAYPORT UK has clear policies that cover: • Serving or processing transactions for family and friends • Personal purchases/transactions • Personal use of equipment such as telephones, laptop computers, etc. • Authorised delegations Have clear transaction procedures, including: • Daily banking – by two people at all times • Dual signatures on cheques • Provision of receipts and acknowledgment of transactions • Segregated purchasing, receipting and paying PAYPORT UK provides strong, consistent supervision of staff: monitoring delegations, supervising employee compliance with procedures, challenge suspicious or unusual transactions. PAYPORT UK maintains security	Anti-Bribery Policy Anti-Fraud Policy Financial Crime Policy and Procedure HR Screening policy IT InfoSecurity Policy Data and Privacy Policy	PAYPORT UK has a regular review and monitoring of our register of assets and your transactions: • Record all transactions • Keep a register of your tools, equipment and assets • engraved all our business property with an identifying number PAYPORT UK has established strong audit procedures: • Reconcile bank deposits with register totals regularly • Audit our IT systems regularly • Conduct regular and random audits of all processes • Randomly check wages and allowances for overpayments

				of information: limiting access to confidential information, enforcing the use of employee ID, regularly changing passwords for computers, alarms etc, reviewing and investigating all security violations, cancelling access promptly when people transfer or leave. PAYPORT UK has established strong human resource management procedures: undertaking pre-employment screening, implementing equitable remuneration system, providing adequate training and education and communicating policies, expectation of compliance, audit regime and consequences of non-compliance.		
	Internal Fraud	Employees	Improper verification of KYC information during account registration	PAYPORT UK has specific and multi-layered on-boarding policy and procedure in place. Regular training and awareness courses are being run to educate staff on fraud, bribery, money laundering and financial crime.	Anti-Bribery Policy Anti-Fraud Policy Financial Crime Policy and Procedure	Transaction monitoring Client on-boarding verification Internal Audit External Audit by Compliance Consultants specialist in Electronic Money and Payment Services
	External Fraud	Contractors Introducing Brokers	External fraud by suppliers includes:	Fraud by suppliers can be prevented by: • Ensuring staff are appropriately trained in accounts payable and stores functions • Ensure that supervision occurs over processing receipts and payments for expenditure • Ensure that purchasing, receipting and	Anti-Bribery Policy Anti-Fraud Policy Financial Crime Policy and Procedure HR Screening policy IT InfoSecurity Policy Data and Privacy Policy	Regular Audit of our suppliers, contractors and Introducing Brokers Transaction monitoring of all payments performed Internal Audit External Audit by Compliance

			• Payment for services and goods not supplied • Kickbacks for biased selection of suppliers • Payments to bogus vendors for false claims • Cheques written for cash only or not property authorised • Purchase of goods for private use	payment functions are segregated so that no single person performs all three duties • Ensuring there are guidelines for relationships between your business members and suppliers to avoid bias and inducements from suppliers (gifts) • Ensuring audits are conducted on all areas of purchasing including petty cash, non-receipted items and all invoices		Consultants specialist in Electronic Money and Payment Services
	External Fraud	Outside parties	Social Engineering Application fraud Identity theft Facility takeover fraud	PAYPORT UK has deployed an appropriate transaction filtering and monitoring systems in place and we use customer profiling (based on risk scores) to detect suspicious payment transactions PAYPORT UK has implemented awareness raising campaigns for staff, contractors, introducing brokers and staff.	Anti-Bribery Policy Anti-Fraud Policy Financial Crime Policy and Procedure HR on-boarding policy IT InfoSecurity Policy Data and Privacy Policy	Exchange of information within industry Regular training for Senior Management on External Fraud Strong InfoSecurity focus within IT department Regular Penetration and Social Engineering testing of

				PAYPORT UK IT department has implemented the following technical measures: Sender Policy Framework DomainKeys Identified Mail Domain-based Message Authentication, Reporting and Conformance		infrastructure and procedures Internal Audit External Audit by Compliance Consultants specialist in Electronic Money and Payment Services