POL00447947

GROUP POLICY

Financial Crime

Version – V8.0

Chief Executive's Endorsement

The Post Office Group is committed to doing things correctly. Our Values and Behaviours represent the conduct we expect. This policy supports these to help us ensure the highest standards of financial crime prevention, detection and management are maintained.

POL00447947

Contents

POL00447947

1. Overview

1.1. Introduction by the Policy Owner

The General Counsel has overall accountability to the Board of Directors for the design and implementation of controls to prevent or deter financial crime. Financial crime is covered within the Compliance agenda item for the Audit and Risk Committees and the Post Office Board is updated as required.

1.2. Purpose

This Policy has been established to set the minimum operating standards relating to the design and implementation of controls to prevent or deter financial crime throughout the Group[1].

It is one of a set of policies which provide a clear risk and governance framework and an effective system of internal control for the mitigation of risk across the Group. Compliance with these policies supports the Group in meeting its business objectives and to balance the needs of shareholders, staff[2] and other stakeholders.

1.3. Core Principles

The governance arrangements described in this Policy are based upon the following core principles:

- The interests of stakeholders are protected by ensuring that excessive powers are not delegated to individuals;
- Decisions taken by management are consistent with the Group's strategic objectives and Risk Appetite, which are approved by the Board;
- Appropriate conduct is demonstrated in executing the requirements contained within the Policy;
- Every member of staff is responsible for understanding and managing the risk they take on behalf of the Group;
- Clear accountabilities are delegated by management to people who have the right level of skill, competency and experience;
- All staff are required to comply with Group Policies.

1.4. Application

This Policy is applicable to all areas within the Group and defines the minimum standards to control financial loss, customer impact, regulatory breaches and reputational damage in line with the Group's Risk Appetite.

In exceptional circumstances, where risk sits outside of the Group's accepted Risk Appetite a Risk Exception can be granted.

Further information in relation to the risk exception process, together with a template can be found here.

---

[1] In this Policy "Post Office" and "Group" mean Post Office Limited and any wholly owned subsidiary that formally adopts this policy

[2] In this policy "employee" and "staff" means all persons working for the Group or on our behalf in any capacity including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, interns, and contractors.

POL00447947

While Post Office does not tolerate events that are criminal in nature and which may give rise to unacceptable and illegal behaviour, it recognises that despite its many endeavours, it is not possible to eliminate all risk of internal and external financial crime and as a result Post Office may incur losses, and therefore takes a risk based approach to financial crime.

Failure to comply with the requirements of this policy by any member of staff[2] will be regarded as a significant breach impacting on the Group's risk and control environment and may lead to disciplinary action up to and including dismissal and possible prosecution.

The risk to the Group in relation to financial crime is reviewed annually and as required by the Board.

1.5. Legislation

"Financial crime" is any offence involving: fraud or dishonesty, misconduct in, or misuse of information or handling the proceeds of crime. It can be internal (by individuals within an organisation) or external (by criminals using an organisation to facilitate financial crime). Financial crime is commonly considered as including one or a combination of the following offences:

- Fraud
- Cyber crime
- Money laundering
- Terrorist financing
- Bribery and corruption
- Tax evasion facilitation
- Information security breaches

There are a number of relevant UK legal and regulatory requirements which deal with financial crime including (but not limited to):

- The Fraud Act 2006
- The Bribery Act 2010
- The Theft Act 1968
- Common Law Offences of Fraud in Scotland
- The Proceeds of Crime Act 2002
- The Criminal Finances Act 2017
- Policing and Crime Act 2017
- The Terrorism Act 2000
- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (known as Money Laundering Regulations 2017) (as amended by the Money Laundering and Terrorist Financing (Amendment) Regulation 2019 and Money Laundering and Terrorist Financing (Amendment) (EU Exit) Regulations 2020)
- Forgery and Counterfeiting Act 1981
- Sanctions and Anti Money Laundering Act 2018
- Identity Documents Act 2010
- Economic Crime (Transparency and Enforcement) Act 2022

The Group has regard for guidance and other assistance offered by regulatory, industry and other specialist bodies, for example UK Finance (which incorporates BBA, UK Payments and Financial Fraud Action UL), and Link, etc., which publish trends and analysis on current threats and issues.

POL00447947

1.6. The Risk

Failure to manage financial crime risks and incidents appropriately could result in financial loss, customer impact, regulatory breaches, fines, prosecution, prevention from selling a particular product, loss of existing or future contracts/relationships and damage to reputation.

These risks include, but are not limited to, the following:

External Financial Crime:
The risk of external events due to acts of a type intended to defraud, steal or misappropriate assets/ property, or which seek to circumvent the law, by a third party. Examples would include:

- Any dishonest or fraudulent act,
- Theft of assets from an organisation or its customers,
- Card or account abuse or account takeover by a third party,
- Counterfeit payment instruments (cards, cheques, etc.) and identity documents,
- ATM fraud and theft,
- Online or mobile fraud,
- Facilitating money laundering
- Cyber crime, and
- Social engineering fraud.

Internal Financial Crime
The risk of internal events due to acts of a type intended to defraud, steal or misappropriate assets/property, or which seek to circumvent regulations or the law applicable to an organisation or its contracts or internal policies or procedures. Examples would include:

- Any dishonest or fraudulent act circumventing regulations or law,
- Profiteering as a result of insider knowledge of an organisation's activities,
- Theft of assets from an organisation or its customers,
- Manipulation of transactional data at point of sale,
- False expense or payroll claims,
- Manipulation of accounts or financial statements, and
- Breach of internal processes or controls for personal gain.

The Group takes the above internal risks and financial crime seriously and will take appropriate action against any person including disciplinary, dismissal and possible prosecution of anyone involved in such events.

POL00447947

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

Risk Appetite is the extent to which Post Office will accept that a risk might happen in pursuit of day to day businesses transactions. It therefore defines the boundaries of activity and levels of exposure that Post Office are willing and able to tolerate.

The risk tolerance level will be varied against each business unit. Information should be sought from the Central Risk Team with regards to the agreed appetite relevant to the policy being written.

Post Office have a five scale approach to risk appetite, Averse, Cautious, Neutral, Flexible and Open. The Group takes its legal and regulatory responsibilities seriously and consequently has[3]:

An averse appetite to being non-compliant with our Statutory & Regulatory requirements.

Post Office acknowledges however that in certain scenarios even after extensive controls have been implemented a product or transaction may still sit outside the agreed Risk Appetite. In this situation, a risk exception waiver will be required. (See section 1.4 for further details)

2.2. Policy Framework

Post Office has established a suite of Financial Crime policies and procedures, on a risk sensitive approach, which are subject to annual review. The policy suite is designed to combat money laundering, terrorist financing, bribery and corruption and fraud and ensure adherence to relevant sanctions regimes. They have been developed to comply with applicable legislation and regulation and cover the following specifically:

- The identification through documented risk assessment of potential or inherent and residual financial crime risks and the effectiveness of controls associated with them,
- Completing compliance oversight monitoring to test the Group's controls and confirm effectiveness and adherence to financial crime policies,
- On a risk sensitive basis, performing due diligence on our employees, agents and third parties,
- Where the Group has primary or contractual responsibility for the customer relationship ensuring Customer Due Diligence, Enhanced Due Diligence and Sanctions checking are set at any appropriate level commensurate with the risk,
- Establishing and maintaining standards for Management Information on financial crime. This includes, but is not limited to, record keeping, customer identity documents, reporting of suspicious activity[4] and details of staff training.

This policy provides an overview of the financial crime risk and governance framework and the effective system of internal control for the mitigation of financial crime risk required across the Group. The Key Financial Crime policies covering the major risk areas to the Group include:

- Anti-Bribery and Corruption Policy
- Anti-Money Laundering and Counter Terrorist Finance Policy
- HMRC Fit & Proper Policy
- Whistleblowing Policy

[3] The Risk appetite was agreed by the ARC March 2021

[4] For more information in relation to the completion and submission of a Suspicious Activity Report please see the Anti -Money Laundering and Counter Terrorism Policy.

POL00447947

- Financial Crime Policy

Associated Policies and Processes include:

- Acceptable Use Policy
- Protecting Personal Data Policy
- Cyber & Information Security Policy
- Investigations Policy

Each of the above policies should be considered and read in conjunction with any other policy where relevant. These policies are supported by the Risk Exceptions process.

2.3. Who must comply?

Compliance with this Policy is mandatory for all Post Office employees and applies wherever in the world the Groups business is undertaken. All third parties who do business with the Group, including consultants, suppliers and business and franchise partners, will be required to agree contractually to this policy or to have their own equivalent Policy. Where non-compliance is identified the matter must be referred to the Policy Owner. Any investigations will be carried out in accordance with the Investigations Policy. Where it is identified that an instance of non-compliance is caused through wilful disregard or negligence, this will be treated as a disciplinary offence.

All Post Office employees are required to report any knowledge or suspicions (internal or external) in relation to financial crime please see 3.2 and a failure to do so may amount to a disciplinary offence.

POL00447947

2.4. Minimum Control Standards

A minimum control standard is an activity which must be in place in order to manage the risks, so they remain within the defined Risk Appetite statements. There must be mechanisms in place within each business unit to demonstrate compliance. The minimum control standards can cover a range of control types, i.e. directive, detective, corrective and preventive which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

The table below sets out the relationships between identified risk and the required minimum control standards in consideration of the stated risk appetite. The subsequent pages define the terms used in greater detail:

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Proposed product or service	Products, services or relationships with third parties may rely on systems or processes where prevention or detection of financial crime has not been considered in the design, resulting in financial loss (whether to the Group, its customers or suppliers), reputational damage and/or regulatory sanctions.	Preventative Control: As part of the design of a new product or service: • A Product Information Pack (see 4.2 below) must be complete and be fully up to date. • Product or service risks must be considered and documented using the Financial Crime Engagement Tool (see 4.2 below) during initial engagement for Business Readiness Assurance at PROVE stage.	Product Managers	During design phase
		Prior to launch, the Product Information Pack (PIP) must be reviewed and approved by the Financial Crime Team. The Financial Crime Team adopts a risk-based approach to determine when the full risk assessment should be completed, and the PIP will provide them with key information to make an informed decision. If the product is deemed high risk, the assessment will be completed prior to launch, following which the Financial Crime Team may require the Product Manager to make changes to reduce the risks prior to launch.	Product Managers and Financial Crime Team	Prior to launch

POL00447947

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Proposed product or service (continued)		The product manager/management team is responsible for ensuring their product complies with legal and regulatory requirements in relation to financial crime.	Product Managers	Ongoing
Existing products and services	Due to changes in law, regulation, incidents, threats or practices over time, there is a risk that the controls to prevent and detect financial crime are no longer adequate.	Preventative Control: Risk assessments must be undertaken at least annually for high risk products and services, where any changes to the product or service (including supplier changes) are made, where an issue is highlighted, significant risk is identified, an incident occurs, or the regulations change.	Product Managers	Annually, or at any time there is a change
		The product manager/management team is responsible for ensuring their product complies with legal and regulatory requirements in relation to financial crime.	Product Managers	Ongoing
		Prior to the scheduled risk assessment, the Product Information Pack (PIP) must be reviewed and updated by Product Management and provided to the Financial Crime Team.	Product Managers	Ongoing
		Prior to any significant product or service changes being implemented, the Product Information Pack (PIP) must be reviewed and updated by Product Management. The Financial Crime Team adopts a risk-based approach to determine when the full risk assessment should be completed, and the PIP will provide them with key information to make an informed decision. If the product is deemed high risk, the assessment will be completed prior to change going live.	Product Managers	When there is a significant change, material issue or incident

POL00447947

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Existing products and services (continued)		Where no initial risk assessment was undertaken, product management must complete a new Product Information pack and provide this to the Financial Crime Team. The Financial Crime Team will then agree a timescale to complete a risk assessment.	Product Managers and Financial Crime Team	Any time there is a change
		Where the reassessed/assessed risk is considered by the Financial Crime Team to rest outside of the Group's Risk Appetite, or where the strength of the controls is deemed inadequate, as part of the Close Down report produced by the team, recommendations will be provided to the Product Manager to implement or improve controls to mitigate the risks. The Product Manager is responsible for recording all product risks on the GRC Tool and take appropriate actions to mitigate the risks as per the Group Risk Policy. Where risks cannot be sufficiently mitigated in line with the Group's risk appetite then then the risk exception process must be followed.	Financial Crime Team and Product Managers	Annually or when there is a material issue or incident
		Corrective Control: Product Management must implement escalation procedures for when an incident is identified, so that the Financial Crime Team are made aware, and if the product is outsourced to a third party, the third party is made aware. Product Management are responsible for addressing and overseeing any control failings to mitigate financial crime risks.	Product Managers	As and when an incident is identified
		A risk assessment may be undertaken where an issue is highlighted by monitoring or an incident occurs that is deemed to be systemic.	Financial Crime Team and Product Managers	As and when an incident is identified

POL00447947

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Human Resources	Due to inadequate screening, there is a risk that the Group employs individuals who do not have the legal right to work in the UK or are unfit to undertake the role.	Preventative Control: To minimise the risk of financial crime by employees, Post Office completes employee screening prior to employment. In addition to this, on a regular basis (proportionate to the role) additional checks will be completed to ensure that there is no risk of internal collusion by any of our employees. For further information please see the employee vetting policy.	Group Chief People Officer	Pre-employment and ongoing where required
Operations	Inadequate training, monitoring and control of internal processes and systems may lead to internal fraud or theft by employees	Directive Control: Post Office has developed a Code of Business Standards and model behaviours that set out the expected standards for all employees and contractors – this is made available to all new and existing staff and reinforced in communications Preventative Control: Access to Post Office systems is via unique user log-ins and annual mandatory compliance training is provided to all staff and contractors. Post Office expenses and payroll systems include management checks and controls. Detective Control: Audit trails for system access are maintained and monitored appropriately	Group Chief People Officer All Employees Chief Information Officer The People Function are responsible for any incidents where further action is required and ensuring completion of mandatory training Internal Audit	Ongoing Ongoing system design and delivery Pre-employment and ongoing where required Ongoing

POL00447947

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Operations	Inadequate building and systems access controls may lead to financial crime that results in financial loss (whether to the Group, its customers or suppliers), reputational damage and/or regulatory sanctions.	Preventative Controls: Relevant business areas including the property and security teams must assess and assure risks relating to employee and customer access to sites, secured areas, systems and software, recommending and implementing additional controls where appropriate. All business areas are responsible for maintaining documented processes and procedures and deploying adequate monitoring and controls to prevent and detect unauthorised access to sites, secured areas, systems and software to prevent financial crime. Detective Control: Audit trails must be maintained so that building, and system access can be monitored. To ensure that the Group's controls remain effective the Group undertakes internal audits to test and assess their effectiveness.	Head of Property Equipment and Security All employees Chief Information Officer and Head of Property Equipment and Security Internal Audit	Ongoing Ongoing Ongoing Ongoing
Financial settlement and reconciliation	Inadequate controls and audit trails relating to financial settlement and reconciliation may result in financial loss (whether to the Group, its customers or suppliers), reputational damage and/or regulatory sanctions.	Preventative Controls: Relevant business areas must assess and assure risks relating to financial settlement and reconciliation and are responsible for maintaining documented processes and procedures and deploying adequate monitoring and control to prevent and detect financial crime. Detective Control: Audit trails must be maintained so that system access can be monitored.	Chief Financial Officer Chief Information Officer	Ongoing Ongoing

POL00447947

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		To ensure that the Group's controls remain effective the Group undertakes internal audits to test and assess their effectiveness.	Internal Audit	Ongoing
Financial settlement and reconciliation	Inadequate controls and audit trails relating to financial settlement and reconciliation may result in financial loss (whether to the Group, its customers or suppliers), reputational damage and/or regulatory sanctions.	Preventative Controls: Relevant business areas must assess and assure risks relating to financial settlement and reconciliation and are responsible for maintaining documented processes and procedures and deploying adequate monitoring and control to prevent and detect financial crime. Detective Control: Audit trails must be maintained so that system access can be monitored. To ensure that the Group's controls remain effective the Group undertakes internal audits to test and assess their effectiveness.	Chief Financial Officer Chief Information Officer Internal Audit	Ongoing Ongoing Ongoing
Criminal facilitation of tax evasion	Inadequate controls lead to Post Office failing to prevent criminal facilitation, by its associated persons (which includes employees, agents, clients, suppliers, contractors, etc.), of a UK or foreign criminal tax evasion	Preventative controls: Post Office ensures that guidance is issued to agents that they must not facilitate tax evasion by any company or person. Agents are expected to have in place reasonable prevention procedures to avoid breaching the Criminal Finances Act 2017 and Post Office's obligations and relevant clauses are included in all supplier contracts. Post Office has a Group wide training programme to ensure that all customer facing staff, back office staff and contractors receive adequate training. Staff and contractors are required to complete mandatory compliance training within 30 days of joining Post Office and annually.	Group Tax and Head of Postmaster Remuneration Development The People Function are responsible for any incidents where further action is required and ensuring completion of mandatory training	Ongoing Ongoing
Criminal facilitation of		Detective Controls:		Ongoing

POL00447947

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
tax evasion (continued)		Pass rate and number of failures of specific test questions is monitored to identify risk areas, any additional training or guidance required or those areas of training that need to be enhanced.	Financial Crime Team is responsible for reviewing training effectiveness	
Internal Financial Crime/Fraud	Controls to deter, prevent and detect financial crime and fraud are not adequate to prevent crime by employees	Directive Control: Post Office has developed a Code of Business Standards and model behaviours that set out the expected standards for all employees and contractors – this is made available to all new and existing staff and reinforced in communications. Staff are also encouraged to report suspicions or actual wrong-doing to Grapevine or via the Whistleblowing reporting avenues. Detective Controls: All reports received of or instances identified of internal fraud will be fully investigated and where appropriate, Post Office will prosecute individuals.	Group Chief People Officer Head of Internal Audit and General Counsel	Ongoing Ongoing

POL00447947

3. Where to go for help

3.1. Additional Policies

This Policy is one of a set of policies. The full set of policies can be found on the SharePoint Hub under Policies.

3.2. How to raise a concern

Any Post Office employee who suspects that Post Offices products, services or processes have been used to facilitate money laundering, terrorist financing, or dishonest or fraudulent activity has a duty to raise a Suspicious Activity Report by calling Grapevine on GRO

Any Post Office employee who suspects that there is a breach in this Policy should report this without any undue delay, staff may:

- Their line manager, or
- A senior member of the HR Team, or
- Direct to the Whistleblowing Manager (whistleblowing GRO), or
- Contacting the "Speak Up" line, a confidential reporting service which is run by an independent company Convercent:
  - Telephone Number: GRO
  - http://speakup.postoffice.co.uk/ which is a secure on-line web portal

3.3. Who to contact for more information

If you need further information about this policy or wish to report an issue in relation to this policy, please contact financial.crime GRO

POL00447947

4. Governance

4.1. Governance Responsibilities

The policy sponsor, responsible for overseeing this policy is the General Counsel of Post Office Limited.

The policy owner is the Director of Compliance who is responsible for ensuring that the Financial Crime Team conducts an annual review of this policy and tests compliance across the Group. Additionally, the Director of Compliance and the Financial Crime Team are responsible for providing appropriate and timely reporting to the Risk and Compliance Committee and the Audit and Risk Committee.

The Audit and Risk Committee are responsible for approving the policy and overseeing compliance.

The Board is responsible for setting the groups risk appetite.

4.2. Tools

The Financial Crime Engagement Tool
The Financial Crime Engagement Tool has been created by the Financial Crime Team and enables Product Managers to provide the Financial Crime Team with key details about their project so that the team have an understanding of the financial crime risks posed and support the Product Manager with their project. The Compliance Engagement Tool takes into account inherent risks (e.g. payment method, channel, customer demographic etc.), UK regulations and legislation and industry best practice, enabling the Financial Crime Team to ensure that appropriate controls and product features are in place to mitigate the inherent risks and meet regulatory and legal requirements

The Financial Crime Engagement Tool can be found here.

Product Information Pack
Product Management are responsible for keeping the Product Information Pack (PIP) up to date in line with any product changes. The purpose of the PIP is to provide an overview of the product or service, including customer/transactional journey, parties involved, any contractual responsibilities, monitoring and control requirements. It should consider the inherent risks the product is exposed to from a Group and customer perspective and the framework for the effective risk mitigation of the product.

The existence of detailed operating policies, procedures and processes may be referred to throughout this document and is to be used to illustrate how the risks associated with the product are reduced.

The Product Information Pack can be found here.

Financial Crime Risk Assessment
The Financial Crime Team will conduct a risk assessment using the information provided by the Product Manager within the PIP. The team will issue a final report to the Product Team highlighting all the financial crime risks identified and recommendations on how to improve the controls in place. The Product Manager is responsible for recording all product risks on the GRC Tool and take appropriate actions to mitigate the risks as per the Group Risk Policy.

More information on the Financial Crime Risk Assessment can be found here.

POL00447947

5. Document Control

5.1. Document Control Record

SUMMARY			
GE Policy Sponsor	Policy Owner	Policy Author	Policy Approver
Group General Counsel	Group Compliance Director	Head of Financial Crime	RCC & ARC
Version	Document Review Period	Policy – effective date	Policy location
8..0	Annually	July 2023	Sharepoint Hub

REVISION HISTORY			
Version	Date	Changes	Updated by
1	November 2016	Roll out of Final version	Georgina Blair
1.3	July 2017	Final draft	Thomas Richmond
1.4	July 2017	POL R&CC approval	Sally Smith
2	September 2017	Final Version approved by ARC	Sally Smith
2.1	October 2018	Annual review and amends	Sally Smith
2.2	October 2018	POL R&CC approval	Sally Smith
2.3	October 2018	POL ARC approval	Sally Smith
2.4	December 2018	POMS ARC Approval	Thomas Richmond
3	December 2018	Final draft	Thomas Richmond
3.1	September 2019	Annual review and amends	Sally Smith
3.2	September 2019	POL R&CC approval	Sally Smith
4.0	September 2019	Final version approved by ARC's	Sally Smith
4.1	April 2020	Updated with new Speak Up service contact details	Sally Smith
4.2	June 2020	Annual review and amends	Sally Smith
4.3	July 2020	POL RCC approval	Sally Smith
5.0	July 2020	Final version approved by ARC's	Sally Smith
5.1	June 2021	Annual Revisions and Legal Review	Sally Smith/Sarah Gray
5.2	July 2021	RCC Approved	Sally Smith
6.0	July 2021	Final version approved by ARC's	Sally Smith
6.1	June 2022	Transfer to new template and annual revisions	Sally Smith
6.2	June 2022	RCC approval	Sally Smith
7.0	Oct 2022	Final version approved by ARC's	Sally Smith
7.1	June 2023	Annual Revisions and Legal Review; new legislative addition and new company registered address	Sally Smith/Jane Beeko
7.2	June 2023	POL RCC approval	Sally Smith
8.0	July 2023	Final version approved by POL and POMS ARC	Sally Smith

POL00447947

5.2. Oversight Committee: Risk and Compliance Committee / Audit and Risk Committee

Committee	Date Approved
POL R&CC	27th June 2023
POL ARC	10th July 2023
POMS ARC	10th July 2023

Next Policy Annual Review Date: July 2024

5.3. Company Details

Post Office Limited and Post Office Management Services Limited are registered in England and Wales. Registered numbers 2154540 and 08459718 respectively. Registered Office: 3rd Floor, 100 Wood Street, London EC2V 7ER.

Post Office Management Services Limited is authorised and regulated by the Financial Conduct Authority (FCA), FRN 630318. Its Information Commissioners Office registration number is ZA090585.

Post Office Limited is authorised and regulated by Her Majesty's Revenue and Customs (HMRC), REF 12137104. Its Information Commissioners Office registration number is Z4866081.

Payzone Bill Payment Limited is a limited company registered in England and Wales under company number: 11310918. VAT registration number GB 172 6705 02. Registered office: 3rd Floor, 100 Wood Street, London EC2V 7ER