Financial crime Policy

Contents

Phillips Capital Group
97 Baltic Quay, Mill Road, Gateshead NE8 3QX
T: 0800 061 4649 | **E:** ask@phillipscapital.info | **W:** phillipscapitalgroup.co.uk

1. Purpose

The Purpose of the Policy

The purpose of this policy is to provide a consistent, coherent, and proportionate approach to deterring, detecting, preventing, and reporting all types of 'financial crime' across PCG, relative to PCG's risk profile. PCG is subject to significant financial crime regulation, and this policy is designed to ensure compliance with UK legislation, regulations, rules, and industry guidance for the financial services industry, as enforced by the Financial Conduct Authority (FCA). This helps protect colleagues, customers, and the sector from the impacts of financial crime.

Applicable Regulations and Legislation

PCG is authorised and regulated by the Financial Conduct Authority (FCA). PCG has a duty to comply with prevailing UK legal and regulatory requirements relating to Anti-Money Laundering (AML); Counter Terrorist Financing (CTF); Financial Sanctions; Fraud; Tax Evasion; Anti-Bribery & Corruption (ABC); Modern Slavery; and Human Trafficking. The applicable UK laws and regulations include:

- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (Money Laundering Regulations 2017), as amended by:
    - Money Laundering and Terrorist Financing (Amendment) Regulations 2019 (MLR's)
    - The Money Laundering and Terrorist Financing (Amendment) (EU Exit) Regulations 2020
    - The Money Laundering and Terrorist Financing (Amendment) (High-Risk Countries) Regulations 2021
    - The Money Laundering and Terrorist Financing (Amendment) Regulations 2022
- The Proceeds of Crime Act 2002 (POCA), as amended by:
    - Serious Organised Crime and Police Act 2005 (SOCPA)
    - Proceeds of Crime Act (Amendment) Regulations 2007
- The Terrorism Act 2000, as amended by:
    - The Anti-Terrorism, Crime & Security Act 2001
    - Terrorism Act (Amendment) Regulations 2007
- The Terrorism Act 2006
- Counter Terrorism Act 2008
- Terrorist Asset-Freezing Act 2010
- The Modern Slavery Act 2015
- The Fraud Act 2006
- The UK Bribery Act 2010

- The Policing and Crime Act 2017
- The FCA Handbook of Rules and Guidance, particularly the Senior Management Arrangements, Systems and Controls (SYSC) Sourcebook

Additional industry standards and guidance observed by PCG include:

- The Joint Money Laundering Steering Group (JMLSG) Guidance for the UK Financial Sector on the prevention of money laundering/combating terrorist financing
- The FCA Financial Crime Guide

Requirements of the Policy

All persons in scope of this policy are required to adhere to its contents to enable a high standard of financial crime prevention and awareness across PCG.

2. Scope

This policy applies to:

- PCG (including all legal entities/subsidiaries operating in the UK)
- All individuals working within or for PCG in the UK, including permanent and temporary colleagues, Non-Executive Directors, contingent workers (consultants, contractors, third-party agents, and their employees), together with any other associated persons or third parties
- All businesses and operations of PCG in the UK
- Collaborative activities with third-party organisations in the UK

Where PCG holds a supplier relationship with a third party in the UK and it is appropriate for the supplier to adhere to this policy, provisions should be included within their contracts to reflect this.

3. Definitions

For the purposes of this policy, 'financial crime' includes Money Laundering; Terrorist Financing; Financial Sanctions; Fraud (internal and external); Tax Evasion or the Facilitation of Tax Evasion; Bribery; Corruption; Modern Slavery; and Human Trafficking.

- Money Laundering: The techniques, procedures, or processes used to convert illegal funds obtained from criminal activities into assets and to conceal their true origin so that it appears the money comes from a legitimate or lawful source.
- Terrorist Financing: The process of raising, storing, and moving funds for the purpose of directly committing terrorist acts and/or sustaining a terrorist organisation.
- Financial Sanctions: Restrictions that the UK government imposes on certain types of transactions with targeted entities or individuals to achieve national security or policy goals.
- Fraud (internal and external): Any wilful act or omission whereby a person's conduct is dishonest, and their intention is to make a gain or cause a loss or the risk of a loss to another.

- Tax Evasion or the Facilitation of Tax Evasion: An offence of cheating the public revenue or an offence under UK law consisting of being knowingly concerned in, or taking steps with a view to, the fraudulent evasion of a tax. The facilitation of tax evasion occurs where PCG fails to prevent the organisation from being used by associated persons to commit tax evasion.
- Bribery: A means of giving or receiving an unearned reward to influence an individual's behaviour by either providing or receiving favourable treatment.
- Corruption: Any unlawful or improper behaviour that seeks to gain an advantage by way of unethical, unlawful, or illegitimate actions.
- Modern Slavery: Crimes associated with holding a person in a position of slavery, servitude, forced, or compulsory labour.
- Human Trafficking: Arranging or facilitating the travel of another person with a view to their exploitation.

4. Policy Statements

PCG's Board and Senior Management are committed to minimising the risk of PCG being used to facilitate financial crime through the application of risk-based internal policies, procedures, systems, and controls to effectively deter, detect, prevent, and report instances of financial crime in the UK. We strive to ensure that high standards of financial crime prevention and awareness are maintained across PCG. PCG will adhere to all UK laws and FCA regulations applicable to our business activities, and we expect our customers and third parties in the UK with whom we have working relationships to adhere to the same standards.

4.1 Risk Appetite

PCG, like all UK financial institutions, is exposed to some degree of financial crime risk as part of its day-to-day operations. Our risk appetite towards financial crime helps achieve our commercial objectives whilst mitigating financial crime risk through the effective implementation of financial crime controls.

PCG has an extremely low tolerance for financial crime and is committed to fulfilling our lawful and regulatory obligations with respect to financial crime risk through a risk-based approach to deter, detect, prevent, and report money laundering; terrorist financing; bribery; corruption; the facilitation of tax evasion; modern slavery; and human trafficking.

PCG adopts a firm but flexible appetite against fraud to enable the business to continue to progress in a safe and controlled manner whilst providing customers with an appropriate customer experience, and as such actively takes steps to minimise our exposure to internal and external fraud and theft.

PCG has no appetite for unauthorised engagement with an individual or entity subject to financial sanctions and is committed to the application of a risk-based control framework that allows PCG to identify this risk at the point of onboarding or through the duration of a relationship. Should PCG inadvertently enter into or identify that it has entered into an unauthorised relationship with a person or entity subject to financial sanctions, then this relationship will be declined or terminated.

Relationships where the level of financial crime risk is outside of PCG's risk appetite will be declined or terminated.

4.2 Key Financial Crime Principles

PCG will:

a) Maintain an effective governance and control environment including:

- Undertaking reporting activities, including updates to committees and an annual MLRO report, to ensure senior management have a clear understanding of PCG's financial crime risk profile
- Articulating a risk appetite to ensure that residual risk is kept within defined and agreed levels
- Ensuring that the appropriate risk structure is implemented with effective controls in place at each level
- Appointing a suitably experienced MLRO with responsibility for independent oversight of PCG's systems and controls in combatting money laundering and terrorist financing, ensuring compliance with FCA SYSC rules
- Appointing a suitably experienced Nominated Officer (NO) with the responsibility for receiving, investigating, and reporting any suspicions of money laundering or terrorist financing to the National Crime Agency (NCA)
- Allocating overall responsibility for the firm's policies and procedures for countering the risk that the firm might be used to further financial crime and ensuring the establishment and maintenance of effective financial crime systems and controls to a Director/Senior Manager, including holding the FCA's Prescribed Responsibility 'D'

b) Comply with all applicable UK legal and regulatory requirements relating to financial crime prevention, including but not limited to the regulations/legislation, standards, and guidance listed in section 1.

c) Foster an environment where the deterrence, detection, prevention, and reporting of financial crime is paramount to all employees:

- Ensuring clear functional Senior Management accountability for implementation of the Financial Crime Policy, the underlying Business Standards, and any control weaknesses identified within their responsibilities
- Maintaining appropriate channels for raising concerns, including a helpline, internal reporting mechanisms, and a confidential whistleblowing process accessible by all employees
- Maintaining a strong ongoing anti-financial crime culture through all levels within PCG, with endorsement from and being led by PCG's Board, Executive Leadership Team, and senior managers

d) Support ongoing Risk Assessments and a Risk-Based Approach towards financial crime:

- Maintaining up-to-date risk assessments that are reflective of the latest UK legislative, regulatory, and industry position to measure financial crime risk across PCG's products and services, and the effectiveness of PCG's financial crime controls
- Maintaining this policy, appropriate standards, and response plans, including internal incident escalation processes. Continually looking forward to identify new emerging trends in financial crime risks, changes in UK legislation, regulations, and industry movement, and where necessary completing interim risk assessments to measure the financial crime risk across PCG, particularly in relation to customer, product, and activity profiles, distribution channels, complexity and volume of transactions, processes, systems, and the operating environment

- Documenting, reviewing annually, and applying a risk-based approach to the financial crime control framework
- Ensuring resources are focused towards high-risk areas through utilising a risk-based approach giving consideration to the following risk factors: customers (and their underlying beneficial owners); products/services; transactions; and delivery channels
- Ensuring the MLRO has access to sufficient resources to effectively discharge their regulatory obligations

e) Maintain effective controls to deter, detect, prevent, and report instances of money-laundering and terrorist financing including:

- Documenting AML/CTF standards and procedures for use throughout PCG
- Implementing a risk-based approach to due diligence at onboarding and periodically throughout the business relationship for all parties, including personal customers, commercial customers, suppliers, and colleagues. Considering Simplified Due Diligence (SDD) or reliance on regulated third parties where appropriate for low-risk relationships and Enhanced Due Diligence (EDD) for high-risk relationships (including PEPs) and transactions
- Maintaining appropriate due diligence records in line with regulatory requirements and PCG's data retention standards
- Implementing technology to enable employees to make appropriate decisions in respect of financial crime risks
- Adopting and maintaining a control framework whereby colleagues throughout PCG can identify where activity is not in line with the risk profile of the customer and report suspicions of money laundering or terrorist financing for further investigation by the Nominated Officer, or other persons where authority has been delegated
- Fulfilling legal and regulatory obligations in relation to timely disclosure of knowledge or suspicion of money laundering or terrorist financing activity through Suspicious Activity Reports (SARs) to the National Crime Agency (NCA), co-operating with their investigations, and maintaining confidentiality
- Ensuring appropriate controls are in place to protect the privacy and confidentiality of PCG's customer, colleague, and third-party data, adhering to relevant UK legislation, regulation, and guidance. Where a customer is subject to a financial crime investigation and requests access to their data, PCG's Data Subject Access Request (DSAR) process should be followed

f) Comply with all applicable UK financial sanctions legal and regulatory requirements:

- Conducting customer screening at onboarding and on a daily basis, including via usage of 'fuzzy logic matching' on a proportionate and risk-based approach to ensure that PCG does not directly or indirectly make available or deal with funds or economic resources belonging to, owned, held, or controlled by persons or entities subject to UK financial sanctions
- Ensuring PCG does not engage in actions that directly or indirectly circumvent UK financial sanctions prohibitions

- Conducting proportionate and risk-based screening of inbound and outbound payments to ensure that PCG does not directly or indirectly make available or deal with funds or economic resources belonging to, owned, held, or controlled by persons or entities subject to UK financial sanctions

- Reporting to the appropriate authorities (e.g., OFSI) and, where necessary, obtaining the relevant licences to cease business relationships where it is identified that a customer or transaction is connected to a sanctioned individual or entity

g) Comply with all applicable UK anti-bribery & corruption legal and regulatory requirements:

- Ensuring appropriate systems and controls are in place to identify and report conflicts of interest

- Ensuring appropriate systems and controls are in place to enable the recording of given or accepted gifts and hospitality, ensuring these are legal and appropriate and do not provide PCG or a third party with a commercial benefit

h) Implement anti-fraud systems and controls to ensure adherence to our Fraud Risk appetite and UK regulatory standards:

- Including obtaining and validating appropriate details to identify fraudulent applications and transactions for all product lines and to support responsible lending decisions

i) Undertake transaction monitoring to ensure PCG's control framework identifies and reports activity that is reflective of known financial crime-related typologies:

- Including using industry typologies and indicators to inform the operation of suspicious activity monitoring. Additional account-level transactional monitoring may also be required in certain circumstances

j) Have reasonable and proportionate controls in place to prevent the facilitation of tax evasion:

- Including adhering to guiding principles released by HM Revenue and Customs, having an effective risk assessment process to inform a risk-based application of controls, and ongoing staff training on key tax evasion typologies applicable to PCG's business model

k) Produce management information (MI) for Money Laundering, Terrorist Financing, Financial Sanctions, Fraud, Bribery, Corruption, Modern Slavery, Human Trafficking, and Tax Evasion threats, updating PCG's approach and control framework where appropriate to reduce the possibility of reoccurrence

l) Have reasonable and proportionate controls in place to detect, deter, prevent, and report instances of Human Trafficking and Modern Slavery:

- Adopting and maintaining an appropriate control framework for the identification and reporting of instances indicative of Human Trafficking or Modern Slavery

- Conducting due diligence on third-party vendors and within our business and supply chains in the UK to identify risks related to modern slavery and human trafficking

PCG, its colleagues, contingent workers, and Non-Executive Directors must not engage in any activity that might lead to a breach of this policy, including, but not limited to:

m) Failing to make an internal report, or in the case of the Nominated Officer, or other persons where authority has been delegated, a disclosure to NCA as soon as practicable, when they know or suspect that another person is engaged in money laundering or terrorist financing, or have reasonable grounds to know or suspect this

n) Knowingly entering into or becoming involved in an arrangement that conceals, disguises, converts, or transfers criminal property or terrorist funds

o) Engaging in business relationships (including opening and operating accounts or effecting payments) which involve any direct or indirect link with sanctioned persons or entities

p) Engaging in fraudulent activity against PCG, its customers, or any other party

q) Assisting other persons in activities intended to breach PCG's financial crime policy or related procedures

r) Tipping off a customer or third party who is the subject of a SAR that a disclosure has been made to a Nominated Officer or to the NCA, or that the police or customs authorities are carrying out or intending to carry out an investigation

s) Engaging directly or indirectly in activity that facilitates the fraudulent evasion of tax

t) Offering or accepting bribes, or becoming involved in any corrupt activities

u) Directly or indirectly engaging in activities that facilitate modern slavery or human trafficking

5. Implementation and Monitoring

Implementation

This policy is approved by the PCG Board, and in implementing this policy, the Board has delegated executive responsibility for risk management in respect of financial crime to several oversight committees across PCG.

The owner of this policy will ensure that the policy is implemented in practice and will inform the owners of other impacted policies where new or significant changes are made to this policy.

This policy and future changes will be communicated via internal communication channels, including PCG's internal intranet platform (accessible by all employees) and email communication to key stakeholders.

The owners of related policies must undertake the required review and any subsequent amendments to their own policies to ensure they are aligned with this policy.

The implementation of this policy will be supported through ongoing training, the associated business standards and procedures, and relevant systems and controls. The business standards will contain definitions of relevant terms found within this policy to aid with local procedural compliance. The governance framework, oversight activities, and the annual CBT test requirements will provide assurance that colleagues understand their responsibilities.

Monitoring

PCG operates a Three Lines of Defence (LoD) approach towards risk management. Each LoD has different responsibilities for managing the risk and therefore carries different actions:

- First LoD: Directly responsible for the day-to-day management and control of risk throughout the business, generally within business functions

- Second LoD: Accountable for competent risk management across PCG and overseeing the effectiveness and integrity of the Enterprise Risk Management Framework
- Third LoD: Provides independent assurance across the first and second LoD through our internal Audit function

Any non-compliance with this policy or breach of financial crime-related regulations must be discussed with the Director of Shared Services and Resilience as noted in the relevant business standards and, where appropriate, reported through the Regulatory Compliance Breach Incident (RCBI) process.

6. Approval

This policy will be reviewed and updated annually (or more frequently as necessary) to ensure ongoing relevance and compliance with UK regulatory or legislative changes and to reflect any lessons learned from both internal and external events.

This policy is classified as a Board policy. It is therefore subject to review and endorsement at Group Risk Committee and approval at the Board on an annual basis.

Appendix 1: Description of Roles, Responsibilities, and Authorities

The competence and/or performance of all colleagues will be monitored and recorded via appraisals and the maintenance of training and competency records.

Policy Owner

The Policy Owner is responsible for:

- Writing the policy document and ensuring that it always remains up to date
- Reviewing the policy periodically and in the event of any significant change (e.g., UK legislative, regulatory, organisational, operational, etc.)
- Seeking approval/re-approval from the Policy Sponsor and the relevant governance committee
- Communicating the policy to all affected colleagues, ensuring that adequate supporting training is developed and delivered as required
- Monitoring the application of the policy and escalating to the Policy Sponsor and Enterprise Risk Management Team any breach in policy
- Ensuring the relevant policy guides are aligned to the policy
- The Owner of this policy can delegate responsibility for the day-to-day management, implementation, and monitoring of compliance with the policy to the Director of Shared Services and Resilience

Risk Category Owner

The Risk Category Owner is responsible for:

- Assessing PCG's compliance with all aspects of the policy

- Ensuring any instance of non-compliance to the policy is escalated through the relevant governance channels
- Ensuring PCG assesses its financial crime risk profile and control effectiveness by undertaking enterprise-level risk assessments
- Updating PCG's Anti-Money Laundering/Counter Terrorist Financing, Fraud, Financial Sanctions, and Customer Due Diligence business standards documentation to reflect the contents of this policy
- Ensuring the associated business standards are communicated to PCG and adherence to the standards is monitored

Chief Risk Officer (Senior Manager/Director Accountability and FCA Prescribed Responsibility 'D' & Policy Sponsor)

The Chief Risk Officer is responsible for:

- Overall responsibility for PCG's policies and procedures for countering the risk that the firm might be used to further financial crime
- Ensuring the establishment and maintenance of effective financial crime systems and controls
- Ensuring PCG's compliance with The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (Money Laundering Regulations 2017), as amended by the Money Laundering and Terrorist Financing (Amendment) Regulations 2019; the Money Laundering and Terrorist Financing (Amendment) (EU Exit) Regulations 2020, the Money Laundering and Terrorist Financing (Amendment) (High-Risk Countries) Regulations 2021, and The Money Laundering and Terrorist Financing (Amendment) Regulations 2022
- Supervision and direct management of the MLRO, where these roles are held by separate persons

However, the MLRO responsibility has been delegated to the Director of Compliance, Money Laundering Reporting Officer & Data Protection Officer.

As Policy Sponsor, the Chief Risk Officer is responsible for:

- Providing direction to the Policy Owner as required
- Supporting the Policy Owner in discharging their responsibilities, specifically ensuring sufficient investment is made available to enable implementation and monitoring of policy adherence
- Endorsing the Policy prior to it being submitted to the relevant governance committee for approval

Money Laundering Reporting Officer (MLRO)

The MLRO is responsible for:

- Oversight of PCG's compliance with relevant UK legislation, FCA regulatory rules, and guidance in respect of AML/CTF, including the requirements of SYSC 6.3, the Money Laundering Regulations, and associated financial crime industry guidance

- Acting as PCG's focal point for all AML/CTF activities, supporting and coordinating senior management focus on managing the money laundering/terrorist financing risk across PCG
- Monitoring the day-to-day operation of PCG's AML/CTF policies, ensuring any identified weaknesses are appropriately escalated through the correct governance channels, including direct access to the Executive Leadership Team and Board, where appropriate. Acting autonomously, if necessary, without reference to or undue influence from management
- Ensuring the effective and timely investigation of Suspicious Activity Reports (SARs) and, where necessary, ensuring the appropriate reports are made to law enforcement agencies by PCG's Nominated Officer
- Ensuring a full and rapid response to enquiries for information made by the FCA, law enforcement agencies, or other appropriate bodies

Nominated Officer

The Nominated Officer is responsible for:

- Receiving reports of suspicious activity from any employee in the business
- Considering all reports and evaluating whether there is - or seems to be - any suspicion of money laundering or terrorist financing
- Reporting any suspicious activity or transaction to the National Crime Agency (NCA) by completing and submitting a Suspicious Activity Report
- Liaising with the NCA for a defence to a money laundering offence (DaML) in relation to any reported transaction that has not been processed, to ensure the transaction does not continue to be processed where there is a suspicion of money laundering or terrorist financing facilitation

Operational Management

Operational Management is responsible for:

- Ensuring that the Policy is implemented in practice within their functional area
- Ensuring that colleagues within their functional area are appropriately trained
- Impacted Policy Owners must undertake the required review and any subsequent amendments to their own policies to ensure they are aligned with this policy

All Colleagues

All colleagues must adhere to the requirements and duties placed upon them by the policy, specifically including those outlined in section 4. Where necessary, those colleagues who are not management level but hold relevant responsibilities must ensure adherence to the clauses set out within the 'Operational Management' section.

Appendix 2: Glossary of Key Terms and Abbreviations

The following is a glossary of the key terms and abbreviations used in this policy:

- 1/2/3LOD: First / Second / Third Line of Defence

- ABC: Anti-Bribery & Corruption
- AML: Anti-Money Laundering
- Associated Persons: In the context of the facilitation of tax evasion, an associated person includes anyone who provides services for or on behalf of PCG, such as contractors, agents, or employees
- Breach: Failure to adhere to one or more mandatory Policy or Standards requirements where prior consent has not been obtained from the policy owner
- Business Relationship: Any service or product PCG provides/enters into with a new or existing customer, be it a one-off transaction or ongoing relationship
- CBT: Computer Based Training – annual mandatory financial crime training for all employees
- CTF: Counter Terrorist Financing
- Colleagues: PCG employees (permanent and temporary)
- Contingent Workers: Individuals who work for or with PCG through either their own Limited Company, a third-party company, or employed by a PCG agency. This category of worker is often referred to as either a contractor or a consultant
- EDD: Enhanced Due Diligence – measures that must be applied on a risk-sensitive basis in any situation which can present a higher risk of money laundering or terrorist financing, e.g., where a customer is identified as a PEP and additional information about that customer must be obtained
- FCA: Financial Conduct Authority
- FC: Financial Crime – for the purposes of this policy, financial crime includes AML/CTF, Sanctions, and Fraud
- High-Risk Customer: A customer who presents a higher level of money laundering or terrorist financing risk, e.g., customers with political connections
- HMT: Her Majesty's Treasury
- MI: Management Information
- MLRO: Money Laundering Reporting Officer
- Must: The use of 'must' in this policy conveys a mandatory requirement to be undertaken
- NCA: National Crime Agency – crime-fighting agency in the UK
- OFSI: The Office of Financial Sanctions Implementation, part of HM Treasury, which helps ensure that financial sanctions requirements are properly understood, implemented, and enforced in the United Kingdom
- PEP: Politically Exposed Person – an individual who is entrusted with prominent public functions, other than as a middle-ranking or more junior official. Such individuals can pose a higher money laundering risk as

their position may make them vulnerable to corruption. This risk also extends to members of their immediate families and to known close associates

- POCA: Proceeds of Crime Act 2002
- SAR: Suspicious Activity Report – a report to law enforcement agencies that a customer's activity is in some way suspicious and may indicate money laundering or terrorist financing
- SYSC: The FCA's Senior Management Arrangements, Systems and Controls Sourcebook
- Waiver: A formal approval for an exemption to the documented policy or procedure in place across PCG