Financial Crime Guide: A firm's guide to countering financial crime risks (FCG)

Financial Crime Guide: A firm's guide to countering financial crime risks (FCG)

Chapter 1

Introduction

1.1 What is the FCG?

1.1.1 G *FCG* provides practical assistance and information for firms of all sizes and across all *FCA*-supervised sectors on actions they can take to counter the risk that they might be used to further financial crime. Its contents are drawn primarily from *FCA* and *FSA* thematic reviews, with some additional material included to reflect other aspects of our financial crime remit.

1.1.2 G Effective systems and controls can help firms to detect, prevent and deter financial crime.*FCG* provides guidance on financial crime systems and controls, both generally and in relation to specific risks such as money laundering, bribery and corruption and fraud. Annexed to *FCG* is a list of common and useful terms. ■ FCG Annex 1 is provided for reference purposes only and is not a list of 'defined terms'. Where a word or phrase is in italics, its definition will be the one used for that word or phrase in the *Glossary* to the *FCA Handbook*.

1.1.3 G *FCTR* provides summaries of, and links to, *FSA* (now the *FCA*) thematic reviews of various financial crime risks and sets out the full examples of good and poor practice that were included with the reviews' findings.

1.1.4 G We will keep *FCG* under review and will continue to update it to reflect the findings of future thematic reviews, enforcement actions and other *FCA* publications and to cover emerging risks and concerns.

1.1.5 G The material in *FCG* does not form part of the *Handbook*, but it does contain *guidance* on *Handbook rules* and *principles*, particularly:

- ■ SYSC 3.2.6R and ■ SYSC 6.1.1R, which require firms to establish and maintain effective systems and controls to counter the risk that they might be used to further financial crime;
- Principles 1 (integrity), 2 (skill, care and diligence), 3 (management and control) and 11 (relations with regulators) of our Principles for Businesses, which are set out in ■ PRIN 2.1.1R;
- the Statements of Principle for Approved Persons set out in ■ APER 2.1A.3R and the conduct rules set out in ■ COCON 2.1 and ■ 2.2; and
- in relation to guidance on money laundering, the rules in ■ SYSC 3.2.6 to ■ SYSC 3.2.6 IR and ■ SYSC 6.3 (Financial crime).

Where *FCG* refers to guidance in relation to *SYSC* requirements, this may also be relevant to compliance with the corresponding Principle in our Principles for Businesses and corresponding requirements in the *Payment Services Regulations* and the *Electronic Money Regulations*. All elements of the *FCG* but particularly ■ FCG 3 on money laundering and ■ FCG 7 on sanctions will be relevant to cryptoasset businesses registered with us under the *Money Laundering Regulations*.

1.1.6 G Direct references in *FCG* to requirements set out in our rules or other legal provisions include a cross reference to the relevant provision.

1.1.7 G *FCG* contains 'general guidance' as defined in section 139B of the Financial Services and Markets Act 2000 (FSMA). The guidance is not binding and we will not presume that a firm's departure from our guidance indicates that it has breached our rules.

1.1.8 G Our focus, when supervising firms, is on whether they are complying with our rules and their other legal obligations. Firms can comply with their financial crime obligations in ways other than following the good practice set out in *FCG*. But we expect firms to be aware of what we say where it applies to them and to consider applicable guidance when establishing, implementing and maintaining their anti-financial crime systems and controls. More information about *FCA* guidance and its status can be found in our Reader's Guide: an introduction to the Handbook; ■ DEPP 6.2.1G(4) and ■ ENFG 3.4.

1.1.9 G *FCG* also contains guidance on how firms can meet the requirements of the *Money Laundering Regulations* and the EU Funds Transfer Regulation. While the relevant parts of the guide that refer to the *Money Laundering Regulations* may be 'relevant guidance' under these regulations, it is not approved by HM Treasury.

1.1.10 G The Joint Money Laundering Steering Group's (JMLSG) guidance for the UK financial sector on the prevention of money laundering and combating terrorist financing is 'relevant guidance' and is approved by HM Treasury under the *Money Laundering Regulations*. As confirmed in ■ DEPP 6.2.3G, ■ ENFG 6.1.2G and ■ ENFG App 2.2, the *FCA* will continue to have regard to whether firms have followed the relevant provisions of JMLSG's guidance when deciding whether conduct amounts to a breach of relevant requirements.

1.1.11 G *FCG* is not a standalone document; it does not attempt to set out all applicable requirements and should be read in conjunction with existing laws, rules and guidance on financial crime. If there is a discrepancy between *FCG* and any applicable legal requirements, the provisions of the relevant requirement prevail. If firms have any doubt about a legal or other provision or their responsibilities under FSMA or other relevant legislation or requirements, they should seek appropriate professional advice.

Among other requirements, firms should consider whether their financial crime systems and controls are consistent, where applicable, with their Consumer Duty obligations.

1

For instance, in complying with the Consumer Duty, firms may consider additional steps in their customer journeys to help prevent financial crime, including fraud. They may also consider offering additional consumer support, such as:

- a real-time human interface to deal with security or fraud concerns;
- engagement with customers during customer due diligence processes; or
- providing information on their application or application outcome for products and services.

Firms should consider FG22/5 when applying their financial crime systems and controls. In particular, firms may find it helpful to consider the following provisions:

- *Principle* 12: A firm must act to deliver good outcomes for retail customers;
- Cross-cutting obligations:
  - PRIN 2A.2.1R: A firm must act in good faith towards retail customers;
  - PRIN 2A.2.8R: A firm must avoid causing foreseeable harm to retail customers; and
  - PRIN 2A.2.14R: A firm must enable and support retail customers to pursue their financial objectives; and
- Consumer Duty outcome provisions:
- PRIN 2A.5 (Consumer Duty: retail customer outcome on consumer understanding); and
- PRIN 2A.6 (Consumer Duty: retail customer outcome on consumer support).

Firms should note that the Consumer Duty does not replace or override other applicable rules, guidance or law and does not require firms to act in a way that is incompatible with any legal or regulatory requirements, such as those under financial crime rules and obligations under the *Money Laundering Regulations*.

1.1.12 G To find out more on the Consumer Duty, see 'FG22/5 Final Non-Handbook Guidance for firms on the Consumer Duty' (www.fca.org.uk/publication/finalised-guidance/fg22-5.pdf).

1.2 How to use the FCG

1.2.1. G **Who should read this chapter?** This paragraph indicates the types of firm to which the material applies. A reference to 'all firms' in the body of the chapter means all firms to which the chapter is applied at the start of the chapter.

1.2.2 G Each section discusses how firms tackle a different type of financial crime. Sections open with a short passage giving context to what follows. In *FCG* we use:

- 'must' where provisions are mandatory because they are required by legislation or our rules
- 'should' to describe how we would normally expect a firm to meet its financial crime obligations while acknowledging that firms may be able to meet their obligations in other ways, and
- 'may' to describe examples of good practice that go beyond basic compliance.

1.2.3 G Firms should apply the guidance in a risk-based, proportionate way taking into account such factors as the nature, size and complexity of the firm. For example:

- We say in FCG 2.2.1G (Governance) that senior management should actively engage in a firm's approach to addressing financial crime risk. The level of seniority and degree of engagement that is appropriate will differ based on a variety of factors, including the management structure of the firm and the seriousness of the risk.
- We ask in FCG 3.2.5G (Ongoing monitoring) how a firm monitors transactions to spot potential money laundering. While we expect that a global retail bank that carries out a large number of customer transactions would need to include automated systems in its processes if it is to monitor effectively, a small firm with low transaction volumes could do so manually.
- We say in FCG 4.2.1G (General – preventing losses from fraud) that it is good practice for firms to engage with relevant cross-industry efforts to combat fraud. A national retail bank is likely to have a greater exposure to fraud, and therefore to have more information to contribute to such efforts, than a small local building society, and we would expect this to be reflected in their levels of engagement.

1.3 Format of the FCG

Financial crime: a guide for firms

1.3.1 G *FCG* looks at key aspects of firms' efforts to counter different types of crime. It is aimed at firms big and small; material will not necessarily apply to all situations. If guidance is specific to certain types of firm, this is indicated by italics.

Self-assessment questions:

- These questions will help you to consider whether your firm's approach is **appropriate**. (Text in brackets expands on this.)
- The *FCA* may follow **similar lines of inquiry** when discussing financial crime issues with firms.
- The questions draw attention to some of the key points firms should consider when deciding how to address a financial crime issue or comply with a financial crime requirement.

Examples of good practice	Examples of poor practice
• This list provides **illustrative** examples of **good practices**.	• This list provides **illustrative** examples of **poor practices**.
• Good practice examples are drawn from **conduct seen** in firms during thematic work in relation to financial crime.	• Poor practice examples are also drawn from **conduct seen** during thematic work.
• We would draw comfort from seeing **evidence** that these practices take place.	• Some show a lack of commitment, others fall short of our expectations; some, as indicated in the text, may breach regulatory requirements or be **criminal offences**.
• Note that **if these practices are lacking** it may not be a problem. The *FCA* would consider whether a firm has taken other measures to meet its obligations.	• These **do not identify all cases** where conduct may give rise to regulatory breaches or criminal offences.

Case studies and other information

1.3.2 G Most sections contain case studies outlining occasions when a person's conduct fell short of the regulatory expectations, and enforcement action followed; or information on topics relevant to the section.

1.4 Further financial crime information

1.4.1 G Where to find out more:

- Most sections close with some sources of further information..
- This includes cross-references to relevant guidance in *FCTR*.
- It also includes links to external websites and materials. Although the external links are included to assist readers of *FCG*, we are not responsible for the content of these, as we neither produce nor maintain them

Chapter 2

Financial crime systems and controls

2.1 Introduction

2.1.1 G **Who should read this chapter?** This chapter applies to **all firms** subject to the financial crime rules in ■ SYSC 3.2.6R or ■ SYSC 6.1.1R. It also applies to e-money institutions and payment institutions within our supervisory scope.

2.1.2 G The Annex I *financial institutions* which we supervise for compliance with their obligations under the *Money Laundering Regulations* are not subject to the financial crime rules in *SYSC*. But the guidance in this chapter applies to them as it can assist them to comply with their obligations under the Regulations.

2.1.3 G All firms must take steps to defend themselves against financial crime, but a variety of approaches is possible. This chapter provides guidance on themes that should form the basis of managing financial crime risk. The general topics outlined here are also relevant in the context of the specific financial crime risks detailed in subsequent chapters. See ■ SYSC 6.1.1R and ■ SYSC 3.2.6R.

2.2 Themes

Governance

2.2.1 G We expect **senior management** to take **clear responsibility** for managing financial crime risks, which should be treated in the same manner as other risks faced by the business. There should be evidence that senior management are **actively engaged** in the firm's approach to addressing the risks. In considering senior management arrangements in the Guide, firms should consider their arrangements to comply with the Senior Managers and Certification Regime (SM&CR).

[**Editor's note:** see https://www.fca.org.uk/firms/senior-managers-certification-regime]

Self-assessment questions:

- When did senior management, including the board or appropriate sub-committees, last consider financial crime issues? What action followed discussions?
- How are senior management kept **up to date** on financial crime issues? (This may include receiving reports on the firm's performance in this area as well as ad hoc briefings on individual cases or emerging threats.)
- Is there evidence that **issues have been escalated** where warranted?

Examples of good practice	Examples of poor practice
• Senior management **set the right tone** and demonstrate leadership on financial crime issues.	• There is little evidence of senior staff **involvement** and **challenge** in practice.
• A firm takes **active steps** to prevent criminals taking advantage of its services.	• A firm concentrates on **narrow compliance** with **minimum regulatory standards** and has little engagement with the issues.
• We would draw comfort from seeing evidence that these practices take place.	• Financial crime issues are dealt with on a purely **reactive** basis.
• A firm has a strategy for self-improvement on financial crime.	• There is **no meaningful record** or evidence of senior management considering financial crime risks.
• There are clear criteria for **escalating** financial crime issues.	

2

Management information (MI)

2.2.2 G MI should provide senior management with **sufficient information** to understand the financial crime risks to which their firm is exposed. This will help senior management effectively manage those risks and adhere to the firm's own risk appetite. MI should be provided regularly and ad hoc, as risk dictates.

Examples of financial crime MI include:

- an overview of the financial crime risks to which the firm is exposed, including information about emerging risks and any changes to the firm's risk assessment
- legal and regulatory developments and the impact these have on the firm's approach
- an overview of the effectiveness of the firm's financial crime systems and controls
- an overview of staff expenses, gifts and hospitality and charitable donations, including claims that were rejected, and
- relevant information about individual business relationships, for example:
  - the number and nature of new business relationships, in particular those that are high risk
  - the number and nature of business relationships that were terminated due to financial crime concerns
  - the number of transaction monitoring alerts
  - details of any true sanction hits, and
  - information about suspicious activity reports considered or submitted, where this is relevant.

MI may come from more than one source, for example the compliance department, internal audit, the MLRO or the nominated officer.

Structure

2.2.3 G Firms' **organisational structures** to combat financial crime may differ. Some large firms will have a single unit that coordinates efforts and which may report to the head of risk, the head of compliance or directly to the CEO. Other firms may spread responsibilities more widely. There is no one 'right answer' but the firm's structure should promote coordination and information sharing across the business.

Self-assessment questions:

- Who has ultimate **responsibility** for financial crime matters, particularly: a) anti-money laundering; b) fraud prevention; c) data security; d) countering terrorist financing; e) anti-bribery and corruption and f) financial sanctions?
- Do staff have **appropriate seniority** and **experience**, along with clear reporting lines?

•Does the structure promote a **coordinated approach** and **accountability**?

•Are the firm's financial crime teams **adequately resourced** to carry out their functions effectively? What are the annual budgets for dealing with financial crime, and are they **proportionate** to the risks?

•In smaller firms: do those with financial crime responsibilities have **other roles**? (It is reasonable for staff to have more than one role, but consider whether they are spread too thinly and whether this may give rise to conflicts of interest.)

Examples of good practice	Examples of poor practice
• Financial crime risks are addressed in a **coordinated** manner across the business and information is shared readily.	• The firm makes no effort to understand or address **gaps** in its financial crime defences.
• Management responsible for financial crime are **sufficiently senior** as well as being credible, independent, and experienced.	• Financial crime officers are relatively **junior** and lack access to senior management. They are often **overruled** without documented justification.
• A firm has considered how counter-fraud and anti-money laundering efforts can **complement** each other.	• Financial crime departments are **under-resourced** and senior management are reluctant to address this.
• A firm has a strategy for self-improvement on financial crime.	
• The firm bolsters insufficient in-house knowledge or resource with **external expertise**, for example in relation to assessing financial crime risk or monitoring compliance with standards.	

Risk assessment

2.2.4 G A **thorough understanding** of its **financial crime risks** is key if a firm is to apply proportionate and effective systems and controls.

A firm should identify and assess the financial crime risks to which it is exposed as a result of, for example, the products and services it offers, the jurisdictions it operates in, the types of customer it attracts, the complexity and volume of transactions, and the distribution channels it uses to service its customers. Firms can then target their financial crime resources on the areas of greatest risk.

A **business-wide risk assessment** – or risk assessments – should:

•be comprehensive and consider a wide range of factors – it is not normally enough to consider just one factor

•draw on a wide range of relevant information – it is not normally enough to consider just one source, and

2

- be proportionate to the nature, scale and complexity of the firm's activities.

Firms should build on their business-wide risk assessment or risk assessments to determine the level of risk associated with **individual relationships**. This should:

- enable the firm to take a holistic view of the risk associated with the relationship, considering all relevant risk factors, and
- enable the firm to apply the appropriate level of due diligence to manage the risks identified.

The assessment of risk associated with individual relationships can inform, but is not a substitute for, business-wide risk assessments.

Firms should regularly review both their business-wide and individual risk assessments to ensure they remain current.

Self-assessment questions:

- What are the main financial crime **risks** to the business?
- How does your firm seek to **understand** the financial crime risks it faces?
- When did the firm last **update** its **risk assessment**?
- How do you **identify new or emerging** financial crime risks?
- Is there evidence that risk is considered and recorded systematically, assessments are updated and **sign-off** is appropriate?
- Who **challenges** risk assessments and how? Is this process sufficiently rigorous and well-documented?
- How do **procedures** on the ground adapt to emerging risks? (For example, how quickly are policy manuals updated and procedures amended?)

Examples of good practice	Examples of poor practice
• The firm's risk assessment is **comprehensive**.	• Risk assessment is a **one-off** exercise.
• Risk assessment is a **continuous** process based on the best information available from internal and external sources.	• Efforts to understand risk are **piecemeal** and lack coordination.
• The firm assesses where risks are greater and **concentrates its resources** accordingly.	• Risk assessments are **incomplete**.
• The firm actively considers the **impact of crime** on customers.	• The firm targets financial crimes that affect the bottom line (e.g. fraud against the firm) but **neglects** those

Examples of good practice	Examples of poor practice
	where third parties suffer (e.g. fraud against customers).
• The firm considers financial crime risk when **designing new products** and **services**.	

Policies and procedures

2.2.5 G A firm must have in place up-to-date policies and procedures appropriate to its business. These should be **readily accessible**, **effective** and **understood** by all relevant staff.

Self-assessment questions:

•How often are your firm's policies and procedures **reviewed**, and at what level of **seniority**?

•How does it **mitigate** the financial crime risks it identifies?

•What steps does the firm take to ensure that relevant policies and procedures **reflect new risks** or **external events**? How quickly are any necessary changes made?

•What steps does the firm take to ensure that staff **understand** its policies and procedures?

•For larger groups, how does your firm ensure that policies and procedures are **disseminated** and **applied** throughout the business?

Examples of good practice	Examples of poor practice
• There is **clear documentation** of a firm's approach to complying with its legal and regulatory requirements in relation to financial crime.	• A firm has no **written policies** and **procedures**.
• Policies and procedures are **regularly reviewed** and **updated**.	• The firm **does not tailor** externally produced policies and procedures to suit its business.
• **Internal audit** or another independent party monitors the effectiveness of policies, procedures, systems and controls.	• The firm **fails to review** policies and procedures in light of events.
	• The firm **fails to check** whether policies and procedures are applied consistently and effectively.
	• A firm has not considered whether its policies and procedures are consistent with its obligations under legislation that forbids **discrimination**.

See ■ SYSC 3.2.6R and ■ SYSC 6.1.1R.

2

Staff recruitment, vetting, training, awareness and remuneration

2.2.6 G Firms must employ staff who possess the skills, knowledge and expertise to carry out their functions effectively. They should review employees' competence and take appropriate action to ensure they remain competent for their role. Vetting and training should be appropriate to employees' roles.

Firms should manage the risk of staff being rewarded for taking unacceptable financial crime risks. In this context, Remuneration Principle 12(h), as set out in ■ SYSC 19A.3.51R and ■ 19A.3.52E, may be relevant to firms subject to the Remuneration Code.

Self-assessment questions:

- What is your approach to **vetting** staff? Do vetting and management of different staff reflect the financial crime risks to which they are exposed?
- How does your firm ensure that its employees are aware of financial crime risks and of their **obligations** in relation to those risks?
- Do staff have access to training on an **appropriate range** of financial crime risks?
- How does the firm ensure that training is of **consistent quality** and is **kept up to date**?
- Is training **tailored** to particular roles?
- How do you assess the **effectiveness** of your training on topics related to financial crime?
- Is training material relevant and up to date? When was it **last reviewed**?

Examples of good practice	Examples of poor practice
•	•
• Staff in higher risk roles are subject to **more thorough vetting**.	• Staff are **not competent** to carry out preventative functions effectively, exposing the firm to financial crime risk.
• **Temporary staff** in higher risk roles are subject to the same level of vetting as permanent members of staff in similar roles.	• Staff vetting is a **one-off** exercise.
• Where **employment agencies** are used, the firm periodically satisfies itself that the agency is adhering to the agreed vetting standard.	• The firm fails to **identify changes** that could affect an individual's integrity and suitability.
• **Tailored** training is in place to ensure staff knowledge is adequate and up to date.	• The firm **limits enhanced vetting** to senior management roles and fails to vet staff whose roles expose them to higher financial crime risk.

Examples of good practice	Examples of poor practice
• New staff in **customer-facing** positions receive financial crime training tailored to their role before being able to interact with customers.	• The firm fails to identify whether staff whose roles expose them to bribery and corruption risk have **links to relevant political or administrative decision-makers**.
• Training has a strong **practical** dimension (e.g. case studies) and some form of testing.	• Poor compliance records are not reflected in **staff appraisals and remuneration**.
• The firm satisfies itself that staff **understand** their responsibilities (e.g. computerised training contains a test).	• Training dwells unduly on **legislation and regulations** rather than practical examples.
• **Whistleblowing** procedures are clear and accessible, and respect staff confidentiality.	• Training material is **not kept up to date**.
	• The firm **fails to identify** training needs.
	• There are no **training logs** or tracking of employees' training history.
	• Training **content** lacks management sign-off.
	• Training does not cover **whistleblowing** and **escalation** procedures.

See ■ SYSC 3.1.6R and ■ SYSC 5.1.1R.

Quality of oversight

2.2.7 G A firm's efforts to combat financial crime should be subject to **challenge**. We expect senior management to ensure that policies and procedures are appropriate and followed.

Self-assessment questions:

•How does your firm ensure that its approach to reviewing the effectiveness of financial crime systems controls is **comprehensive**?

•What are the **findings** of recent internal audits and compliance reviews on topics related to financial crime?

•How has the firm progressed **remedial measures**?

Examples of good practice	Examples of poor practice
• **Internal audit** and **compliance** routinely test the firm's defences against financial crime, including specific financial crime threats.	• Compliance unit and audit teams **lack experience** in financial crime matters.

Examples of good practice	Examples of poor practice
• Decisions on allocation of compliance and audit resource are **risk-based**. • Management **engage constructively** with processes of oversight and challenge. • Smaller firms seek **external help** if needed.	• Audit findings and compliance conclusions are **not shared** between business units. Lessons are not spread more widely.

2.3 Further guidance

2.3.1 G *FCTR* contains the following additional guidance on governance:

- FCTR 6.3.1G (Governance), from the *FSA's* thematic review Data security in Financial Services
- FCTR 8.3.1G (Senior management responsibility) from the *FSA's* thematic review Financial services firms' approach to UK financial sanctions
- FCTR 9.3.1G (Governance and management information) from the *FSA's* thematic review Anti-bribery and corruption in commercial insurance broking
- FCTR 11.3.1G (Governance, culture and information sharing) from the *FSA's* thematic review Mortgage fraud against lenders

2.3.2 G *FCTR* contains the following additional guidance on **risk assessment**:

- FCTR 8.3.2G (Risk assessment) from the *FSA's* thematic review Financial services firms' approach to UK financial sanctions
- FCTR 9.3.2G (Risk assessment and responses to significant bribery and corruption events) from the *FSA's* thematic review Anti-bribery and corruption in commercial insurance broking
- FCTR 10.3.7G (Responsibilities and risk assessments) from the *FSA's* thematic review The Small Firms Financial Crime Review
- FCTR 12.3.3G (High risk customers and PEPs – Risk assessment) and (Correspondent banking – Risk assessment of respondent banks) from the *FSA's* thematic review Banks' management of high money laundering risk situations

2.3.3 G *FCTR* contains the following additional guidance on **policies and procedures**:

- FCTR 8.3.3G (Policies and procedures) from the *FSA's* thematic review Financial services firms' approach to UK financial sanctions
- FCTR 10.3.1G (Regulatory/Legal obligations) from the *FSA's* thematic review The Small Firms Financial Crime Review

- FCTR 12.3.2G (High risk customers and PEPs – AML policies and procedures) from the *FSA's* thematic review Banks' management of high money laundering risk situations

2.3.4 G *FCTR* contains the following additional guidance on **staff recruitment, vetting, training and awareness**:

- FCTR 6.3.2G (Training and awareness) and FCTR 6.3.3G (Staff recruitment and vetting) from the *FSA's* thematic review Data security in Financial Services
- FCTR 8.3.4G (Staff training and awareness) from the *FSA's* thematic review Financial services firms' approach to UK financial sanctions
- FCTR 9.3.5G (Staff recruitment and vetting) and FCTR 9.3.6G (Training and awareness) from the *FSA's* thematic review Anti-bribery and corruption in commercial insurance broking
- FCTR 10.3.6G (Training) from the *FSA's* thematic review The Small Firms Financial Crime Review
- FCTR 11.3.6G (Staff recruitment and vetting) and FCTR 11.3.8G (Staff training and awareness) from the *FSA's* thematic review Mortgage fraud against lenders laundering risk situations

2.3.5 G *FCTR* contains the following additional guidance on **quality of oversight**:

- FCTR 6.3.15G (Internal audit and compliance monitoring) from the *FSA's* thematic review Data security in Financial Services
- FCTR 9.3.9G (The role of compliance and internal audit) from the *FSA's* thematic review Anti-bribery and corruption in commercial insurance broking
- FCTR 11.3.5G (Compliance and internal audit) from the *FSA's* thematic review Mortgage fraud against lenders

2.3.6 G For firms' obligations in relation to whistleblowers see the Public Interest Disclosure Act 1998: www.legislation.gov.uk/ukpga/1998/23/contents

Chapter 3

Money laundering and terrorist financing

3.1 Introduction

3.1.1 G **Who should read this chapter?** This section applies to **all firms** who are subject to the money laundering provisions in ■ SYSC 3.2.6A – J or ■ SYSC 6.3. It also applies to Annex I **financial institutions** and **e-money institutions** for whom we are the supervisory authority under the *Money Laundering Regulations*.

3.1.2 G This guidance does not apply to **payment institutions**, which are supervised for compliance with the *Money Laundering Regulations* by HM Revenue and Customs. But it may be of interest to them, to the extent that we may refuse to authorise them, or remove their authorisation, if they do not satisfy us that they comply with the *Money Laundering Regulations*.

3.1.3 G This guidance is less relevant for those who have more limited anti-money laundering (AML) responsibilities, such as mortgage brokers, general insurers and general insurance intermediaries. But it may still be of use, for example, to assist them in establishing and maintaining systems and controls to reduce the risk that they may be used to handle the proceeds from crime; and to meet the requirements of the Proceeds of Crime Act 2002 to which they are subject.

3.1.4 G ■ FCG 3.2.2G (The Money Laundering Reporting Officer (MLRO)) applies only to firms who are subject to the money laundering provisions in ■ SYSC 3.2.6A – J or ■ SYSC 6.3, except it does not apply to **sole traders who have no employees**.

3.1.5 G ■ FCG 3.2.13G (Customer payments) applies to banks subject to ■ SYSC 6.3.

3.1.6 G The guidance in this chapter relates both to our interpretation of requirements of the *Money Laundering Regulations* and to the financial crime and money laundering provisions of ■ SYSC 3.2.6R – ■ 3.2.6JG, ■ SYSC 6.1.1R and ■ SYSC 6.3.

3.1.7 G The Joint Money Laundering Steering Group (JMLSG) produces detailed guidance for firms in the UK financial sector on how to comply with their legal and regulatory obligations related to money laundering and terrorist financing. *FCG* is not intended to replace, compete or conflict with the JMLSG's guidance, which should remain a key resource for firms.

3

3.1.7A G The European Supervisory Authorities (ESAs) have produced guidelines that firms should consider when assessing the ML/TF risk associated with a business relationship or occasional transaction. The *Money Laundering Regulations* require firms subject to the regulations to take account of these guidelines when complying with the customer due diligence requirements in Regulations 33 and 37.

3.1.8 G When considering a firm's systems and controls against money laundering and terrorist financing, we will consider whether the firm has followed relevant provisions of the JMLSG's guidance, guidance issued by the *FCA* or taken account of the ESA guidelines.

3

3.2 Themes

Governance

3.2.1 G The guidance in ■ FCG 2.2.1G on governance in relation to financial crime also applies to money laundering. We expect senior management to take responsibility for the firm's anti-money laundering (AML) measures. This includes knowing about the money laundering risks to which the firm is exposed and ensuring that steps are taken to mitigate those risks effectively.

Regulation 21(1)(a) of the *Money Laundering Regulations* requires that where appropriate with regard to the size and nature of its business, *firms* subject to the regulations must appoint one individual who is a member of its board of directors (or if there is no board, of its equivalent *management body*) or of its *senior management* as the officer responsible for compliance with the regulations. Regulation 21(3) also requires the appointment of a nominated officer. Regulation 21(4) requires a *firm* to inform their supervisory authority of the identity of the individual appointed (including any subsequent appointments) within 14 *days* of such appointment.

As ■ SYSC 6.3.9R and ■ SYSC 3.2.6IR also require firms subject to those provisions to have an MLRO, the *FCA* expects that this individual can be the same individual appointed under Regulation 21(1)(a) and/or 21(3) of the *Money Laundering Regulations* and so *firms* do not need to make a separate notification to the FCA.

Self-assessment questions:

- Who has **overall responsibility** for establishing and maintaining effective AML controls? Are they sufficiently senior?
- What are the **reporting lines**?
- Do senior management receive **informative, objective information** that is sufficient to enable them to meet their AML obligations?
- How regularly do senior management commission **reports** from the **MLRO**? (This should be at least annually.) What do they do with the reports they receive? What **follow-up** is there on any recommendations the MLRO makes?
- How are senior management involved in **approving relationships** with high risk customers, including politically exposed persons (PEPs)?

Examples of good practice	Examples of poor practice
• **Reward structures** take account of any failings related to AML compliance.	• There is **little evidence** that AML is **taken seriously** by senior management. It is seen as a legal or **regulatory necessity** rather than a matter of true concern for the business.
• Decisions on accepting or maintaining high money laundering risk relationships are reviewed and challenged **independently** of the business relationship and escalated to senior management or committees.	• Senior management attach greater importance to the risk that a customer might be involved in a **public scandal**, than to the risk that the customer might be corrupt or otherwise engaged in financial crime.
• Documentation provided to senior management to inform decisions about entering or maintaining a business relationship provides an **accurate picture** of the risk to which the firm would be exposed if the business relationship were established or maintained.	• The board **never considers** MLRO reports.
• A UK parent undertaking meets the obligations under Regulation 20 of the *Money Laundering Regulations* including ensuring that AML policies, controls and procedures apply to all its branches and subsidiaries outside the UK.	• A UK branch or subsidiary uses group policies which **do not comply** fully with UK AML legislation and regulatory requirements.

The Money Laundering Reporting Officer (MLRO)

3.2.2 G This section applies to firms who are subject to the money laundering provisions in ■ SYSC 3.2.6A – J or ■ SYSC 6.3, except it does not apply to sole traders who have no employees.

Firms to which this section applies must appoint an individual as MLRO. The MLRO is responsible for oversight of the firm's compliance with its anti-money laundering obligations and should act as a focal point for the firm's AML activity. Regulation 21(1)(a) of the *Money Laundering Regulations* also requires the appointment of a *senior manager* as the officer responsible for the relevant person's compliance with these regulations. Where appropriate, this section can be relevant to how that person meets their obligations under the *Money Laundering Regulations*. If the MLRO meets the requirements in regulation 21(1)(a) and (3), firms need not make a separate notification to us.

Self-assessment questions:

•Does the MLRO have sufficient resources, experience, access and seniority to carry out their role effectively?

•Do the firm's staff, including its senior management, consult the MLRO on matters relating to money-laundering?

•Does the MLRO escalate relevant matters to senior management and, where appropriate, the board?

•What awareness and oversight does the MLRO have of the highest risk relationships?

Examples of good practice	Examples of poor practice
• The MLRO is independent, knowledgeable, robust and well-resourced, and poses effective challenge to the business where warranted.	• The MLRO lacks credibility and authority, whether because of inexperience or lack of seniority.
• The MLRO has a direct reporting line to executive management or the board.	• The MLRO does not understand the policies they are supposed to oversee or the rationale behind them.
	• The MLRO of a firm which is a member of a group has not considered whether group policy adequately addresses UK AML obligations.
	• The MLRO is unable to retrieve information about the firm's high-risk customers on request and without delay and plays no role in monitoring such relationships.

See ■ SYSC 3.2.6IR and ■ SYSC 6.3.9R.

Risk assessment

3.2.3 G The guidance in ■ FCG 2.2.4G and ■ FCG 7.2.5G on risk assessment in relation to financial crime and proliferation financing (PF) also applies.

The assessment of financial crime and PF risk is at the core of the firm's AML, counter-terrorist financing (CTF) and PF effort and is essential to the development of effective AML/CTF/PF policies and procedures. A firm is required by Regulation 18 of the *Money Laundering Regulations* to undertake a risk assessment. This also includes a risk assessment by relevant persons in relation to PF as set out in Regulation 18A of those regulations.

Firms must therefore put in place systems and controls to identify, assess, monitor and manage money laundering, terrorist financing and PF risk. These systems and controls must be comprehensive and proportionate to the nature, scale and complexity of a firm's activities. Firms must regularly review their risk assessment to ensure it remains current.

Under section 188 of the Economic Crime and Corporate Transparency Act 2023, firms are able to share information with one another for the purpose of preventing, detecting and investigating economic crime. Regulated firms should use this information to assist with their risk-based decision making and should not share it for commercial reasons or to provide sectors with additional powers to exclude customers inappropriately. Firms must also consider their obligations under the *General data protection regulation*.

Self-assessment questions:

•Which parts of the business present **greater risks** of money laundering, terrorist financing and PF? (Has your firm identified the

risks associated with different types of customers or beneficial owners, products, services, activities, transactions, business lines, geographical locations and delivery channels (e.g. internet, telephone, branches)? Has it assessed the extent to which these risks are likely to be an issue for the firm?)

•How does the risk assessment inform your day-to-day operations? (For example, is there evidence that it informs the level of customer due diligence you apply or your decisions about accepting or maintaining relationships?)

•For *cryptoasset businesses*, how do you assess and address the risks of different types of cryptoasset (e.g. anonymity-enhanced or privacy coins)?

Examples of good practice	Examples of poor practice
• There is evidence that the firm's risk assessment informs the design of anti-money laundering controls.	• An inappropriate risk classification system makes it almost impossible for a relationship to be classified as 'high risk'.
• The firm has identified good sources of information on money laundering, terrorist financing and PF risks, such as National Risk Assessments, FATF mutual evaluations and typology reports, NCA alerts, press reports, court judgements, reports by non-governmental organisations and commercial due diligence providers.	• Higher risk countries are allocated low-risk scores to avoid enhanced due diligence measures.
• Consideration of money laundering, terrorist financing and PF risk associated with individual business relationships takes account of factors such as: company structures; political connections; country risk; the customer's or beneficial owner's reputation; source of wealth; source of funds; expected account activity; factors relating to the customer's countries or geographic areas of operations; products and services; transactions; delivery channels; sector risk; and involvement in public contracts.	• Relationship managers are able to **override customer risk scores** without sufficient evidence to support their decision.

3

Examples of good practice	Examples of poor practice
• The firm identifies where there is a risk that a relationship manager might become too close to customers to identify and take an objective view of the money laundering risk. It manages that risk effectively.	• Risk assessments on money laundering are unduly influenced by the **potential profitability** of new or existing relationships. • The firm **cannot evidence** why customers are rated as high, medium or low risk. • A UK branch or subsidiary relies on group risk assessments without assessing their compliance with UK AML requirements.
• The firm **engages** with **public-private partnerships and private-private partnerships** to gather insights on the latest financial crime typologies and additional controls that might be relevant and shares its own best practice examples.	

See regulation 18 of the *Money Laundering Regulations*, ■ SYSC 3.2.6AR, ■ SYSC 3.2.6CR, ■ SYSC 6.3.1R and ■ SYSC 6.3.3R.

Customer due diligence (CDD) checks

3.2.4 G Firms must **identify** their customers and, where applicable, their beneficial owners, and then **verify** their identities. Firms must also understand the **purpose** and **intended nature** of the customer's relationship with the firm and collect information about the customer and, where relevant, beneficial owner. This should be sufficient to obtain a complete picture of the risk associated with the business relationship and provide a meaningful basis for subsequent monitoring.

Firms should note that CDD measures also apply when contacting an existing customer as part of any legal duty in the course of a calendar year for the purpose of reviewing information which is relevant to the risk assessment of the customer, and relates to beneficial ownership of the customer.

Firms should also note that CDD measures must also be applied when the relevant person has to contact an existing customer in order to fulfil any duty under the International Tax Compliance Regulations 2015.

CDD measures must also include taking reasonable steps to understand the ownership and control structure of a customer where the customer is a legal person, trust, company, foundation or similar legal arrangement.

Firms are required to keep written records in circumstances where all possible means of identifying the beneficial owner of a *body corporate* have been taken and the beneficial owner cannot be identified satisfactorily or at all. In circumstances where the beneficial owner of a *body corporate* cannot be identified, reasonable measures must be taken to verify the identity of the senior person in the *body corporate* responsible for managing it. In doing so, firms should keep written records made of the actions taken and any difficulties encountered.

Firms are required to collect proof of company registration (or an excerpt from the register) before establishing a business relationship with certain legal entities including a company subject to the requirements of Part 21A of the Companies Act 2006, a limited liability partnership or an eligible Scottish partnership. Firms are required to report to Companies House discrepancies between this information and information which otherwise becomes available to them in the course of complying with the *Money Laundering Regulations*. Firms may wish to refer to further guidance from the Companies House.

In situations where the money laundering risk associated with the business relationship is increased, banks must carry out additional, enhanced due diligence (EDD). ■ FCG 3.2.8G below considers enhanced due diligence.

Where a firm cannot apply customer due diligence measures, including where a firm cannot be satisfied that it knows who the beneficial owner is, it must not enter into, or continue, the business relationship.

Firms should note that an electronic identification process may be regarded as a reliable source for the purposes of CDD verification where that process is independent of the person whose identity is being verified, secure from fraud and misuse and capable of providing an appropriate level of assurance that the person claiming a particular identity is in fact that person with that identity.

Self-assessment questions:

•Does your firm apply **customer due diligence** procedures in a risk-sensitive way?

•Do your CDD processes provide you with a **comprehensive understanding** of the risk associated with individual business relationships?

•How does the firm **identify** the customer's **beneficial owner(s)**? Are you satisfied that your firm takes risk-based and adequate steps to verify the beneficial owner's identity in all cases? Do you understand the rationale for beneficial owners using complex corporate structures?

•Are procedures **sufficiently flexible** to cope with customers who cannot provide more common forms of identification (ID)?

•With **non-face-to-face** transactions, how does your firm's approach provide confidence that the person is **who they claim to be**? How do you test any technology used as part of onboarding?

Examples of good practice	Examples of poor practice
• A firm which uses e.g. **electronic verification checks** or **PEPs databases** understands their capabilities and limitations.	• Procedures are not **risk-based**: the firm applies the same CDD measures to products and customers of varying risk.
• The firm can cater for **customers who lack common forms of ID** (such as the socially ex-	• The firm has **no method for tracking** whether checks on customers are complete.

Examples of good practice	Examples of poor practice
cluded, those in care, etc).	
• The firm understands and documents the **ownership and control structures** (including the reasons for any complex or opaque corporate structures) of customers and their beneficial owners.	• The firm allows **language difficulties** or **customer objections** to get in the way of proper questioning to obtain necessary CDD information.
• The firm obtains information about the purpose and nature of the business relationship sufficient to be satisfied that it **understands** the **associated money laundering risk**.	• Staff do **less CDD** because a customer is referred by senior executives or influential people.
• Staff who approve new or ongoing business relationships satisfy themselves that the firm has obtained **adequate CDD** information before doing so.	• The firm has **no procedures** for dealing with situations requiring enhanced due diligence. **This breaches the** *Money Laundering Regulations*.
	• The firm fails to consider: any individuals who ultimately control more than 25% of shares or voting rights of a corporate customer; any individuals who exercise control over the management of a corporate customer; and any individuals who control the body corporate when identifying and verifying the customer's beneficial owners. **This breaches the** *Money Laundering Regulations*.

See regulations 5, 6, 27, 28, 30A, 31, 33, 34 and 35 of the *Money Laundering Regulations*.

Ongoing monitoring

3.2.5 G A firm must conduct ongoing monitoring of its business relationships on a risk-sensitive basis. Ongoing monitoring means **scrutinising transactions** to ensure that they are consistent with what the firm knows about the customer, and taking steps to ensure that the firm's knowledge about the business relationship remains current. As part of this, firms must keep documents, data and information obtained in the CDD context (including information about the purpose and intended nature of the business relationship) up to date. It must apply CDD measures where it doubts the truth or adequacy of previously obtained documents, data or information (see ■ FCG 3.2.4G).

Where the risk associated with the business relationship is increased, firms must carry out enhanced ongoing monitoring of the business relationship. ■ FCG 3.2.9G provides guidance on enhanced ongoing monitoring.

Self-assessment questions:

•How are transactions **monitored** to spot potential money laundering? Are you satisfied that your monitoring (whether automatic, manual or both) is adequate and effective considering such factors as the size, nature and complexity of your business?

•Does the firm **challenge** unusual activity and explanations provided by the customer where appropriate?

•How are **unusual transactions** reviewed? (Many alerts will be false alarms, particularly when generated by automated systems. How does your firm decide whether behaviour really is suspicious?)

•How do you feed the **findings from monitoring** back into the customer's risk profile?

•Do you frequently **review** the monitoring system rules and typologies for effectiveness? Do you **understand** the threshold and rule rationales?

Examples of good practice	Examples of poor practice
• A large retail firm complements its other efforts to spot potential money laundering by using an **automated system** to monitor transactions	• The firm fails to take adequate measures to understand the risk associated with the business relationship and is therefore **unable to conduct meaningful monitoring**.
• Where a firm uses automated transaction monitoring systems, it understands their capabilities and limitations.	• The MLRO can provide **little evidence** that **unusual transactions** are brought to their attention.
• Small firms are able to apply credible **manual procedures** to scrutinise customers' behaviour.	• Staff **always accept a customer's explanation** for unusual transactions at face value and do not probe further.
• The '**rules**' underpinning monitoring systems are understood by the relevant staff and updated to reflect new trends.	• The firm does not take risk-sensitive measures to ensure CDD information is **up to date**. **This is a breach of the** *Money Laundering Regulations*.
• The firm uses **monitoring results** to find out whether CDD remains adequate.	• A cryptoasset business assumes that blockchain analysis is all that is required to monitor transactions and fails to do its **own transaction monitoring** based on the **knowledge** of its customers or **relying on** off-chain information.
• The firm takes advantage of **customer contact** as an oppor-	• •The firm's measures fail to conduct a **full assessment** of

Examples of good practice	Examples of poor practice
tunity to update due diligence information. • The firm demonstrates a **risk-based approach** following a **monitoring event**. This could include implementing regular periodic reviews and having procedures for event-driven reviews. • **Customer-facing staff** are engaged with, but do not control, the ongoing monitoring of relationships. • The firm updates CDD information and reassesses the risk associated with the business relationship where monitoring indicates **material changes** to a customer's profile.	the risk. For instance, the firm does not consider **changes** in the nature of the relationship or expected activities.

See regulations 27, 28(11), 33, 34 of the *Money Laundering Regulations*.

The use of transaction monitoring

3.2.5A G This section is relevant to a firm using transaction monitoring as part of its ongoing monitoring efforts to detect money laundering, financing of terrorism and proliferation financing (see ■ FCG 3.2.5G (Ongoing monitoring)). This could be relevant to firms serving either retail or wholesale customers.

To date, many large institutions have used transaction monitoring systems that work on a transaction-by-transaction or unusual transaction basis, or combination of the two, flagging fund movements that exceed rule-driven thresholds for human scrutiny. We understand that more sophisticated approaches show potential in this area, and can be used to take a more rounded view of customer behaviour – for example, showing how the customer fits into broader networks of activity. Examples of such sophisticated technologies include the use of machine learning tools or tools based on artificial intelligence to detect suspicious activity or triage existing alerts.

This section applies to the use of both automated and manual transaction monitoring, unless specified otherwise.

Self-assessment questions:

- Do you **understand the effectiveness** of your automated monitoring in different business areas?
- What actions have been taken to **mitigate shortcomings** that have been identified in business areas?
- What **consideration** has been given to alternative varieties of automated monitoring, including the use of novel approaches?

•Where a firm uses automated methods for **triaging alerts** generated by threshold-driven transaction-monitoring systems (e.g. scorecards overlaid on existing systems or other systems to prioritise which alerts receive manual attention), can this be **justified** within the context of the firm's overall approach to monitoring?

Examples of good practice	Examples of poor practice
• New approaches are piloted or subject to evaluation periods, with firms able to demonstrate **appropriate testing**.	
• Monitoring arrangements (whether automated or manual or both) seek to take a **holistic view** of customer behaviour and draw on a range of data, rather than just transaction-by-transaction analysis.	• The **control framework** around automated monitoring is **weak**. For example, senior management have an unrealistic expectation of what automated monitoring systems are feasibly able to achieve, while manual scrutiny of alerts lacks resources and is unable to cope.
• Monitoring is applied, where appropriate, at multiple levels of aggregation: transaction level (the lowest); account level (the aggregate of transactions for an account); customer level (the aggregate of accounts for a specific customer); and linked-entity level (i.e. across a group of linked customers by relationship managers).	• Threshold-based transaction monitoring **approaches** are used in situations where they are **not suitable**, while other methods of scrutiny (such as oversight of customers by relationship managers) are neglected.
• When **decommissioning** an existing automated system (or aspects of that system, such as particular rule sets), a firm is able to **justify** this decision. Consideration may	• A threshold-based, rule-driven transaction monitoring system is used but is **poorly calibrated** and the firm **struggles to articulate the rationale** for

Examples of good practice	Examples of poor practice
be given to, for example, the relative merits of other approaches (including manual approaches), the systems' resource implications, and the systems' performance outcomes (such as the intelligence-value of alerts and the proportion of 'false positives').	particular rules and scenarios.
• Before a new system replaces an existing one, a **robust judgement** is formed about the relative **usefulness of both systems**. While each system may not flag all the same events, the firm is able to demonstrate that one approach produces better quality alerts overall.	• Data fed into an automated system is not migrated smoothly when feeder systems are modified or upgraded or transactions from a specific system have been erroneously omitted from the transaction monitoring system.
• A firm **explores** the use of **new approaches** to automated monitoring (e.g. network analysis or machine learning). Consideration is given to the **limitations** of these approaches and how any resultant risks can be contained. (For example, it will not be clear to operators of more free-form varieties of machine learning why the software has made its recommendations, which can pose ethical and audit challenges.)	
• The firm **tailors** the monitoring system rules to its **business, risk and relevant typologies**. The system and rules are **tested and reviewed** for right outcomes	• The firm uses a transaction monitoring system with set rules (which could include use of off-the-shelf systems) and does **not calibrate** these to the **firms' individual needs** or **review** them regularly for efficiency.
• The firm practices **good record keeping**. For example, records of decision making and rationales for thresholds are documented and accessible.	
• Where a firm learns that criminals have abused its facilities, a **review** is performed to **learn** how monitoring methods could be	

Examples of good practice	Examples of poor practice
improved to **lessen the risk of recurrence**.	
• Where a firm learns that criminals have abused its facilities, a **review** is performed to **learn** how monitoring methods could be improved to **lessen the risk of recurrence**.	
	• A firm **does not** check that a **counterparty** firm is monitoring customer activity.
• A firm using an automated system keeps records of how the system has been trained. It records the process for making adjustments and how the interpretable model can be maintained.	• A firm using an automated system **lacks an understanding of what the system is detecting and why.** This may be because of, for example, staff turnover, poor documentation or weak communication with the system's vendor.

See regulations 27, 28(11), 33 and 34 of the *Money Laundering Regulations*.

Case study – transaction monitoring

3.2.5B G

The *FCA* found that 3 key parts of HSBC's transaction monitoring systems showed serious weaknesses over an extended period of several years. The systems were ineffective and not sufficiently risk sensitive for a prolonged period. They exposed the bank and community to avoidable risks.

In particular, the bank failed to:

•consider whether the scenarios used to identify indicators of money laundering or terrorist financing covered relevant risks;

•carry out timely risk assessments for new scenarios;

•appropriately test and update the parameters within the systems that were used to determine whether a transaction was indicative of potentially suspicious activity. There was a failure to understand those rules and certain thresholds set made it almost impossible for the relevant scenarios to identify potentially suspicious activity; and

•check the accuracy and completeness of the data being fed into, and contained within, monitoring systems. This resulted in millions of transactions worth billions of pounds that were either monitored incorrectly or not at all.

The *FCA* imposed a financial penalty of £63,946,800.

See the *FCA's* press release: www.fca.org.uk/news/press-releases/fca-fines-hsbc-bank-plc-deficient-transaction-monitoring-controls.

3

Source of wealth and source of funds

3.2.6 G Establishing the source of funds and the source of wealth can be useful for ongoing monitoring and due diligence purposes because it can help firms ascertain whether the level and type of transaction is consistent with the firm's knowledge of the customer. It is a requirement where the customer is a PEP.

'Source of wealth' describes how a customer or beneficial owner acquired their total wealth.

'Source of funds' refers to the origin of the funds involved in the business relationship or occasional transaction. It refers to the activity that generated the funds, for example salary payments or sale proceeds, as well as the means through which the customer's or beneficial owner's funds were transferred.

The JMLSG's guidance provides that, in situations where the risk of money laundering/terrorist financing is very low and subject to certain conditions, firms may assume that a payment drawn on an account in the customer's name with a UK, EU or equivalent regulated credit institution satisfied the standard CDD requirements. This is sometimes referred to as 'source of funds as evidence' and is distinct from 'source of funds' in the context of Regulation 28(11) and Regulations 33 and 35 of the *Money Laundering Regulations* and of *FCG*. Nothing in *FCG* prevents the use of 'source of funds as evidence' in situations where this is appropriate.

Where the customer is either a PEP, a family member of a PEP or known close associate of a PEP, a firm may have regard to guidance issued by the *FCA* on the treatment of PEPs.

[**Editor's Note:** see https://www.fca.org.uk/publications/finalised-guidance/fg17-6-treatment-politically-exposed-persons-peps-money-laundering.]

Handling higher risk situations

3.2.7 G The law requires that firms' anti-money laundering policies and procedures are sensitive to risks. This means that in higher risk situations, firms must apply enhanced due diligence and ongoing monitoring. **Situations that present a higher money laundering risk** might include, but are not restricted to: customers linked to higher risk countries or business sectors; or who have unnecessarily complex or opaque beneficial ownership structures; and transactions which are unusual, lack an obvious economic or lawful purpose, are complex or large or might lend themselves to anonymity.

Firms must take account of risk factors set out under regulation 33(6) which relate to customer risk, product risk and geographical risk when assessing whether there is a high risk of money laundering or terrorist financing in a particular situation and the extent of measures which should be taken to manage and mitigate that risk.

The *Money Laundering Regulations* also set out some scenarios in which specific enhanced due diligence measures have to be applied:

- **Correspondent relationships**: where a correspondent credit institution or financial institution, involving the execution of payment, is from a third country (see regulation 34 of the *Money Laundering Regulations*), the UK credit or financial institution should apply both EDD measures in regulation 33 as well as additional measures outlined in regulation 34 commensurate to the risk of the relationship. This can include in higher risk situations thoroughly

understanding its correspondent's business, reputation, and the quality of its defences against money laundering and terrorist financing. Senior management must also give approval before establishing a new correspondent relationship. JMLSG guidance sets out how firms should apply EDD in differing correspondent trading relationships.

•**Politically exposed persons (PEPs), family members and known close associates of a PEP**: a PEP is a person entrusted with a prominent public function, other than as a middle-ranking or more junior official. PEPs (as well as their family members and known close associates) must be subject to enhanced scrutiny. A senior manager at an appropriate level of authority must also approve the initiation of a business relationship with a PEP (or with a family member, or known close associate, of a PEP). This includes approving a relationship continuing with an existing customer who became a PEP after the relationship begun. In meeting these obligations firms may have regard to the *FCA's* guidance on a risk-based approach to PEPs.

•**Business relationships or a 'relevant transaction' where either party is established in a high risk third country**: the *Money Laundering Regulations* defines:

(a)a high-risk third country as a country named by FATF on its list of High-Risk Jurisdictions subject to a Call for Action or its list of Jurisdictions under Increased Monitoring;

(b)a relevant transaction as being a transaction in relation to which the relevant person is required to apply customer due diligence under Regulation 27;

(c)established in a country in the case of a legal person as being the country of incorporation or principal place of business, or, in the case of a financial institution or credit institution, where its principal regulatory authority is.

In these scenarios, EDD must include specified measures which include obtaining additional information on the customer, the beneficial owner, the intended nature of the business relationship, source of funds and wealth, reasons for the transactions and senior management approval for the business relationship. Conducting enhanced monitoring is also a requirement.

•**Other transactions**: EDD must be performed:

() in any case where a transaction is complex or unusually large, or there is an unusual pattern of transactions, or the transaction or transactions have no apparent economic or legal purpose. In this scenario, there are specified EDD measures which must include, as far as reasonably possible, examining the background and purpose of the transaction and increasing the degree and nature of monitoring of the business relationship in which the transaction is made to determine whether that transaction or that relationship appears to be suspicious;

() in any other case which by its nature can present a higher risk of money laundering, proliferation financing or terrorist financing. This can include where there is evidence that a cryptoasset transaction has involved privacy-enhancing techniques or products such as 'mixers' or 'tumblers', privacy coins and

transactions involving the use of self-hosted addresses, obfuscated ledger technology, ring signatures, stealth addresses, ring confidential transactions, atomic swaps and non-interactive zero knowledge proofs; and

() where findings from blockchain analysis indicates exposure to criminal or sanctioned activities.

Where the customer is the beneficiary of a life insurance policy, is a legal person or a legal arrangement, and presents a high risk of money laundering or terrorist financing for any other reason, credit and financial institutions must take reasonable measures to identify and verify the identity of the beneficial owners of that beneficiary before making a payment under the life insurance policy.

The extent of enhanced due diligence measures that a firm undertakes can be determined on a risk-sensitive basis. The firm must be able to demonstrate that the extent of the enhanced due diligence measures it applies is commensurate with the money laundering and terrorist financing risks.

See regulations 19, 20, 21, 28(16), 33 and 34 of the *Money Laundering Regulations*.

Handling higher risk situations – enhanced due diligence (EDD)

3.2.8 G Firms must apply EDD measures in situations that present a higher risk of money laundering.

EDD should give firms a **greater understanding** of the customer and their associated risk than standard due diligence. It should provide more certainty that the customer and/or beneficial owner is who they say they are and that the purposes of the business relationship are legitimate; as well as increasing opportunities to identify and deal with concerns that they are not.
■ FCG 3.2.3G considers risk assessment.

The extent of EDD must be **commensurate to the risk** associated with the business relationship or occasional transaction but firms can decide, in most cases, which aspects of CDD they should enhance. This will depend on the reason why a relationship or occasional transaction was classified as high risk.

Examples of EDD include:

•obtaining more information about the customer's or beneficial owner's business

•obtaining more robust verification of the beneficial owner's identity based on information from a reliable and independent source

•gaining a better understanding of the customer's or beneficial owner's reputation and/or role in public life and assessing how this affects the level of risk associated with the business relationship

•carrying out searches on a corporate customer's directors or other individuals exercising control to understand whether their business or integrity affects the level of risk associated with the business relationship

•establishing how the customer or beneficial owner acquired their wealth to be satisfied that it is legitimate

•establishing the source of the customer's or beneficial owner's funds to be satisfied that they do not constitute the proceeds from crime.

Self-assessment questions:

•How does EDD differ from standard CDD? How are issues that are flagged during the due diligence process **followed up** and **resolved**? Is this adequately documented?

•How is EDD information **gathered, analysed, used** and **stored**?

•What involvement do senior management or committees have in **approving high risk customers**? What information do they receive to inform any decision-making in which they are involved?

Examples of good practice	Examples of poor practice
• The MLRO (and their team) have **adequate oversight** of all high risk relationships.	• Senior management **do not give approval** for taking on high risk customers. **If the customer is a PEP or a non-EEA correspondent , this breaches the** *Money Laundering Regulations*.
• The firm establishes the legitimacy of, and documents, the **source of wealth** and **source of funds** used in high risk business relationships.	• [deleted]
• Where money laundering risk is very high, the firm obtains **independent** internal or **external intelligence** reports.	• The firm **does not distinguish** between the customer's source of funds and their source of wealth.
• When assessing EDD, the firm **complements staff knowledge** of the customer or beneficial owner with more objective information.	• The firm relies entirely on a **single source** of information for its enhanced due diligence.
• The firm is able to provide evidence that relevant information staff have about customers or beneficial owners is **documented and challenged** during the CDD process.	• A firm relies on intra-group introductions where **overseas standards are not UK-equivalent** or where due diligence data is **inaccessible** because of legal constraints.
• A member of a group satisfies itself that it is appropriate to rely on due diligence performed by **other entities** in the same group.	• The firm considers the **credit risk** posed by the customer, but not the **money laundering risk**.
• The firm proactively **follows up gaps in, and updates,** CDD of higher risk customers.	• The firm **disregards** allegations of the customer's or beneficial owner's **criminal activity** from reputable sources repeated over a sustained period of time.

Examples of good practice	Examples of poor practice
• A correspondent bank seeks to **identify PEPs** associated with their respondents	• The firm ignores adverse allegations simply because customers hold a UK **investment visa**.
• . A correspondent bank takes a view on the strength of the **AML regime** in a respondent bank's home country, drawing on discussions with the respondent, overseas regulators and other relevant bodies.	• A firm grants **waivers** from establishing source of funds, source of wealth or other due diligence without good reason.
• A correspondent bank gathers information about **respondent banks' procedures** for sanctions screening, PEP identification and management, account monitoring and suspicious activity reporting.	• A correspondent bank conducts inadequate due diligence on **parents** and **affiliates** of respondents.
	• A correspondent bank **relies exclusively** on the Wolfsberg Group AML questionnaire.

See regulations 33, 34, 34(1)(d), 35 and 35(5)(a) of the *Money Laundering Regulations*.

Handling higher risk situations – enhanced ongoing monitoring

3.2.9 G Firms must enhance their ongoing monitoring in higher risk situations.

Self-assessment questions:

•How does your firm **monitor** its high risk business relationships? How does enhanced ongoing monitoring differ from ongoing monitoring of other business relationships?

•Are reviews carried out **independently** of relationship managers?

•What **information** do you store in the files of high risk customers? Is it useful? (Does it include risk assessment, verification evidence, expected account activity, profile of customer or business relationship and, where applicable, information about the ultimate beneficial owner?)

Examples of good practice	Examples of poor practice
• Key AML staff have a **good understanding** of, and **easy access** to, information about a bank's highest risk customers.	• The firm treats annual reviews as a **tick-box exercise** and copies information from previous reviews without thought.
• New higher risk clients are more closely monitored to confirm or amend **expected account activity**.	• A firm in a group relies on others in the group to carry out monitoring **without understanding** what they did and what they found.
• **Alert thresholds** on automated monitoring systems are	• There is **insufficient challenge** to explanations from relation-

Examples of good practice	Examples of poor practice
lower for PEPs and other higher risk customers. Exceptions are **escalated** to more senior staff.	ship managers and customers about unusual transactions.
• Decisions across a group on whether to keep or exit high risk relationships are **consistent** and in line with the firm's overall risk appetite or assessment.	• The firm **focuses too much** on **reputational or business issues** when deciding whether to exit relationships with a high money laundering risk. • The firm makes no enquiries when accounts are used for purposes **inconsistent with expected** activity (e.g. personal accounts being used for business).

See regulation 33(1) of the *Money Laundering Regulations*.

Liaison with law enforcement

3.2.10 G Firms must have a **nominated officer**. The nominated officer has a legal obligation to **report any knowledge or suspicions** of money laundering to the National Crime Agency (NCA) through a 'Suspicious Activity Report', also known as a 'SAR'. (See ■ FCG Annex 1 list of common terms for more information about nominated officers and Suspicious Activity Reports.)

Staff must report their concerns and may do so to the firm's nominated officer, who must then consider whether a report to NCA is necessary based on all the information at their disposal. Law enforcement agencies may seek information from the firm about a customer, often through the use of Production Orders (see ■ FCG Annex 1).

Self-assessment questions:

- Is it clear who is **responsible** for different types of liaison with the authorities?
- How does the **decision-making** process related to **SARs** work in the firm?
- Are procedures clear to staff?
- Do staff report suspicions to the **nominated officer**? If not, does the nominated officer take steps to identify why reports are not being made? How does the nominated officer deal with reports received?
- What evidence is there of the rationale **underpinning decisions** about whether a SAR is justified?
- Is there a documented process for responding to **Production Orders**, with clear timetables?

3

Examples of good practice	Examples of poor practice
• All staff **understand procedures for escalating suspicions** and follow them as required.	• The nominated officer **passes all internal reports** to NCA without considering whether they truly are suspicious. These 'defensive' reports are likely to be of little value.
• The firm's **SARs** set out a clear narrative of events and include detail that law enforcement authorities can use (e.g. names, addresses, passport numbers, phone numbers, email addresses).	• The nominated officer **dismisses concerns** escalated by staff without reasons being documented.
• SARs set out the reasons for suspicion in **plain English**. They include some context on any previous related SARs rather than just a cross-reference.	• The firm **does not train** staff to make internal reports, thereby exposing them to personal legal liability and increasing the risk that suspicious activity goes unreported.
• There is a clear process for **documenting** decisions.	• The nominated officer **turns a blind eye** where a SAR might harm the business. **This could be a criminal offence**.
• A firm's processes for dealing with suspicions reported to it by **third party administrators** are clear and effective.	• A firm provides extraneous and irrelevant detail in response to a **Production Order**.

See regulation 21 of the *Money Laundering Regulations* and s.330 POCA and s.331 POCA and s.21A of the Terrorism Act 2000.

Record keeping and reliance on others

3.2.11 G Firms must keep copies of any documents and information obtained to meet CDD requirements and sufficient supporting records for transactions for **five years** after the business relationship ends or five years after an occasional transaction. However, records relating to transactions occurring in a business relationship need not be kept beyond 10 years. Where a firm is **relied on by others** to do due diligence checks, it must keep its records of those checks for the same time period. Firms must keep records sufficient to demonstrate to us that their CDD measures are appropriate in view of the risk of money laundering and terrorist financing. Regulation 40(5) requires that any data collected is deleted after these periods. Regulation 41 also sets out that personal data collected under the *Money Laundering Regulations* should only be processed for the purposes of preventing money laundering or terrorist financing.

Self-assessment questions:

- Can your firm retrieve records **promptly** in response to a Production Order?

- If the firm **relies on others** to carry out AML checks (see 'Reliance' in FCG Annex 1), is this within the limits permitted by the *Money Laundering Regulations*? How does it satisfy itself that it can rely on these firms?

Examples of good practice	Examples of poor practice
• Records of customer ID and transaction data can be **retrieved quickly and without delay**.	• The firm keeps customer records and related information in a way that **restricts** the **firm's access** to these records or their timely sharing with authorities.
• Where the firm routinely relies on checks done by a third party (for example, a fund provider relies on an IFA's checks), it **requests sample documents** to test their reliability.	• A firm cannot access CDD and related records for which it has relied on a third party. **This breaches the** *Money Laundering Regulations*.
	• Significant proportions of CDD records **cannot be retrieved** in good time.
	• The firm has not considered whether a **third party** consents to being relied upon.
	• There are **gaps** in customer records, which cannot be explained.

See regulations 28(16), 40 and 40(7) of the *Money Laundering Regulations*.

Countering the finance of terrorism

3.2.12 G Firms have an important role to play in providing information that can assist the authorities with counter-terrorism investigations. Many of the controls firms have in place in relation to terrorism will overlap with their anti-money laundering measures, covering, for example, risk assessment, customer due diligence checks, transaction monitoring, escalation of suspicions and liaison with the authorities.

Self-assessment questions:

•How have **risks** associated with terrorist finance been assessed? Did assessments consider, for example, risks associated with the customer base, geographical locations, product types, distribution channels, etc.?

•Is it clear who is responsible for **liaison with the authorities** on matters related to countering the finance of terrorism? (See ■ FCG 3.2.10G)

Examples of good practice	Examples of poor practice
• The firm has and uses an effective **process** for liaison with the authorities.	• Financial crime **training** does not mention terrorist financing.
• A firm identifies **sources of information** on terrorist financing risks: e.g. press reports, NCA alerts, Financial Action Task Force typologies, court judgements, etc.	• A firm doing cross-border business has not assessed terrorism-related risks in **countries** in which it has a presence or does business.

Examples of good practice	Examples of poor practice
• This information informs the design of **transaction monitoring systems**. • Suspicions raised within the firm inform its own **typologies**.	• A firm has not considered if its approach to **customer due diligence** is able to capture information relevant to the risks of terrorist finance.

Customer payments

3.2.13 G This section applies to banks subject to ■ SYSC 6.3.

Interbank payments can be abused by criminals. International policymakers have taken steps intended to increase the transparency of interbank payments, allowing law enforcement agencies to more easily trace payments related to, for example, drug trafficking or terrorism. The *Money Laundering Regulations* require banks to collect and attach information about payers and payees of wire transfers (such as names and addresses) to payment messages. Banks are also required to check this information is present on inbound payments, and chase missing data. The *FCA* has a legal responsibility to supervise banks' compliance with these requirements. Concerns have also been raised about interbank transfers known as "cover payments" (see ■ FCG Annex 1) that can be abused to disguise funds' origins. To address these concerns, the SWIFT payment messaging system now allows originator and beneficiary information to accompany these payments.

From 1 September 2023, similar obligations have applied for cryptoasset transfers undertaken by cryptoasset businesses registered with the *FCA* under the *Money Laundering Regulations*. This chapter may assist cryptoasset businesses in implementing this requirement but they should also have regard to specific expectations set out by the *FCA*. For further information, see www.fca.org.uk/news/statements/fca-sets-out-expectations-uk-cryptoasset-businesses-complying-travel-rule.

Self-assessment questions:

•How does your firm ensure that customer payment instructions contain **complete payer and payee information**? (For example, does it have appropriate procedures in place for checking payments it has received?)

•Does the firm review its **respondent banks'** track record on providing payer data and using appropriate SWIFT messages for cover payments?

•Does the firm use guidance issued by the ESAs? [**Editor's Note:** see http://www.eba.europa.eu/-/esas-provide-guidance-to-prevent-terrorist-financing-and-money-laundering-in-electronic-fund-transfers.].

Examples of good practice	Examples of poor practice
• Following processing, banks conduct **risk-based sampling** for inward payments to	• A bank fails to make use of the correct **SWIFT message type** for cover payments.

Examples of good practice	Examples of poor practice
identify inadequate payer and payee information.	
• An intermediary bank chases up **missing** information.	• Compliance with regulations related to international customer payments has not been reviewed by the firm's **internal audit** or compliance departments.
	The following practices breach the Funds Transfer Regulation:
• A bank sends dummy messages to test the effectiveness of filters.	International customer payment instructions sent by the payer's *bank* **lack meaningful payer and payee information**.
• A bank is aware of guidance from the **Basel Committee** and the **Wolfsberg Group** on the use of cover payments, and has considered how this should apply to its own operations.	An intermediary bank **strips** payee or payer information from payment instructions before passing the payment on.
• The quality of payer and payee information in payment instructions from **respondent banks** is taken into account in the bank's ongoing review of correspondent banking relationships.	The payee bank does not check any i**ncoming payments** to see if they include complete and meaningful data.
• The firm actively engages in **peer discussions** about taking appropriate action against banks which persistently fail to provide complete payer information.	

Case study – poor AML controls

3.2.14 G The *FSA* fined Alpari (UK) Ltd, an online provider of foreign exchange services, £140,000 in May 2010 for poor anti-money laundering controls.

- Alpari failed to carry out satisfactory customer due diligence procedures at the account opening stage and failed to monitor accounts adequately.
- These failings were particularly serious given that the firm did business over the internet and had customers from higher risk jurisdictions.

- The firm failed to ensure that resources in its compliance and anti-money laundering areas kept pace with the firm's significant growth.

Alpari's former money laundering reporting officer was also fined £14,000 for failing to fulfil his duties.

See the *FCA's* press release for more information: www.fca.org.uk/publication/final-notices/alpari.pdf.

Case studies – wire transfer failures

3.2.15 G A UK bank that falls short of our expectations when using payment messages does not just risk *FCA* enforcement action or prosecution; it can also face criminal sanctions abroad.

In January 2009, Lloyds TSB agreed to pay US$350m to US authorities after Lloyds offices in Britain and Dubai were discovered to be deliberately removing customer names and addresses from US wire transfers connected to countries or persons on US sanctions lists. The US Department of Justice concluded that Lloyds TSB staff removed this information to ensure payments would pass undetected through automatic filters at American financial institutions. See its press release: www.usdoj.gov/opa/pr/2009/January/09-crm-023.html.

In August 2010, Barclays Bank PLC agreed to pay US$298m to US authorities after it was found to have implemented practices designed to evade US sanctions for the benefit of sanctioned countries and persons, including by stripping information from payment messages that would have alerted US financial institutions about the true origins of the funds. The bank self-reported the breaches, which took place over a decade-long period from as early as the mid-1990s to September 2006. See the US Department of Justice's press release: www.justice.gov/opa/pr/2010/August/10-crm-933.html.

Case study – poor AML controls: PEPs and high risk customers

3.2.16 G The *FSA* fined Coutts & Company £8.75 million in March 2012 for poor AML systems and controls. Coutts failed to take reasonable care to establish and maintain effective anti-money laundering systems and controls in relation to their high risk customers, including in relation to customers who are Politically Exposed Persons.

- Coutts failed adequately to assess the level of money laundering risk posed by prospective and existing high risk customers.

- The firm failed to gather sufficient information to establish their high risk customers' source of funds and source of wealth, and to scrutinise appropriately the transactions of PEPs and other high risk accounts.

- The firm failed to ensure that resources in its compliance and anti-money laundering areas kept pace with the firm's significant growth.

These failings were serious, systemic and were allowed to persist for almost three years. They were particularly serious because Coutts is a high profile bank with a leading position in the private banking market, and because the weaknesses resulted in an unacceptable risk of handling the proceeds of crime.

This was the largest fine yet levied by the *FSA* for failures related to financial crime.

See the *FCA's* press release for more information: www.fca.org.uk/publication/final-notices/coutts-mar12.pdf .

Poor AML controls: risk assessment

3.2.17 G The *FSA* fined Habib Bank AG Zurich £525,000, and its MLRO £17,500, in May 2012 for poor AML systems and controls.

Habib Bank AG Zurich failed adequately to assess the level of money laundering risk associated with its business relationships. For example, the firm excluded higher risk jurisdictions from its list of high risk jurisdictions on the basis that it had group offices in them.

- Habib Bank AG Zurich failed to conduct timely and adequate enhanced due diligence on higher risk customers by failing to gather sufficient information and supporting evidence
- The firm also failed to carry out adequate reviews of its AML systems and controls.
- The MLRO failed properly to ensure the establishment and maintenance of adequate and effective anti- money laundering risk management systems and controls.

See the *FCA's* press release for more information: www.fca.org.uk/publication/final-notices/habib-bank.pdf.

3

3.3 Further guidance

3.3.1 G *FCTR* contains the following additional AML guidance:

- FCTR 4 summarises the findings of, and consolidates good and poor practice from, the *FSA's* thematic review of Automated Anti-Money Laundering Transaction Monitoring Systems

- FCTR 5 summarises the findings of, and consolidates good and poor practice from, the *FSA's* Review of firms' implementation of a risk-based approach to anti-money laundering (AML)

- FCTR 10 summarises the findings of the Small Firms Financial Crime Review. It contains guidance directed at small firms on:

  Regulatory/Legal obligations (FCTR 10.3.1G)

  Account opening procedures (FCTR 10.3.2G)

  Monitoring activity (FCTR 10.3.3G)

  Suspicious activity reporting (FCTR 10.3.4G)

  Records (FCTR 10.3.5G)

  Responsibilities and risk assessments (FCTR 10.3.7G)

- FCTR 12 summarises the findings of the *FSA's* thematic review of Banks' management of high money laundering risk situations. It includes guidance on:

  High risk customers and PEPs – AML policies and procedures (FCTR 12.3.2G)

  High risk customers and PEPs – Risk assessment (FCTR 12.3.3G)

  High risk customers and PEPs – Customer take-on (FCTR 12.3.4G)

  High risk customers and PEPs – Enhanced monitoring of high risk relationships (FCTR 12.3.5G)

  Correspondent banking – Risk assessment of respondent banks (FCTR 12.3.6G)

  Correspondent banking – Customer take-on (FCTR 12.3.7G)

  Correspondent banking – Ongoing monitoring of respondent accounts (FCTR 12.3.8G)

  Wire transfers – Paying banks (FCTR 12.3.9G)

  Wire transfers – Intermediary banks (FCTR 12.3.10G)

  Wire transfers – Beneficiary banks (FCTR 12.3.11G)

Wire transfers – Implementation of SWIFT MT202COV (■ FCTR 12.3.12G)

3.3.2 G *FCTR* also summarises the findings of the following thematic reviews:

- ■ FCTR 3: Review of private banks' anti-money laundering systems and controls
- ■ FCTR 7: Review of financial crime controls in offshore centres
- ■ FCTR 15: Banks' control of financial crime risks in trade finance (2013)

3

3.4 Sources of further information

3.4.1 G To find out more on **anti-money laundering**, see:

• The *Money Laundering Regulations*

The NCA's website, which contains information on how to report suspicions of money laundering: www.nationalcrimeagency.gov.uk

•The latest UK National Risk Assessment of money laundering and terrorist financing 2020 - www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2020

•The JMLSG's guidance on measures firms can take to meet their anti-money laundering obligations, which is available from its website:www.jmlsg.org.uk .

3.4.2 G To find out more on countering terrorist finance, see:

•Material relevant to terrorist financing that can be found throughout the JMLSG guidance: www.jmlsg.org.uk

•The European Supervisory Authorities (ESAs) have published risk factors guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849- https://www.eba.europa.eu/sites/default/files/documents/10180/1890686/66ec16d9-0c02-428b-a294-ad1e3d659e70/Final%20Guidelines%20on%20Risk%20Factors%20%28JC%202017%2037%29.pdf

•FATF's work on terrorist financing: http://www.fatf-gafi.org/publications/fatfgeneral/documents/terroristfinancing.html

3.4.3 G To find out more on customer payments, see:

•JMLSG guidance (www.jmlsg.org.uk/guidance/current-guidance/):

Sector 22 of Part II (Cryptoasset exchange providers and custodian wallet providers) and Annex 22-I of Part II (Cryptoassets Transfers ('Travel Rule')); and

Chapter 1 of Part III (Transparency in electronic payments (Wire transfers)), which will be banks' chief source of guidance on this topic.

•The Basel Committee's May 2009 paper on due diligence for cover payment messages: www.bis.org/publ/bcbs154.pdf

•The Wolfsberg Group's statement on payment standards: https://db.wolfsberg-group.org/assets/373dbb28-b518-4080-82cc-4be7a54aa16e/Wolfsberg%20Group%20Payment%20Transparency%20Standards%202023.pdf

•The *Money Laundering Regulations*

•*FCA* statement: www.fca.org.uk/news/statements/fca-sets-out-expectations-uk-cryptoasset-businesses-complying-travel-rule

3.4.4 G To find out more on correspondent banking relationships see:

•FATF Guidance on correspondent banking services (October 2016)- http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Correspondent-Banking-Services.pdf

•Basel Committee on Banking Supervision guidance "Sound management of risks related to money laundering and financing of terrorism: revisions" (updated July 2017) https://www.bis.org/bcbs/publ/d405.htm

3.4.5 G To find out more on proliferation financing, see:

•The UK National risk assessment of proliferation financing 2021: assets.publishing.service.gov.uk/media/65a01397e96df50014f844fe/Risk_assessment_of_proliferation_financing__1_.pdf

•FATF work on proliferation financing: www.fatf-gafi.org/en/topics/proliferation-financing.html

Chapter 4

Fraud

4

4.1 Introduction

4.1.1 G **Who should read this chapter?** This chapter applies to *all firms* subject to the financial crime rules in ■ SYSC 3.2.6R or ■ SYSC 6.1.1R and to *e-money institutions* and *payment institutions* within our supervisory scope, with the following exceptions:

1 • ■ FCG 4.2.2 applies only to *mortgage lenders* within our supervisory scope;

2 • ■ FCG 4.2.3 applies to *mortgage intermediaries* only; and

3 • ■ FCG 4.2.5 applies to *retail deposit takers* only.

4.1.2 G All firms must take steps to defend themselves against financial crime, but a variety of approaches is possible. This chapter provides guidance on themes that should form the basis of managing financial crime risk. The general topics outlined here are also relevant in the context of the specific financial crime risks detailed in subsequent chapters.

4.1.3 G The contents of *FCG's* fraud chapter reflect the *FSA's* previous thematic work in this area. This means it does not specifically address such topics as plastic card, cheque or insurance fraud. This is not because the *FCA* regards fraud prevention as unimportant. Rather it reflects our view that our limited resources are better directed elsewhere, given the strong incentive firms should have to protect themselves from fraud; and the number of other bodies active in fraud prevention. Links to some of these other bodies are provided in ■ FCG 4.4.

4

4.2 Themes

Preventing losses from fraud

4.2.1 G All firms will wish to protect themselves and their customers from fraud. Management oversight, risk assessment and fraud data will aid this, as will tailored controls on the ground. We expect a firm to consider the full implications of the breadth of fraud risks it faces, which may have wider effects on its reputation, its customers and the markets in which it operates.

The general guidance in ■ FCG 2 also applies in relation to fraud.

Self-assessment questions:

- What **information** do senior management receive about fraud trends? Are fraud losses accounted for clearly and separately to other losses?
- Does the firm have a clear picture of what parts of the business are **targeted by fraudsters**? Which **products, services and distribution channels** are vulnerable?
- How does the firm respond when reported fraud **increases**?
- Does the firm's investment in **anti-fraud systems** reflect fraud trends?

Examples of good practice	Examples of poor practice
• The firm takes a view on what areas of the firm are most **vulnerable** to fraudsters, and tailors defences accordingly.	• Senior management appear **unaware** of fraud incidents and trends. No management information is produced.
• Controls adapt to **new fraud threats**.	• **Fraud losses are buried** in bad debts or other losses.
• The firm engages with relevant **cross-industry efforts** to combat fraud (e.g. data-sharing initiatives like CIFAS and the Insurance Fraud Bureau, collaboration to strengthen payment systems, etc.) in relation to both internal and external fraud.	• There is no clear and consistent **definition** of fraud across the business, so reporting is haphazard.
• **Fraud response plans and investigation procedures** set out how the firm will respond to incidents of fraud.	• Fraud risks are not explored when **new products** and **delivery channels** are developed.

4

Examples of good practice	Examples of poor practice
• **Lessons** are learnt from incidents of fraud.	• Staff **lack awareness** of what constitutes fraudulent behaviour (e.g. for a salesman to misreport a customer's salary to secure a loan would be fraud).
• **Anti-fraud good practice** is shared widely within the firm.	• **Sales incentives** act to encourage staff or management to turn a blind eye to potential fraud.
• To guard against **insider fraud**, staff in high risk positions (e.g. finance department, trading floor) are subject to enhanced vetting and closer scrutiny. 'Four eyes' procedures (see FCG Annex 1 for common terms) are in place.	• Banks fail to implement the requirements of the **Payment Services Regulations** and **Banking Conduct of Business rules**, leaving customers out of pocket after fraudulent transactions are made.
• **Enhanced due diligence** is performed on higher risk customers (e.g. commercial customers with limited financial history. See 'long firm fraud' in FCG Annex 1).	• **Remuneration structures** may incentivise behaviour that increases the risk of mortgage fraud.
• Cryptoasset businesses **prescreen** outbound transactions for addresses **linked to fraud**.	

Mortgage fraud – lenders

4.2.2 G This section applies to mortgage lenders within the supervisory scope of the appropriate regulator.

Self-assessment questions:

•Are systems and controls to detect and prevent mortgage fraud **coordinated across the firm**, with resources allocated on the basis of an assessment of where they can be used to best effect?

•How does your firm contain the fraud risks posed by corrupt **conveyancers, brokers and valuers**?

•How and when does your firm engage with **cross-industry information-sharing exercises**?

Examples of good practice	Examples of poor practice
• A firm's underwriting process can **identify** applications that may present a **higher risk** of mortgage fraud.	• A lender fails to report relevant information to the *FCA's* **Information from Lenders (IFL)** scheme as per *FCA* guidance on IFL referrals.
• Membership of a lender's **panels** of brokers, conveyan	• A lender **lacks a clear definition** of mortgage fraud, un-

Examples of good practice	Examples of poor practice
cers and valuers is subject to ongoing review. Dormant third parties are identified.	dermining data collection and trend analysis.
• A lender **reviews existing mortgage books** to identify and assess mortgage fraud indicators.	• A lender's panels of conveyancers, brokers and valuers are **too large to be manageable**.
• A lender verifies that funds are being dispersed **in line with instructions** before it releases them.	• The lender does no work to identify **dormant parties**.
• A lender **promptly discharges** mortgages that have been redeemed and checks whether conveyancers register charges with the **Land Registry** in good time.	• A lender relies solely on the Financial Services Register when **vetting brokers**.
	• Underwriters' demanding work targets **undermine** efforts to contain mortgage fraud.

Mortgage fraud – intermediaries

4.2.3 G This section applies to mortgage intermediaries.

Self-assessment questions:

•does your firm satisfy itself that it is able to **recognise** mortgage fraud?

•When processing applications, does your firm consider whether the information the applicant provides is **consistent**? (For example, is declared income believable compared with stated employment? Is the value of the requested mortgage comparable with what your firm knows about the location of the property to be purchased?)

•What due diligence does your firm undertake on **introducers**?

Examples of good practice	Examples of poor practice
• Asking to see **original documentation** whether or not this is required by lenders.	• Failing to undertake due diligence on **introducers**.
• Using the *FCA's* **Information from Brokers** scheme to report intermediaries it suspects of involvement in mortgage fraud.	• Accepting all applicant information at **face value**.
	• Treating due diligence as the **lender's responsibility**.

Enforcement action against mortgage brokers

4.2.4 G Breaches the *FCA* has identified as part of enforcements actions against mortgage brokers have included:

- deliberately submitting to lenders applications containing false or misleading information; and
- failing to have adequate systems and controls in place to deal with the risk of mortgage fraud.

The *FCA* has referred numerous cases to law enforcement, a number of which have resulted in criminal convictions.

Investment fraud

4.2.5 G UK consumers are targeted by share-sale frauds and other scams including land-banking frauds, unauthorised collective investment schemes and Ponzi schemes. Customers of UK deposit-takers may fall victim to these frauds, or be complicit in them. We expect these risks to be considered as part of deposit-takers' risk assessments, and for this to inform management's decisions about the allocation of resources to a) the detection of fraudsters among the customer base and b) the protection of potential victims.

Self-assessment questions:

- Have the risks of investment fraud (and other frauds where customers and third parties suffer losses) been considered by the firm?
- Are resources allocated to mitigating these risks as the result of purposive decisions by management?
- Are the firm's anti-money laundering controls able to identify customers who are complicit in investment fraud?

Examples of good practice	Examples of poor practice
• A bank regularly assesses the risk to itself and its customers of losses from fraud, including investment fraud, in accordance with their established risk management framework. The risk assessment does not only cover situations where the bank could cover losses, but also where customers could lose and not be reimbursed by the bank. Resource allocation and mitigation measures are informed by this assessment.	• A bank has performed no risk assessment that considers the risk to customers from investment fraud.
• A bank contacts customers if it suspects a payment is being made to an investment fraudster.	• A bank fails to use actionable, credible information it has about known or suspected perpetrators of investment fraud in its financial crime prevention systems.

Examples of good practice	Examples of poor practice
• A bank has transaction monitoring rules designed to detect specific types of investment fraud. Investment fraud subject matter experts help set these rules.	• Ongoing monitoring of commercial accounts is allocated to customer-facing staff incentivised to bring in or retain business. • A bank allocates excessive numbers of commercial accounts to a staff member to monitor.

4

4.3 Further guidance

4.3.1 G *FCTR* contains the following additional material on fraud:

- FCTR 10 summarises the findings of the Small Firms Financial Crime Review. It contains guidance directed at small firms on:
  - Monitoring activity (FCTR 10.3.3G)
  - Responsibilities and risk assessments (FCTR 10.3.7G)
  - General fraud (FCTR 10.3.13G)
  - Insurance fraud (FCTR 10.3.14G)
  - Investment fraud (FCTR 10.3.15G)
  - Mortgage fraud (FCTR 10.3.16G)
  - Staff/Internal fraud (FCTR 10.3.17G)
- FCTR 11 summarises the findings of the *FSA's* thematic review Mortgage fraud against lenders. It contains guidance on:
  - Governance, culture and information sharing (FCTR 11.3.1G)
  - Applications processing and underwriting (FCTR 11.3.2G)
  - Mortgage fraud prevention, investigations, and recoveries (FCTR 11.3.3G)
  - Managing relationships with conveyancers, brokers and valuers (FCTR 11.3.4G)
  - Compliance and internal audit (FCTR 11.3.5G)
  - Staff recruitment and vetting (FCTR 11.3.6G)
  - Remuneration structures (FCTR 11.3.7G)
  - Staff training and awareness (FCTR 11.3.8G)
- FCTR 14 summarises the findings of the *FSA's* thematic review Banks' defences against investment fraud. It contains guidance directed at deposit-takers with retail customers on:
  - Governance (FCTR 14.3.2G)
  - Risk assessment (FCTR 14.3.3G)
  - Detecting perpetrators (FCTR 14.3.4G)
  - Automated monitoring (FCTR 14.3.5G)
  - Protecting victims (FCTR 14.3.6G)

Management reporting and escalation of suspicions (■ FCTR 14.3.7G)

Staff awareness (■ FCTR 14.3.8G)

Use of industry intelligence (■ FCTR 14.3.9G)

4.3.2 G ■ FCTR 2 summarises the *FSA's* thematic review Firms' high-level management of fraud risk.

4

4.4 Sources of further information

4.4.1 G To find out more about what *FCA* is doing about fraud, see:

- Details of the *FCA's* Information from Lenders scheme: https://www.fca.org.uk/firms/fraud/report-mortgage-fraud-lenders
- Details of the *FCA's* Information from Brokers scheme: https://www.fca.org.uk/firms/fraud/report-mortgage-fraud-advisers

4.4.2 G The list of other bodies engaged in counter-fraud activities is long, but more information is available from:

- Action Fraud, which is the UK's national fraud reporting centre: www.actionfraud.police.uk
- Fighting Fraud Action (FFA-UK) is responsible for leading the collective fight against financial fraud on behalf of the UK payments industry.
- The City of London Police, which has 'lead authority' status in the UK for the investigation of economic crime, including fraud https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/Pages/default.aspx
- The Fraud Advisory Panel, which acts as an independent voice and supporter of the counter fraud community: www.fraudadvisorypanel.org/

Chapter 5

Data security

5.1 Introduction

5.1.1 G **Who should read this chapter?** This chapter applies to **all firms** subject to the financial crime rules in ■ SYSC 3.2.6R or ■ SYSC 6.1.1R and to **e-money institutions** and **payment institutions** within our supervisory scope.

5.1.2 G Customers routinely entrust firms with important personal data; if this falls into criminal hands, fraudsters can attempt to undertake transactions in the customer's name. Firms must take special care of their customers' personal data, and comply with the data protection principles set out in Schedule 1 to the Data Protection Act 1998. The Information Commissioner's Office provides guidance on the Data Protection Act and the responsibilities it imposes on data controllers and processors. See section 4 and schedule 1 Data Protection Act 1998.

5.2 Themes

Governance

5.2.1 G The guidance in ■ FCG 2.2.1G on governance in relation to financial crime also applies to data security.

Firms should be alert to the financial crime risks associated with holding customer data and have written data security policies and procedures which are proportionate, accurate, up to date and relevant to the day-to-day work of staff.

Self-assessment questions:

- How is **responsibility** for data security apportioned?
- Has the firm ever **lost customer data**? If so, what remedial actions did it take? Did it contact customers? Did it review its systems?
- How does the firm monitor that **suppliers of outsourced services** treat customer data appropriately?
- Are data security standards set in **outsourcing** agreements, with suppliers' performance subject to monitoring?

Examples of good practice	Examples of poor practice
• There is a clear **figurehead** championing the issue of data security.	• The firm does not **contact customers** after their data is lost or compromised.
• Work, including by internal audit and compliance, is **coordinated** across the firm, with compliance, audit, HR, security and IT all playing a role.	• Data security is treated as an **IT** or **privacy issue**, without also recognising the financial crime risk.
• A firm's **plans to respond to data loss incidents** are clear and include notifying customers affected by data loss and offering advice to those customers about protective measures.	• A '**blame culture**' discourages staff from reporting data losses.
• A firm **monitors accounts** following a data loss to spot unusual transactions.	• The firm is unsure how its **third parties**, such as suppliers, protect customer data.
• The firm looks at **outsourcers'** data security practices before doing	

Examples of good practice	Examples of poor practice
business, and monitors compliance.	

Five fallacies of data loss and identity fraud

5.2.2 G

1. **'The customer data we hold is too limited or too piecemeal to be of value to fraudsters.'** This is misconceived: skilled fraudsters can supplement a small core of data by accessing several different public sources and use impersonation to encourage victims to reveal more. Ultimately, they build up enough information to pose successfully as their victim.

2. **'Only individuals with a high net worth are attractive targets for identity fraudsters.'** In fact, people of all ages, in all occupations and in all income groups are vulnerable if their data is lost.

3. **'Only large firms with millions of customers are likely to be targeted.'** Wrong. Even a small firm's customer database might be sold and re-sold for a substantial sum.

4. **'The threat to data security is external.'** This is not always the case. Insiders have more opportunity to steal customer data and may do so either to commit fraud themselves, or to pass it on to organised criminals.

5. **'No customer has ever notified us that their identity has been stolen, so our firm must be impervious to data breaches.'** The truth may be closer to the opposite: firms that successfully detect data loss do so because they have effective risk-management systems. Firms with weak controls or monitoring are likely to be oblivious to any loss. Furthermore, when fraud does occur, a victim rarely has the means to identify where their data was lost because data is held in so many places.

Controls

5.2.3 G

We expect firms to put in place systems and controls to minimise the risk that their operation and information assets might be exploited by thieves and fraudsters. Internal procedures such as IT controls and physical security measures should be designed to protect against **unauthorised access** to customer data.

Firms should note that we support the Information Commissioner's position that it is not appropriate for customer data to be taken off-site on laptops or other portable devices which are not encrypted.

Self-assessment questions:

- Is your firm's customer data taken **off-site**, whether by staff (sales people, those working from home) or third parties (suppliers, consultants, IT contractors etc)?

- If so, what **levels of security** exist? (For example, does the firm require automatic encryption of laptops that leave the premises, or measures to ensure no sensitive data is taken off-site? If customer

data is transferred electronically, does the firm use secure internet links?)

•How does the firm **keep track** of its digital assets?

•How does it **dispose** of documents, computers, and imaging equipment such as photocopiers that retain records of copies? Are accredited suppliers used to, for example, destroy documents and hard disks? How does the firm satisfy itself that data is disposed of competently?

•How are **access** to the premises and sensitive areas of the business **controlled**?

•When are **staff access rights** reviewed? (It is good practice to review them at least on recruitment, when staff change roles, and when they leave the firm.)

•Is there enhanced **vetting** of staff with access to lots of data?

•How are staff made aware of **data security risks**?

Examples of good practice	Examples of poor practice
• **Access** to sensitive areas (call centres, server rooms, filing rooms) is restricted.	• Staff and third party suppliers can access **data they do not need** for their role.
• The firm has **individual user accounts** for all systems containing customer data.	• Files are not **locked away**.
• The firm conducts risk-based, **proactive monitoring** to ensure employees' access to customer data is for a genuine business reason.	• Password standards are not robust and individuals **share passwords**.
• IT equipment is disposed of responsibly, e.g. by using a contractor **accredited** by the British Security Industry Association.	• The firm **fails to monitor** superusers or other staff with access to large amounts of customer data.
• Customer data in electronic form (e.g. on USB sticks, CDs, hard disks etc) is always **encrypted** when taken off-site.	• Computers are disposed of or transferred to new users without data being **wiped**.
• The firm understands what checks are done by **employment agencies** it uses.	• Staff working **remotely** do not dispose of customer data securely.
	• Staff handling large volumes of data also have access to **internet email**.
	• Managers assume staff understand data security risks and **provide no training**.
	• **Unencrypted** electronic data is distributed by post or courier.

Effective cyber practices

5.2.3A G Self-assessment questions:

•Are critical systems and data backed up, and do you test backup recovery processes regularly?

•Are you able to restore services in the event of an incident?

•Are network and computer security systems, software and applications kept up to date and regularly patched? Do you make sure your computer network and information systems are configured to prevent unauthorised access?

•How do you manage user and device credentials? Do you ensure that staff use strong passwords when logging on to hardware and software? Are the default administrator credentials for all devices changed?

•Is two-factor authentication used where the confidentiality of the data is most crucial?

•How do you protect sensitive data that is stored or in transit? Do you use encryption software to protect your critical information from unauthorised access?

Examples of good practice	Examples of good practice
	• Using weak or easy to guess passwords or creating passwords from familiar details.
• The firm carries out regular vulnerability assessments and patching.	• Poor physical management and/or control of devices.
• The firm carries out regular security testing.	• Not setting out appropriate user privileges on access to resources on the firm's network, data storages or applications.
• An application programming interface (API) allows different software to communicate with each other and has security measures in place.	• Not encrypting data at storage or between networks.
	• Not updating devices, software and operating systems with the latest security patches.
	• Not properly vetting third-party systems and vendors.

Examples of good practice	Examples of good practice
	• Not employing multi-factor authentication for devices, systems and services. • Insufficient staff training around social engineering and vishing and phishing campaigns.
• The firm is able to restore systems following an incident and restorations are done in a timely manner.	
	• Inadequate controls to revoke access for staff that leave the firm, the role or the department.

Case study – protecting customers' accounts from criminals

5.2.4 G In December 2007, the *FSA* fined Norwich Union Life £1.26m for failings in its anti-fraud systems and controls.

Firms should note that we support the Information Commissioner's position that it is not appropriate for customer data to be taken off-site on laptops or other portable devices which are not encrypted.

•Callers to Norwich Union Life call centres were able to satisfy the firm's caller identification procedures by providing public information to impersonate customers.

•Callers obtained access to customer information, including policy numbers and bank details and, using this information, were able to request amendments to Norwich Union Life records, including changing the addresses and bank account details recorded for those customers.

•The frauds were committed through a series of calls, often carried out in quick succession.

•Callers subsequently requested the surrender of customers' policies

. •Over the course of 2006, 74 policies totalling £3.3m were fraudulently surrendered.

•The firm failed to address issues highlighted by the frauds in an appropriate and timely manner even after they were identified by its own compliance department.

•Norwich Union Life's procedures were insufficiently clear as to who was responsible for the management of its response to these actual and attempted frauds. As a result, the firm did not give appropriate

priority to the financial crime risks when considering those risks against competing priorities such as customer service.

For more, see the *FCA's* press release: www.fca.org.uk/news/press-releases/fsa-fines-norwich-union-life-%C2%A3126m-exposing-its-customers-risk-fraud

Case study – data security failings

5.2.5 G In August 2010, the *FSA* fined Zurich Insurance plc, UK branch £2,275,000 following the loss of 46,000 policyholders' personal details.

5

- The firm failed to take reasonable care to ensure that it had effective systems and controls to manage the risks relating to the security of confidential customer information arising out of its outsourcing arrangement with another Zurich company in South Africa.

- It failed to carry out adequate due diligence on the data security procedures used by the South African company and its subcontractors.

- It relied on group policies without considering whether this was sufficient and did not determine for itself whether appropriate data security policies had been adequately implemented by the South African company.

- The firm failed to put in place proper reporting lines. While various members of senior management had responsibility for data security issues, there was no single data security manager with overall responsibility.

- The firm did not discover that the South African entity had lost an unencrypted back-up tape until a year after it happened.

The *FCA's* press release has more details: www.fca.org.uk/news/press-releases/fsa-fines-zurich-insurance-%C2%A32275000-following-loss-46000-policy-holders-personal

5.3 Further guidance

5.3.1 G *FCTR* contains the following additional material on data security:

- FCTR 6 summarises the findings of the *FSA's* thematic review of Data security in Financial Services and includes guidance on:
  - Governance (FCTR 6.3.1G)
  - Training and awareness (FCTR 6.3.2G)
  - Staff recruitment and vetting (FCTR 6.3.3G)
  - Controls – access rights (FCTR 6.3.4G)
  - Controls – passwords and user accounts (FCTR 6.3.5G)
  - Controls – monitoring access to customer data (FCTR 6.3.6G)
  - Controls – data back-up (FCTR 6.3.7G)
  - Controls – access to the internet and email (FCTR 6.3.8G)
  - Controls – key-logging devices (FCTR 6.3.9G)
  - Controls – laptop (FCTR 6.3.10G)
  - Controls – portable media including USB devices and CDs (FCTR 6.3.11G)
  - Physical security (FCTR 6.3.12G)
  - Disposal of customer data (FCTR 6.3.13G)
  - Managing third party suppliers (FCTR 6.3.14G)
  - Internal audit and compliance monitoring (FCTR 6.3.15G)
- FCTR 10 summarises the findings of the Small Firms Financial Crime Review, and contains guidance directed at small firms on:
  - Records (FCTR 10.3.5G)
  - Responsibilities and risk assessments (FCTR 10.3.7G)
  - Access to systems (FCTR 10.3.8G)
  - Outsourcing (FCTR 10.3.9G)
  - Physical controls (FCTR 10.3.10G)
  - Data disposal (FCTR 10.3.11G)
  - Data compromise incidents (FCTR 10.3.12G)

5.4 Sources of further information

5

5.4.1 G To find out more, see

- the website of the Information Commissioner's Office: www.ico.org.uk.

- National Cyber Security Centre, 10 Steps to Cyber Security: www.ncsc.gov.uk/collection/10-steps/data-security.

- National Cyber Security Centre, Cyber Security Toolkit for Boards: www.ncsc.gov.uk/collection/board-toolkit/introduction-to-cyber-security-for-board-members.

Chapter 6

Bribery and corruption

6.1 Introduction

6.1.1 G **Who should read this chapter?** This chapter applies to all firms subject to the financial crime rules in ■ SYSC 3.2.6R or ■ SYSC 6.1.1R and to e-money institutions and payment institutions within our supervisory scope.

6.1.2 G Bribery, whether committed in the UK or abroad, is a criminal offence under the Bribery Act 2010, which consolidates and replaces previous anti-bribery and corruption legislation. The Act introduces a new offence for commercial organisations of failing to prevent bribery. It is a defence for firms charged with this offence to show that they had adequate bribery-prevention procedures in place. The Ministry of Justice has published guidance on adequate anti-bribery procedures.

6.1.3 G The *FCA* does not enforce or give guidance on the Bribery Act. But:

- firms which are subject to our rules ■ SYSC 3.2.6R and ■ SYSC 6.1.1R are under a separate, regulatory obligation to establish and maintain effective systems and controls to mitigate financial crime risk; and
- e-money institutions and payment institutions must satisfy us that they have robust governance, effective risk procedures and adequate internal control mechanisms. See E-Money Reg 6 and Payment Service Reg 6.

6.1.4 G Financial crime risk includes the risk of corruption as well as bribery, and so is wider than the Bribery Act's scope. And we may take action against a firm with deficient anti-bribery and corruption systems and controls regardless of whether or not bribery or corruption has taken place. Principle 1 of our Principles for Business also requires authorised firms to conduct their business with integrity. See ■ PRIN 2.1.1R: Principle 1.

6.1.5 G So while we do not prosecute breaches of the Bribery Act, we have a strong interest in the anti-corruption systems and controls of firms we supervise, which is distinct from the Bribery Act's provisions. Firms should take this into account when considering the adequacy of their anti-bribery and corruption systems and controls.

6.2 Themes

Governance

6.2.1 G A firm's senior management are responsible for ensuring that the firm conducts its business with integrity and tackles the risk that the firm, or anyone acting on its behalf, engages in bribery and corruption. A firm's senior management should therefore be kept up-to-date with, and stay fully abreast of, bribery and corruption issues.

Self-assessment questions:

- What **role** do senior management play in the firm's anti-bribery and corruption effort? Do they approve and periodically review the strategies and policies for managing, monitoring and mitigating this risk? What steps do they take to ensure staff are aware of their interest in this area?

- Can your firm's board and senior management **demonstrate** a good understanding of the bribery and corruption risks faced by the firm, the materiality to its business and how to apply a risk-based approach to anti-bribery and corruption?

- How are **integrity** and **compliance** with relevant anti-corruption legislation considered when discussing **business opportunities**?

- What **information** do senior management receive in relation to bribery and corruption, and how frequently? Is it sufficient for senior management effectively to fulfil their functions in relation to anti-bribery and corruption?

Examples of good practice	Examples of poor practice
• The firm is committed to carrying out business fairly, honestly and openly.	• There is a lack of awareness of, or engagement in, anti-bribery and corruption at senior management or board level.
• Senior management lead by example in complying with the firm's anti-corruption policies and procedures.	• An 'ask no questions' culture sees management turn a blind eye to how new business is generated.
• Responsibility for anti-bribery and corruption systems and controls is clearly documented and apportioned to a single senior manager or a committee with appropriate terms of	• Little or no management information is sent to the board about existing and emerging bribery and corruption risks faced by the business, including: higher risk third-party re-

Examples of good practice	Examples of poor practice
reference and senior management membership who reports ultimately to the board.	lationships or payments; the systems and controls to mitigate those risks; the effectiveness of these systems and controls; and legal and regulatory developments.
• Anti-bribery systems and controls are subject to audit.	
• Management information submitted to the board ensures they are adequately informed of internal and external developments relevant to bribery and corruption and respond to these swiftly and effectively.	

6

Risk assessment

6.2.2 G The guidance in ■ FCG 2.2.4G on risk assessment in relation to financial crime also applies to bribery and corruption.

We expect firms to identify, assess and regularly review and update their bribery and corruption risks. Corruption risk is the risk of a firm, or anyone acting on the firm's behalf, engaging in corruption.

Self-assessment questions:

•How do you **define** bribery and corruption? Does your definition cover all forms of bribery and corrupt behaviour falling within the definition of 'financial crime' referred to in ■ SYSC 3.2.6R and ■ SYSC 6.1.1R or is it limited to 'bribery' as that term is defined in the Bribery Act 2010?

•Where is your firm **exposed** to bribery and corruption risk? (Have you considered risk associated with the products and services you offer, the customers and jurisdictions with which you do business, your exposure to public officials and public office holders and your own business practices, for example your approach to providing corporate hospitality, charitable and political donations and your use of third parties?)

•Has the risk of **staff** or **third parties** acting on the firm's behalf **offering** or **receiving bribes** or other corrupt advantage been assessed across the business?

•Who is **responsible** for carrying out a bribery and corruption risk assessment and keeping it up to date? Do they have sufficient levels of expertise and seniority?

Examples of good practice	Examples of poor practice
• Corruption risks are assessed in **all jurisdictions** where the firm operates and across all business channels.	• Departments responsible for identifying and assessing bribery and corruption risk are ill equipped to do so.

Examples of good practice	Examples of poor practice
• The firm considers factors that might lead business units to **downplay** the level of bribery and corruption risk to which they are exposed, such as lack of expertise or awareness, or potential conflicts of interest.	• For fear of harming the business, the firm classifies as low risk a jurisdiction generally associated with high risk. • The risk assessment is only based on generic, external sources.

Policies and procedures

6.2.3 G The guidance in ■ FCG 2.2.5G on policies and procedures in relation to financial crime and in ■ FCG 2.2.6G on staff recruitment, vetting, training, awareness and remuneration also applies to bribery and corruption.

Firms' policies and procedures to reduce their financial crime risk must cover corruption and bribery.

Self-assessment questions:

•Do your anti-bribery and corruption policies adequately address all areas of **bribery and corruption risk** to which your firm is exposed, either in a stand-alone document or as part of separate policies? (for example, do your policies and procedures cover: expected standards of behaviour; escalation processes; conflicts of interest; expenses, gifts and hospitality; the use of third parties to win business; whistleblowing; monitoring and review mechanisms; and disciplinary sanctions for breaches?)

•Have you considered the extent to which **corporate hospitality** might influence, or be perceived to influence, a business decision? Do you impose and enforce limits that are appropriate to your business and proportionate to the bribery and corruption risk associated with your business relationships?

•How do you satisfy yourself that your anti-corruption policies and procedures are applied effectively?

•How do your firm's policies and procedures help it to identify whether someone acting on behalf of the firm is corrupt?

•How does your firm react to suspicions or allegations of bribery or corruption involving people with whom the firm is connected?

Examples of good practice	Examples of poor practice
• The firm **clearly sets out** behaviour expected of those acting on its behalf. • There are **unambiguous consequences** for breaches of the firm's anti-corruption policy.	• The firm **does not assess** the extent to which staff comply with its anti-corruption policies and procedures. • The firm's anti-corruption policies and procedures are **out of date**.

Examples of good practice	Examples of poor practice
• Risk-based, appropriate additional monitoring and due diligence are undertaken for jurisdictions, sectors and business relationships identified as **higher risk**.	• A firm relies on passages in the staff code of conduct that prohibit improper payments, but has no other **controls**.
• Staff responsible for implementing and monitoring anti-bribery and corruption policies and procedures have adequate levels of **anti-corruption expertise**.	• The firm does not **record** corporate hospitality given or received.
• Where appropriate, the firm refers to existing sources of information, such as expense registers, policy queries and whistleblowing and complaints hotlines, to monitor the effectiveness of its anti-bribery and corruption policies and procedures.	• The firm **does not respond** to external events that may highlight weaknesses in its anti-corruption systems and controls.
• **Political and charitable donations** are subject to appropriate due diligence and are approved at an appropriate management level, with compliance input.	• The firm fails to consider whether clients or charities who stand to benefit from corporate hospitality or donations have **links to relevant political or administrative decision-makers**.
• Firms who do not provide staff with access to whistleblowing hotlines have processes in place to allow staff to **raise concerns in confidence or, where possible, anonymously**, with adequate levels of protection.	• The firm fails to maintain **records of incidents and complaints**.

See ■ SYSC 3.2.6R and ■ SYSC 6.1.1R.

Dealing with third parties

6.2.4 G We expect firms to take adequate and risk-sensitive measures to address the risk that a third party acting on behalf of the firm may engage in corruption.

Self-assessment questions:

•Do your firm's policies and procedures **clearly define** 'third party'?

•Do you **know** your third party?

•What is your firm's policy on **selecting** third parties? How do you check whether it is being followed?

•To what extent are third-party relationships **monitored** and **reviewed**? Is the frequency and depth of the monitoring and review commensurate to the risk associated with the relationship?

•Is the **extent** of due diligence on third parties determined on a risk-sensitive basis? Do you seek to identify any bribery and corruption issues as part of your due diligence work, e.g. negative allegations against the third party or any political connections? Is due diligence applied consistently when establishing and reviewing third-party relationships?

•Is the risk assessment and due diligence information **kept up to date**? How?

•Do you have effective systems and controls in place to ensure **payments** to third parties are in line with what is both expected and approved?

Examples of good practice	Examples of poor practice
• Where a firm uses third parties to generate business, these relationships are subject to **thorough due diligence** and management oversight.	• A firm using intermediaries fails to satisfy itself that those businesses have **adequate controls** to detect and prevent where staff have used bribery to generate business.
• The firm reviews in sufficient detail its relationships with third parties on a regular basis to confirm that it is still necessary and appropriate to **continue with the relationship**.	• The firm fails to establish and record an **adequate commercial rationale** to support its payments to overseas third parties. For example, why it is necessary to use a third party to win business and what services would the third party provide to the firm?
• Third parties are paid **directly** for their work.	• The firm is **unable to produce a list** of approved third parties, associated due diligence and details of payments made to them.
• The firm includes **specific anti-bribery and corruption clauses** in contracts with third parties.	• The firm does not discourage the giving or receipt of **cash gifts**.
• The firm provides **anti-bribery and corruption training** to third parties where appropriate.	• There is **no checking** of compliance's operational role in approving new third-party relationships and accounts.
• The firm **reviews and monitors** payments to third parties. It records the purpose of third-party payments.	• A firm **assumes** that long-standing third-party relationships present no bribery or corruption risk.
• There are higher or extra levels of due diligence and ap-	• A firm relies exclusively on **informal** means to assess the

Examples of good practice	Examples of poor practice
proval for **high risk third-party relationships**.	bribery and corruption risks associated with third parties, such as staff's personal knowledge of the relationship with the overseas third parties.
• There is appropriate **scrutiny** of and **approval** for relationships with third parties that introduce business to the firm.	
• The firm's compliance function has **oversight** of all third-party relationships and monitors this list to identify risk indicators, for example a third party's political or public service connections.	

Case study – corruption risk

6.2.5 G In 2020, the *FCA* and the *PRA* fined Goldman Sachs International a total of £96.6m (US$126m) for risk management failures connected to a Malaysian development company ('the company') and its role in 3 fundraising transactions for the company.

The bank failed to assess and manage risk to the standard that was required given the high-risk profile of the transactions and failed to assess risk factors on a sufficiently holistic basis. The bank also failed to address allegations of bribery in 2013 and failed to manage allegations of misconduct in connection with the company in 2015.

The bank breached a number of *FCA* and *PRA* principles and *rules*. In particular, the bank failed to:

- assess with due skill, care and diligence the risk factors that arose in each of the bond transactions on a sufficiently holistic basis;
- assess and manage the risk of the involvement in the bond transactions of a third party about which the bank had serious concerns;
- exercise due skill, care and diligence when managing allegations of bribery and misconduct in connection with the company and the third bond transaction; and
- record in sufficient detail the assessment and management of risk associated with the company bond transactions.

See the *FCA's* press release: www.fca.org.uk/news/press-releases/fca-pra-fine-goldman-sachs-international-risk-management-failures-1mdb.

Case study – inadequate anti-bribery and corruption systems and controls

6.2.6 G In July 2011, the *FSA* fined Willis Limited, an insurance intermediary, £6.9m for failing to take appropriate steps to ensure that payments made to overseas third parties were not used for corrupt purposes. Between January

2005 and December 2009, Willis Limited made payments totalling £27m to overseas third parties who helped win and retain business from overseas clients, particularly in high risk jurisdictions.

Willis had introduced anti-bribery and corruption policies in 2008, reviewed how its new policies were operating in practice and revised its guidance as a result in May 2009. But it should have taken additional steps to ensure they were adequately implemented.

- Willis failed to ensure that it established and recorded an adequate commercial rationale to support its payments to overseas third parties.

- It did not ensure that adequate due diligence was carried out on overseas third parties to evaluate the risk involved in doing business with them.

- It failed to review in sufficient detail its relationships with overseas third parties on a regular basis to confirm whether it was necessary and appropriate to continue with the relationship.

- It did not adequately monitor its staff to ensure that each time it engaged an overseas third party an adequate commercial rationale had been recorded and that sufficient due diligence had been carried out.

See the *FCA's* press release: www.fca.org.uk/news/press-releases/fsa-fines-willis-limited-%C2%A36895-million-anti-bribery-and-corruption-systems-and.

Case study – third parties

6.2.7 G In 2022, the *FCA* fined JLT Speciality Limited £7,881,700 for financial crime control failings, which in one instance allowed bribery of over $3m to take place. The firm failed to consider whether additional safeguards or approvals should be incorporated into processes in respect to overseas introducers engaged by another group entity, where the introduced business was placed by the firm in the London market. Among other issues, the firm's third-party risk assessments failed to:

- ensure that information held by employees who were either involved in negotiating the relationship with the third party or placing the business in the London market, including potential red flags, was brought to the attention of the company's 'know your customer' subcommittee or its financial crime team;

- ensure that the other entity disclosed all material information about the third party to the financial crime team for review, consideration and action as necessary; and

- consider whether additional monitoring and oversight of third parties, in accordance with the firm's process, was appropriate.

See the *FCA's* press release: www.fca.org.uk/news/press-releases/jlt-specialty-limited-fined-7.8m-pounds-financial-crime-control-failings.

6.3 Further guidance

6.3.1 G *FCTR* contains the following additional material on bribery and corruption:

- FCTR 9 summarises the findings of the *FSA's* thematic review Anti-bribery and corruption in commercial insurance broking and includes guidance on:
  - Governance and management information (FCTR 9.3.1G)
  - Risk assessment and responses to significant bribery and corruption events (FCTR 9.3.2G)
  - Due diligence on third-party relationships (FCTR 9.3.3G)
  - Payment controls (FCTR 9.3.4G)
  - Staff recruitment and vetting (FCTR 9.3.5G)
  - Training and awareness (FCTR 9.3.6G)
  - Risk arising from remuneration structures (FCTR 9.3.7G)
  - Incident reporting (FCTR 9.3.8G)
  - The role of compliance and internal audit (FCTR 9.3.9G)
- FCTR 13 summarises the findings of the *FSA's* thematic review on Anti-bribery and corruption systems and controls in investment banks and includes guidance on:
  - Governance and management information (FCTR 13.3.2G)
  - Assessing bribery and corruption risk (FCTR 13.3.3G)
  - Policies and procedures (FCTR 13.3.4G)
  - Third party relationships and due diligence (FCTR 13.3.5G)
  - Payment controls (FCTR 13.3.6G)
  - Gifts and hospitality (FCTR 13.3.7G)
  - Staff recruitment and vetting (FCTR 13.3.8G)
  - Training and awareness (FCTR 13.3.9G)
  - Remuneration structures (FCTR 13.3.10G)
  - Incident reporting and management (FCTR 13.3.11G)

6.4 Sources of further information

6.4.1 G To find out more, see:

- The Bribery Act 2010: www.legislation.gov.uk/ukpga/2010/23/contents

- The Ministry of Justice's guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing: https://assets.publishing.service.gov.uk/media/5d80cfc3ed915d51e9aff85a/bribery-act-2010-guidance.pdf (full version) https://assets.publishing.service.gov.uk/media/5d80cfd5ed915d5257b5b693/bribery-act-2010-quick-start-guide.pdf (quick start guide)

- Our one-minute guide for smaller firms on anti-bribery and corruption: https://www.fca.org.uk/firms/financial-crime/bribery-corruption

Chapter 7

Sanctions, asset freezes and proliferation financing

7.1 Introduction

7

7.1.1 G **Who should read this chapter?** All firms are required to comply with UK financial sanctions. The *FCA's* role is to ensure that the firms it supervises have adequate systems and controls to do so. As such, this chapter applies to **all firms** subject to the financial crime rules in ■ SYSC 3.2.6R or ■ SYSC 6.1.1R. It also applies to **e-money institutions and payment institutions and the cryptoasset sector** within our supervisory scope.

7.1.2 G Firms' systems and controls should also address, where relevant, the risks they face from weapons proliferators, although these risks will be very low for the majority of *FCA*-supervised firms. ■ FCG 7.2.5G, which looks at weapons proliferation, applies to all firms subject to our supervision.

7.1.3 G [deleted]

7.1.4 G Financial sanctions are restrictions put in place by the UK government or the multilateral organisations that limit the provision of certain financial services or restrict access to financial markets, funds and economic resources in order to achieve a specific foreign policy or national security objective.

7.1.5 G All individuals and legal entities who are within or undertake activities within the UK's territory must comply with the UK financial sanctions that are in force. All UK nationals and UK legal entities established under UK law, including their branches, must also comply with UK financial sanctions that are in force, irrespective of where their activities take place.

Under *Principle* 11 (■ PRIN 2.1.1R), we expect authorised firms to notify us if they (or their group companies, *approved persons*, *senior management functions*, *appointed representatives* and *agents*) are targets **of UK** sanctions **or those of any other country or jurisdiction**.

For firms such as *electronic money institutions*, payment services firms, *cryptoasset businesses* and Annex I financial institutions, this is regarded as a material change of circumstance and we expect to be informed if you or any connected entities are **targets of UK** sanctions **or those of any other country or jurisdiction**.

7.1.5A G The Office of Financial Sanctions (OFSI) within the Treasury helps to ensure that financial sanctions are properly understood, implemented and enforced in the United Kingdom. HM Government publishes the UK Sanctions List, which provides details of those designated under regulations made under the Sanctions and Anti-Money Laundering Act. The list also details which

sanctions measures apply to these persons or ships. OFSI maintains a Consolidated List of financial sanctions targets designated by the United Nations and the United Kingdom, which is available from its website. If firms become aware of a breach, they must notify OFSI in accordance with the relevant provisions. OFSI have published guidance on complying with UK obligations and this is available on their website. See https://www.gov.uk/government/publications/financial-sanctions-faqs.

Firms should also consider whether they should report sanctions breaches to the *FCA*. ■ SUP 15.3 contains general notification requirements. Firms are required to tell us, for example, about significant rule breaches (see ■ SUP 15.3.11R(1)). Firms should therefore consider whether a sanctions breach is the result of any matter within the scope of ■ SUP 15.3 – for example, a significant failure in their financial crime systems and controls.

7.1.6 G Alongside financial sanctions, the government imposes controls on certain types of trade. As part of this, the export of goods and services for use in nuclear, radiological, chemical or biological weapons programmes is subject to strict controls. Proliferators seek to gain access to this technology illegally: aiding them is an offence under the Anti-Terrorism, Crime and Security Act 2001. Note that the Treasury can also use powers under the Counter Terrorism Act 2008 (see ■ FCG Annex 1) to direct financial firms to, say, cease business with certain customers involved in proliferation activity.

7.2 Themes

7.2.-1 G The guidance set out in ■ FCG 2.2 (Themes) and ■ FCG 2.3 (Further guidance) also applies to sanctions.

Governance

7

7.2.1 G The guidance in ■ FCG 2.2.1G on governance in relation to financial crime also applies to sanctions.

We expect senior management to take clear responsibility for managing sanctions risks, which should be treated in the same manner as other risks faced by the business. There should be evidence that senior management are actively engaged in the firm's approach to addressing the risks of non-compliance with UK financial sanctions. Where they identify gaps, they should remediate them.

Self-assessment questions:

- Has your firm **clearly allocated** responsibility for adherence to the sanctions regime? To whom?
- How does the firm **monitor performance**? (For example, statistical or narrative reports on matches or breaches.)
- How are **senior management** kept **up to date** with sanctions compliance issues?
- Does the firm's organisational structure with respect to sanctions compliance across **different jurisdictions** promote a **coordinated approach and accountability**?
- Does the firm have **evidence** that sanctions issues are **escalated** where warranted?
- Where sanctions controls processes rely on resource external to the firm, is there **appropriate oversight** and **understanding** of that resource?

Examples of good practice	Examples of poor practice
• An individual of **sufficient authority** is responsible for overseeing the firm's adherence to UK sanctions.	• The firm believes payments to sanctioned individuals and entities are **permitted** when the sums are small. Without a licence from the OFSI, this could be a **criminal offence**.

Examples of good practice	Examples of poor practice
	• Multinational firms **lack** the **communication** between global and regional sanctions teams necessary to **manage** compliance with UK sanctions laws, regulations and guidance.
• It is clear **at what stage customers are screened** in different situations (e.g. when customers are passed from agents or other companies in the group).	• No **internal audit** resource is allocated to monitoring sanctions compliance.
• There is **appropriate escalation** of actual target matches and breaches of UK sanctions. Notifications are timely.	• Some business units in a large organisation think they are **exempt**.

The offence will depend on the sanctions provisions breached.

Management information (MI)

7.2.1A G The guidance in ■ FCG 2.2.2G on MI in relation to financial crime also applies to sanctions.

Senior management should be sufficiently aware of the firm's obligations regarding sanctions to enable them to discharge their functions effectively.

Self-assessment questions:

- How does your firm **monitor performance**? (For example, statistical or narrative reports on matches or breaches.)
- Does **regular and ad hoc MI** provide senior management with a clear understanding of the firm's sanctions compliance risk?
- Is the MI produced relevant to UK sanctions?

Risk assessment

7.2.2 G The guidance in ■ FCG 2.2.4G on risk assessment in relation to financial crime also applies to sanctions and proliferation financing (PF) (see ■ FCG 7.2.5G for PF).

A firm should consider which areas of its business;

- are most likely to provide services or resources to individuals or entities on the Consolidated List;
- are owned and controlled by individuals or entities on the Consolidated List;
- engage in services or transactions prohibited under UK financial sanctions; or
- rely on prohibited suppliers, intermediaries or counterparties.

Self-assessment questions:

•Does your firm have a **clear view** on where within the firm **potential sanctions breaches** are most likely to occur? (This may cover different business lines, sales channels, customer types, geographical locations, etc.)

•How is the risk assessment **kept up to date**, particularly after the firm enters a new jurisdiction or introduces a new product or where **it has identified new sanctions risk events**?

•Has senior management set a clear **risk appetite** in relation to its sanctions risks, including in its exposure to sanctioned persons, activities and **jurisdictions**?

•Does your firm have established **risk metrics** to help detect and manage its sanctions compliance exposure on an ongoing basis?

•Are there established **procedures** to identify and escalate new sanctions risk events, such as new sanctions regimes, sanctioned activities and evasion typologies?

•Is your firm utilising available guidance and resources on **new and emerging** sanctions evasion typologies?

Examples of good practice	Examples of poor practice
• A firm with international operations, or that deals in currencies other than sterling, understands the requirements of relevant **local financial sanctions regimes**.	• There is **no process** for updating the risk assessment.
• A small firm is **aware** of the sanctions regime and where it is most vulnerable, even if risk assessment is only informal.	• The firm assumes financial sanctions **only apply to money transfers** and so has not assessed its risks.
• The firm conducts **contingency planning**, taking a proactive approach to identifying sanctions exposure and is conducting exposure assessments and scenario planning. The firm updates business-wide and customer risk assessments to **account for changes** in the nature and type of sanctions measures.	
• The firm **performs lessons learned** exercises following material sanctions developments to improve its readiness to respond to future events.	
• The firm engages with **public-private partnerships and private-private partnerships** to gather insights on the latest typologies and additional controls that might be relevant	

Examples of good practice	Examples of poor practice
and share its own best practice examples.	

Customer due diligence checks

7.2.2A G As well as being relevant to other financial crime controls, effective customer due diligence (CDD) and know your customer (KYC) assessments are a cornerstone of effective compliance with sanctions requirements.

Examples of good practice	Examples of poor practice
• Sanctions risk is **proactively** included into the firm's CDD process.	• The firm has **low-quality** CDD and KYC assessments and **review backlogs**, raising the risk of not identifying sanctioned individuals and entities.
• The firm's CDD identifies **all parties** relevant for its screening processes.	• The firm's CDD processes are **unable to identify** connected parties and corporate structures that may be subject to sanctions.
• The firm's customer onboarding and due diligence processes **are designed to identify** customers who make use of **corporate vehicles** to obscure ownership or source of funds.	• The firm's CDD **does not articulate** full ownership structures of entities and the firm is unable to show that it is screening all relevant parties.
• The firm **has processes designed** to **identify** activity that is **not in line with the customer profile** or is otherwise **suspicious**.	

7.2.2B G Further guidance on good and bad practice relating to CDD checks can be found in ■ FCG 3.2.4G.

7.2.3 G A firm should have effective, up-to-date screening systems appropriate to the nature, size and risk of its business. Although screening itself is not a legal requirement, screening new customers, counterparties to transactions and payments against the Consolidated List, and screening existing customers when new names are added to the list, helps to ensure that firms will not breach UK sanctions.

Self-assessment questions:

•When are customers screened against **lists**, whether the Consolidated List, internal watchlists maintained by the firm, or lists from commercial providers? (Screening should take place at the time of customer take-on. Good reasons are needed to justify the risk posed by retrospective screening, such as the existence of general licences.)

•If a customer was **referred** to the firm, how does the firm ensure the person is not listed? (Does the firm screen the customer against the list itself, or does it seek assurances from the referring party?)

•How does the firm become **aware of changes** to the Consolidated List? (Are there manual or automated systems? Are customer lists rescreened after each update is issued?)

•Does your firm have a **clear policy** on which customers, counterparties and payments are subject to screening, and what related data is subject to screening?

•Does your firm have **service level agreements** that cover how quickly it updates its sanctions screening lists following updates to the Consolidated List and that are appropriate to the sanctions risks of its business?

•Does your firm **evaluate** its **screening capabilities** so that its screening system is adequately calibrated for its needs and to monitor UK sanctions? Do you regularly **test/measure** the effectiveness of the system?

•Is the team responsible for sanctions compliance properly **resourced and skilled** to effectively perform sanctions screening **and alert management**?

•If using an outsourced service, does your firm have appropriate **control and oversight** of its sanctions screening controls?

Examples of good practice	Examples of poor practice
• The firm has considered what **mixture** of manual and automated screening is most appropriate.	• The firm assumes that an intermediary has screened a customer, but **does not check** this.
• There are quality control checks over **manual screening**.	• Where a firm uses automated systems, it does not understand how to **calibrate** them and does not check whether the number of hits is unexpectedly high or low.
• The firm **understands its automated** screening tool and how it is calibrated, and is able to demonstrate that it is appropriate to the firm's risk exposure.	• Calibration is **not adequately tailored** and the system is either too sensitive or not sensitive enough. This may result in name variations not being detected, for example.
• The firm is able to show the controls in place to **measure the effectiveness** of **its auto**	• There is **limited or no understanding** by the firm about how a third-party tool is calib-

Examples of good practice	Examples of poor practice
mated system, thresholds and parameters – for instance, with sample testing and tuning.	rated and when lists are updated.
• Where a firm uses automated systems these can make **'fuzzy matches'** (e.g. able to identify similar or variant spellings of names, name reversal, digit rotation, character manipulation, etc.). The firm continually seeks ways to enhance the system to help identify **potential** sanctions **breaches**.	• An insurance company **only screens when claims** are made on a policy.
• The firm screens customers' **directors** and known **beneficial owners** on a risk-sensitive basis.	• Screening of customer databases is a **one-off** exercise.
• Where the firm maintains an account for a listed individual or entity, the status of this account is **clearly flagged** to staff.	• Updating from the Consolidated List is **haphazard**. Some business units use out-of-date lists.
• A firm only relies on **other firms' screening** (such as outsourcers or intermediaries) after taking steps to satisfy itself this is appropriate.	• The firm is **overly reliant** on a third-party provider screening solution, with no oversight. The firm has **no means** of monitoring payment instructions.
• The screening tool is **calibrated and tailored** to the firm's **risk** and **is** appropriate for **screening UK sanctions**. Customers and their transactions are screened against relevant updated sanctions lists and effective re-screening is in place to identify activity that may indicate sanctions breaches.	
• Where **blockchain analytics** solutions are deployed, the firm ensures that compliance teams **understand** how these capabilities can be best used to identify transactions linked to higher risk wallet addresses, **including those included on the Consolidated List**.	
• The firm's sanctions teams are adequately **resourced** to avoid backlogs in sanctions screening and are able to react to those at pace.	• The firm **lacks proper resources** and **expertise** to ensure effective screening **and investigation of alerts**. It has significant backlogs and faces the risk of non-compliance with its obligations.

Examples of good practice	Examples of poor practice
	• Increased volumes and pressure on sanctions teams **following changes in the sanctions landscape prevent** firms from taking **appropriate and timely action** for true positive alerts and increase the risk of errors. There is a lack of clarity around prioritisation of alerts, internal service level agreements and governance.

Evasion detection and investigation

7.2.3A G

A firm should have effective, up-to-date screening systems appropriate to the nature, size and risk of its business. However, simple screening of names against the Consolidated List may not always identify potential sanctions evasion involving third parties and alternative detection techniques may be needed. **Potential red flags for sanctions evasion are set out in alerts issued by the National Economic Crime Centre (NECC)**.

Self-assessment questions:

•Does your firm understand potential sanctions **evasion typologies** relevant to its business and has it considered how to detect them?

•Has your firm considered whether **additional procedures are needed** to identify potential sanctions evasion?

Examples of good practice	Examples of poor practice
• The firm is using techniques, such as data analytics, to identify customers who may be close associates or dependents or have transactional links with designated persons, and so may **represent a higher risk** of sanctions non-compliance.	

Asset freezing and licenses

7.2.3B G

When a financial sanction is an asset freeze, the funds and economic resources belonging to or owned, held or controlled by a designated person are generally to be frozen immediately by the person in possession or control of them, unless there is an exception in the legislation they can rely on, or they have a licence from OFSI.

Self-assessment questions:

•Does your firm have **clear policies and procedures** as to when funds and economic resources are frozen or released?

•Have you assessed how any frozen funds and economic resources in your firm's possession or control are **maintained in compliance** with UK sanctions?

•Does your firm have clear policies and procedures to **assess, utilise and monitor** the use of OFSI licences and statutory exceptions?

Reporting and assessing potential sanctions breaches

7.2.3C G Relevant firms are required to report to OFSI where they know or have reasonable cause to suspect a breach of financial sanctions, and notify OFSI if:

•a person they are dealing with, directly or indirectly, is a designated person;

•they hold any frozen assets; or

•they discover or suspect any breach while conducting their business.

In line with *Principle* 11, ■ SUP 15.3.8G(2) and ■ FCG 7, firms must consider whether they need to notify us – for example, whether potential breaches of sanctions resulted from a significant failure in their systems and controls.

Self-assessment questions:

•Is there a clear procedure that sets out what to do if a potential **sanctions breach** is identified? (This might cover, for example, alerting senior management, OFSI and the *FCA*, and giving consideration to whether to submit a Suspicious Activity Report).

•Does your firm consider the **root causes** of any potential sanctions breaches and consider the implications for its policies and procedures?

Examples of good practice	Examples of poor practice
• The firm undertakes **a root cause analysis** of potential sanctions breaches and uses them to update its sanctions controls.	• The firm **does not report a breach** of financial sanctions to OFSI **when required to do so**. This could be a criminal offence.
• After a breach, as well as meeting its formal obligation **to notify OFSI**, the firm **reports the breach to the FCA**. SUP 15.3 contains general notification requirements. Firms are required to tell us about significant *rule* breaches (see SUP 15.3.11R(1)), such as a significant failure in their financial	

Examples of good practice	Examples of poor practice
crime systems and controls.	
• **Significant deficiencies in the firm's systems and controls resulting in potential sanctions breaches are reported** to the *FCA*.	

Matches and escalation

7.2.4 G When a customer's name matches a person on the Consolidated List it will often be a 'false positive' (e.g. a customer has the same or similar name but is not the same person). Firms should have procedures for identifying where name matches are real and for freezing assets where this is appropriate.

Self-assessment questions:

•What steps does your firm take to identify whether **a name match is real**? (For example, does the firm look at a range of identifier information such as name, date of birth, address or other customer data?)

•Is there a **clear procedure** if there is a breach? (This might cover, for example, alerting senior management, the Treasury and the *FCA*, and giving consideration to a Suspicious Activity Report.)

Examples of good practice	Examples of poor practice
• Sufficient resources are available to identify '**false positives**'.	• The firm **does not report a breach** of the financial sanctions regime to OFSI: **this could be a criminal offence**.
• After a breach, as well as meeting its formal obligation to notify **OFSI**, the firm considers whether it should report the breach to the *FCA*. SUP 15.3 contains general notification requirements. Firms are required to tell us, for example, about significant rule breaches (see SUP 15.3.11R(1)). Firms should therefore consider whether the breach is the result of any matter within the scope of SUP 15.3, for example a significant failure in their financial crime systems and controls.	• An account is **not frozen** when a match with the Consolidated List is identified. If, as a consequence, funds held, owned or controlled by a designated person are dealt with or made available to the designated person, **this could be a criminal offence**.
	• A **lack of resources** prevents a firm from **adequately analysing** matches.

Examples of good practice	Examples of poor practice
	• **No audit trail** of decisions where potential target matches are judged to be false positives.

The offence will depend on the sanctions provisions breached.

Weapons proliferation

7.2.5 G Alongside financial sanctions, the government imposes controls on certain types of trade in order to achieve foreign policy objectives. The export of goods and services for use in nuclear, radiological, chemical or biological weapons programmes is subject to strict controls. Firms' systems and controls and policies and procedures should address and mitigate the proliferation risks they face. Firms are also required to carry out proliferation financing risk assessments under regulation 18A of the *Money Laundering Regulations*, either as part of the existing practice-wide risk assessment or as a standalone document.

Self-assessment questions:

•Does your firm finance trade with **high risk countries**? If so, is **enhanced due diligence** carried out on counterparties and goods? Where doubt remains, is evidence sought from exporters that the trade is legitimate?

•Does your firm have **customers from high risk countries**, or with a history of dealing with individuals and entities from such places? If so, has the firm reviewed how the sanctions situation could affect such counterparties, and discussed with them how they may be affected by relevant regulations?

•What **other business** takes place with high risk jurisdictions, and what measures are in place to contain the risks of transactions being related to proliferation?

Examples of good practice	Examples of poor practice
• A bank has identified if its customers export goods to high risk jurisdictions, and subjects transactions to **enhanced scrutiny** by identifying, for example, whether goods may be subject to export restrictions, or end-users may be of concern.	• The firm **assumes** customers selling goods to countries of concern will have checked the exports are legitimate, and **does not ask for evidence** of this from customers.
• Where **doubt exists**, the bank asks the customer to **demonstrate** that appropriate assurances have been gained from relevant government authorities.	• A firm knows that its customers deal with individuals and entities from high risk jurisdictions but **does not communicate with those customers** about relevant regulations in place and how they affect them.
• The firm has considered **how to respond** if the government	• [deleted]

Examples of good practice	Examples of poor practice
takes action under the Counter-Terrorism Act 2008 against one of its customers.	

Case study – deficient sanctions systems and controls

7.2.6 G In August 2010, the *FSA* fined Royal Bank of Scotland (RBS) £5.6m for deficiencies in its systems and controls to prevent breaches of UK financial sanctions.

- RBS failed adequately to screen its customers – and the payments they made and received – against the sanctions list, thereby running the risk that it could have facilitated payments to or from sanctioned people and organisations.
- The bank did not, for example, screen cross-border payments made by its customers in sterling or euros.
- It also failed to ensure its 'fuzzy matching' software remained effective, and, in many cases, did not screen the names of directors and beneficial owners of customer companies.

The failings led the *FSA* to conclude that RBS had breached the Money Laundering Regulations 2007, and our penalty was imposed under that legislation – a first for the *FSA*.

For more information see the *FSA's* press release: www.fsa.gov.uk/pages/Library/Communication/PR/2010/130.shtml

7.3 Further guidance

7.3.1 G *FCTR* contains the following additional material on sanctions and assets freezes:

- FCTR 8 summarises the findings of the *FCA's* thematic review of financial services firms' approach to UK financial sanctions and includes guidance on:
  - Senior management responsibility (FCTR 8.3.1G)
  - Risk assessment (FCTR 8.3.2G)
  - Policies and procedures (FCTR 8.3.3G)
  - Staff training and awareness (FCTR 8.3.4G)
  - Screening during client take-on (FCTR 8.3.5G)
  - Ongoing screening (FCTR 8.3.6G)
  - Treatment of potential target matches (FCTR 8.3.7G)
- FCTR 15 summarises the findings of the *FCA's* thematic review Banks' management of financial crime risk in trade finance and includes guidance on:
  - Sanctions Procedures (FCTR 15.3.7G)
  - Dual-Use Goods (FCTR 15.3.8G)

7.4 Sources of further information

7

7.4.1 G To find out more on financial sanctions, see:

- OFSI's website: https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation
- OFSI provides FAQs on financial sanctions- https://www.gov.uk/government/publications/financial-sanctions-faqs
- Part III of the Joint Money Laundering Steering Group's guidance: www.jmlsg.org.uk
- OFSI UK Financial Sanctions Guidance: www.gov.uk/government/publications/financial-sanctions-general-guidance/uk-financial-sanctions-general-guidance
- Alerts published by the NECC: www.nationalcrimeagency.gov.uk/who-we-are/publications/
- *FCA* sanctions webpages – these pages include our latest updates and details on how to report sanctions breaches to us:

  www.fca.org.uk/russian-invasion-ukraine

  www.fca.org.uk/firms/financial-crime/financial-sanctions

7.4.2 G To find out more on trade sanctions and proliferation, see:

- Part III of the Joint Money Laundering Steering Group's guidance on the prevention of money laundering and terrorist financing, which contains a chapter on proliferation financing that should be firms' chief source of guidance on this topic: www.jmlsg.org.uk
- The website of the UK's Export Control Organisation, which contains much useful information, including lists of equipment requiring a licence to be exported to any destination, because they are either military items or 'dual use' https://www.gov.uk/government/organisations/export-control-organisation
- The NCA's website, which contains guidelines on how to report suspicions related to weapons proliferation: www.nationalcrimeagency.gov.uk/who-we-are/publications/171-sar-guidance-notes/file
- The FATF guidance on proliferation financing:

www.fatf-gafi.org/content/dam/fatf-gafi/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf

www.fatf-gafi.org/en/publications/Financingofproliferation/Proliferation-financing-risk-assessment-mitigation.html

•HM Government's website, which includes the National Risk Assessment of Proliferation Financing: www.ncsc.gov.uk/collection/board-toolkit/introduction-to-cyber-security-for-board-members

•The Office of Trade Sanctions Implementation (OTSI) helps to ensure that trade sanctions are properly understood, implemented and enforced. OTSI has published guidance regarding trade sanctions, and this is available on its website: www.gov.uk/otsi

Chapter 8

Insider dealing and market manipulation

8.1 Introduction

8.1.1 G **Who should read this chapter?** This chapter applies to firms subject to ■ SYSC 6.1.1R.

8.1.2 G Insider dealing is a criminal offence under section 52 of the Criminal Justice Act 1993. Sections 89-91 of the Financial Services Act 2012 set out a range of behaviours which amount to criminal offences, which are together referred to in this guide as market manipulation.

8

8.1.3 G Section 1H(3) of the *Act* defines financial crime to include 'any offence involving:

(a) fraud or dishonesty,

(b) misconduct in, or misuse of information relating to, a financial market,

(c) handling the proceeds of crime, or

(d) the financing of terrorism'.

Insider dealing and market manipulation both meet this definition, in particular because they involve misconduct in a financial market.

8.1.4 G To avoid doubt, all references to insider dealing and market manipulation in this chapter refer to the criminal offences set out above. This chapter does not seek to reproduce a list of those markets, particularly because that list may change over time. Therefore, all references to 'financial markets' and 'markets' in this chapter refer to the markets to which the criminal regimes of insider dealing and market manipulation apply, unless the context specifies otherwise. The civil offences of insider dealing, unlawful disclosure of inside information and market manipulation set out in the *Market Abuse Regulation* are referred to collectively herein as market abuse.

8.1.5 G We recognise that many firms will not distinguish between the criminal or civil regimes for the purposes of conducting surveillance and monitoring of their clients' and employees' activities. As such, firms may find it simpler to consider this guidance as applying to all instruments to which both the *Market Abuse Regulation* and the criminal regimes set out in ■ FCG 8.1.2G apply. Note though that the *FCA* cannot and does not mandate that this guidance applies to those financial instruments which are captured by the *Market Abuse Regulation*, but not by the criminal regimes set out above.

8.1.6 G To commit insider dealing, as well as certain forms of market manipulation, the perpetrator must typically engage with, or work within, a firm able to access the relevant financial markets on their behalf. It is critical that firms that offer access to relevant financial markets have adequate policies and procedures to counter the risk that the firm might be used to further financial crime, in accordance with ■ SYSC 6.1.1R.

FCG is not intended to be prescriptive to every business model type. It is incumbent upon a firm to ensure that its policies, procedures and risk framework are tailored and appropriate to the nature of its business, eg client type(s), product type(s), means of order transmission and execution, risks posed by employees, etc.

8.1.7 G On 3 July 2016, *Market Abuse Regulation* came into force. The *Market Abuse Regulation* sets out the civil offences of market abuse. Article 16 of the *Market Abuse Regulation* also imposes specific requirements on:

- Market operators and investment firms that operate a trading venue to establish and maintain effective arrangements, systems and procedures aimed at detecting and preventing insider dealing, market manipulation and attempted insider dealing and market manipulation. Such persons shall report orders and transactions that could constitute insider dealing or market manipulation (or attempts at such) to the competent authority of the trading venue. This is imposed under article 16(1).

- Any person professionally arranging or executing transactions to establish and maintain effective arrangements, systems and procedures to detect and report suspicious orders and transactions. This is imposed under article 16(2).

8.1.8 G There is a key distinction between the obligations under article 16(2) of the *Market Abuse Regulation* and the requirements of ■ SYSC 6.1.1R. Article 16(2) of the *Market Abuse Regulation* requires persons professionally arranging or executing transactions to establish arrangements, systems and procedures to detect and report potential market abuse, whereas ■ SYSC 6.1.1R requires firms to have policies and procedures for countering the risk that the firm might be used to further financial crime. (As noted above, article 16(1) of the *Market Abuse Regulation* obliges market operators and investment firms that operate a trading venue to have systems aimed at preventing as well as detecting potential market abuse). This document does not provide any *FCA* guidance in relation to the *Market Abuse Regulation* article 16.

8.1.9 G Appropriate policies and procedures for countering the risk that the firm might be used to further financial crime are likely to fall into two distinct categories:

(1) Identification of, and taking steps to counter financial crime pre-trade, and

(2) Mitigation of future risks posed by clients or employees who have been identified as having already traded suspiciously.

8.1.10 G Firms which have identified activity they suspect may amount to insider dealing or market manipulation should consider their further obligations in relation to countering the risk of financial crime should the relevant client seek to transfer or use the proceeds of that suspicious activity (see ■ FCG 3). This includes, where appropriate, seeking consent from the National Crime Agency.

8.2 Themes

Governance

8.2.1 G The guidance in ■ FCG 2.2.1G above on governance in relation to financial crime also applies to insider dealing and market manipulation.

We expect senior management to take responsibility for the firm's measures in relation to insider dealing and market manipulation. This includes:

- Understanding the risks of insider dealing or market manipulation that their firm is exposed to (both through employee and client activity).

- Establishing adequate policies and procedures to counter the risk that their firm is used to further these offences in accordance with ■ SYSC 6.1.1R.

Senior management should also be aware and manage the potential conflict of interest which may arise from the firm's focus on revenue generation versus its obligation to counter the risk of the firm being used to further financial crime.

Self-assessment questions:

- Does the firm's senior management team understand the legal definitions of insider dealing and market manipulation, and the ways in which the firm may be exposed to the risk of these crimes?

- Does the firm's senior management team regularly receive management information in relation to suspected insider dealing or market manipulation?

- How does senior management make sure that the firm's systems and controls for detecting insider dealing and market manipulation are robust? How do they set the tone from the top?

- How does the firm's MLRO interact with the individual/departments responsible for order and trade surveillance/monitoring?

- How does senior management make decisions in relation to concerns about potential insider dealing or market manipulation raised to them by Compliance or another function? Do they act appropriately to mitigate these risks?

- How does senior management make sure that its employees have the appropriate training to identify potential insider dealing and market manipulation?

Examples of good practice	Examples of poor practice
• Senior management are able to recognise and articulate the warning signs that insider dealing and market manipulation might be taking place.	• There is little evidence that possible insider dealing or market manipulation is taken seriously by senior management. Addressing these risks is seen as a legal or regulatory necessity rather than a matter of true concern for the business.
• Senior management regularly receive management information in relation to any possible insider dealing or market manipulation that occurs.	• Senior management considers revenue above obligations to counter financial crime.
• The individual(s) responsible for overseeing the firm's monitoring for suspected insider dealing and market manipulation has regular interaction and shares relevant information with the MLRO.	• Senior management considers the firm's financial crime obligations are fulfilled solely by submitting a STOR and/or SAR.
• Senior management appropriately supports decisions proposed by Compliance.	• The Compliance function has limited independence and the first line can block concerns from being escalated.

Risk assessment

8.2.2 G The guidance in ■ FCG 2.2.4G above on risk assessment in relation to financial crime also applies to insider dealing and market manipulation.

Firms should assess and regularly review the risk that they may be used to facilitate insider dealing or market manipulation. A number of factors should be incorporated into this assessment, including the client types, products, instruments and services offered/ provided by the firm. Firms' assessments should also consider the risk which employees may pose too.

Firms should consider how their policies and procedures seek to mitigate the financial crime risks they have identified. This could include, but is not limited to:

- undertaking enhanced order and transaction monitoring on clients or employees,
- setting client specific pre-trade limits, and
- ultimately declining business or terminating client or employee relationships if appropriate (see ■ FCG 8.2.3 for more detail).

Self-assessment questions:

- Has the firm considered whether any of the products/services it offers, or the clients it has, pose a greater risk that the firm might be used to facilitate insider dealing or market manipulation? How has the firm determined this?

•Who is responsible for carrying out the risk assessment and keeping it up to date? Do they have sufficient levels of expertise (including markets and financial crime knowledge) and seniority?

What framework does the firm have in place for assessing the risk of insider dealing and market manipulation being committed by its employees?

•How does the firm use its risk assessment when deciding which business to accept?

•How often is the risk framework reviewed and who approves it? • How does the firm's risk framework for countering the risk of insider dealing and market manipulation interact with the firm's AML risk framework? Are the risk assessments aligned?

Examples of good practice	Examples of poor practice
• Insider dealing and market manipulation risks are assessed across every asset class to which the criminal regimes of insider dealing and market manipulation apply, and across all client types with which the firm operates.	• Risk assessments are generic, and not based upon the firm's own observations.
• There is evidence that the firm's risk assessment informs the design of its surveillance controls.	• An inappropriate risk classification system makes it almost impossible for a client relationship to be considered 'high risk'.
• The firm identifies and uses all information at its disposal to make informed judgments about the level of financial crime risk posed to its business.	• The firm fails to consider the risks associated with employees using discretionary accounts to commit insider trading or market manipulation.
• The firm's risk framework is regularly tested and reviewed.	• Risk assessments are inappropriately influenced by profitability of new or existing relationships.
• Where a firm identifies a risk that it may be used to facilitate insider dealing or market manipulation, it takes appropriate steps to mitigate that risk.	• The firm submits a significant number of SARs and/or STORs on a particular client, but continues to service that client without considering its obligation to counter the risk of furthering financial crime.
• The firm considers where relationship managers might become too close to customers to take an objective view of risk, and manages that risk effectively.	• The firm fails to consider additional account information it has access to, such as Power of Attorney arrangements, when designing its surveillance controls.

Policies and procedures

8.2.3 G The guidance in ■ FCG 2.2.5G above on policies and procedures in relation to financial crime also apply.

Firms' policies and procedures should include steps designed to counter the risk of insider dealing and market manipulation occurring through the firm. Policies and procedures should be aligned and make reference to the firm's insider dealing and market manipulation risk assessment.

Firms should ensure that their policies and procedures cover both:

(1) identifying and taking steps to counter the risk of financial crime before any trade is executed, and

(2) mitigating future risks posed by clients or employees who have already been identified as having traded suspiciously.

Firms should make sure that front office employees are aware of the firm's policies and procedures with regard to countering the risk that the firm is used to further financial crime. Among other things, these should reflect the *FCA's* expectation that market participants do not knowingly or intentionally aid, abet, counsel or procure the commission of a criminal offence (insider dealing or market manipulation). Therefore, where the firm holds information which leads to the conclusion that its employee or client is seeking to trade either manipulatively or on the basis of inside information, it should refuse to execute the trade where it is able to do so.

Firms' policies and procedures should state clearly how they identify and monitor employees' trading, in addition to their clients' trading. ■ COBS 11.7 requires firms that conduct designated investment business to have a personal account dealing (PAD) policy. Appropriately designed PAD policies can:

- counter the risk that employees of the firm commit financial crime themselves,

- make sure that conflicts of interest that might result in employees not escalating suspicious activity are avoided. For example, if employees are allowed to copy clients' trades on their own accounts, they may be less inclined to escalate financial crime concerns that only become apparent post-trade, as, by reporting the client they would, by implication, be reporting their own trading as suspicious.

Policies and procedures relevant to each business area, including front office functions, should be communicated and embedded.

Self-assessment questions:

- Does the policy define how the firm will counter the risk of being used to facilitate insider dealing and market manipulation? For example, in what circumstances would the firm conduct enhanced monitoring or stop providing trading access to a particular client or employee?

- Does the firm have established procedures for following up and reviewing possibly suspicious behaviour?

- Do front office staff understand how insider dealing and market manipulation might be committed through the firm, to escalate potentially suspicious activity when appropriate, and challenge client or employee orders (where relevant), if they believe the activity will amount to financial crime? Does the firm have effective

whistleblowing arrangements in place to support appropriate financial crime detection and reporting?

Examples of good practice	Examples of poor practice
• The firm has clear and unambiguous expectations for its employees and anyone acting on its behalf, such as introducing brokers.	• The firm's policies and procedures aren't updated for legal or regulatory changes.
• Employees in dealing roles understand and are able to identify potentially illegal conduct, and their trading is regularly monitored by Compliance.	• Policies and procedures are generic and don't consider the specific processes or risks of the firm.
• The policies and procedures make adequate reference to the firm's risk assessment.	• Policies and procedures cover only post-trade identification and reporting of suspicious activity and do not cover countering the risk of financial crime.
• Policies and procedures make sure that the risk of financial crime is considered throughout the lifecycle of a security transaction, including before the order has been executed.	• The firm sets apparently robust procedures for assessing and mitigating identified financial crime risk, but sets thresholds for engaging these measures which mean that they are almost impossible to trigger.
• Where the financial intermediary is aware that a client is intending to trade on the basis of inside information or manipulate the market, the firm refuses to execute the order(s).	• The firm doesn't have policies detailing the circumstances when it will consider rejecting a prospective client or terminating an existing client relationship.
• The firm takes swift, robust action for breaches of its policies and procedures.	• The firm doesn't have appropriate policies or procedures in place regarding personal account dealing, so that staff are able to deal in a manner which creates conflict in escalating suspected market abuse.
• The firm's policies and procedures include controls designed to counter the risk of financial crime being committed by employees, for example wall crossings, restricted lists and personal account dealing restrictions.	

Ongoing monitoring

8.2.4 G We recognise that the *Market Abuse Regulation* already imposes monitoring requirements on persons professionally arranging or executing transactions, in order to detect and report suspicious orders and transactions in the form of STORs (as well as imposing similar monitoring obligations on market

operators and investment firms that operate a trading venue). It may be appropriate to use the results of this monitoring for the purpose of countering financial crime.

Firms should note that the markets and instruments to which the criminal offences of insider dealing and market manipulation apply are different to those covered by the *Market Abuse Regulation*. Firms should therefore assess whether their arrangements to detect and report market abuse can be appropriately relied on to monitor for potential insider dealing and market manipulation.

For their risk assessments, firms should regularly take steps to consider whether their employees and/or clients may be conducting insider dealing or market manipulation. This could be achieved by transaction, order and communications surveillance, with consideration given to the employee's or client's usual trading behaviour and/or strategies, and in respect of clients: initial on-boarding checks and ongoing due diligence, or other methods.

Firms should consider the risks that arise in scenarios whereby their client is not the decision maker behind the activity taking place, with orders and trades being instructed by an underlying client. In this scenario, where a firm is concerned either about a particular client or trade, firms should consider the steps they could take to gain further information, or an understanding, of the client, underlying client and/or activity. The firm may wish to engage with its client to obtain further information about the trading in question and/or the nature of the underlying client(s).

If a firm is, based on their understanding of a client and monitoring of that client's transactions, suspicious that a client might have committed or attempted to commit insider dealing or market manipulation, the firm should comply with its obligations to report those suspicions via a STOR and/or SAR (where appropriate). In addition, it may be appropriate for the firm to document the options available to it to counter the risk of any ongoing financial crime posed by its ongoing relationship with that client, and when these options should be considered.

In addition, a firm must also submit a STOR where it identifies suspicious trading by an employee. The nominated officer of the firm would also be required to report any knowledge or suspicions of money laundering or terrorist financing arising from trade by submitting a SAR to the NCA. Again, the firm's policies and procedures should document the options available to it to counter the risk of any ongoing financial crime related to employee trading activity, and when these options should be considered.

Options available to firms to counter the risk of being used to further financial crime by its clients and/or employees could include:

- Carrying out enhanced due diligence on a client and enhanced monitoring of a client's or employee's trading activity.
- Restricting the client's access to particular markets or instruments.
- Restricting services provided to the client (eg direct market access).
- Restricting the amount of leverage the firm is willing to provide to the client.
- Taking disciplinary action against an employee.
- Ultimately terminating the client or employee relationship. The appropriate response will depend on the outcome of the firm's

monitoring procedures and the extent and nature of any suspicious activity identified.

Self-assessment questions:

•Does the firm consider its obligations to counter financial crime when a client's or employee's activity is determined as suspicious via surveillance systems and subsequent investigation?

•How do the firm's monitoring arrangements interact with the client-on-boarding process / AML framework?

•Does the firm undertake enhanced monitoring for high risk clients?

•Does the firm's monitoring cover the activity of any employee trading?

•In instances where a firm is concerned about a client which is not the individual or entity who is making the decision to trade, has the firm considered information it has access to, or ways it can gain information, to allow it to counter the risk of being used to further financial crime?

Examples of good practice	Examples of poor practice
• The firm's monitoring seeks to identify trends in clients' or employee's behaviour, in addition to one off events.	• The firm believes that its obligations cease when it reports the suspicious transactions and orders.
• The firm undertakes enhanced monitoring of clients it has determined are high risk.	• Suspicious transactions and orders are identified but not investigated further.
• The firm conducts regular, targeted monitoring of voice and electronic communications.	• Monitoring identifies individual suspicious events but does not attempt to identify patterns of suspicious behaviour by the same client or a group of clients, using, for example, historical assessments of potentially suspicious activity or STORs submitted.
• Front office employees escalate suspicious activity promptly to Compliance.	• The firm does not consider engaging with its clients, whether to understand their trading activity or the activity of their underlying client(s).
• The firm takes additional steps to understand and ensure it is comfortable with the rationale behind the trading strategies employed by its client(s) and/or staff.	• The firm does not use information obtained via monitoring and subsequent investigation to consider the suitability of retaining a client relationship.
• The firm conducts regular monitoring of its employee trading activity, whether personal account dealing or trad-	• In instances when a client is placing orders on behalf of its underlying clients, the firm fails to make use of informa-

Examples of good practice	Examples of poor practice
ing on behalf of the firm or clients.	tion which could allow it to understand the nature and potential risk of their client (for example, number of underlying clients, trading strategies, the nature of their business).
• In instances when a client is placing orders on behalf of its underlying clients, the firm engages with their client to establish whether they maintain appropriate systems and controls for countering the risk of being used to further financial crime.	
• The firm considers a client or employee's ongoing risk of committing insider dealing or market manipulation following the submission of a STOR and/or SAR.	

Chapter Annex

Common terms

Common terms

This annex provides a list of common and useful terms related to financial crime. It also includes references to some key legal provisions. It is for reference purposes and is not a list of 'defined terms' used in *FCG*. This annex does not provide guidance on rules or amend corresponding references in the *Handbook's Glossary*.

Term	Meaning
Action Fraud	The UK's national fraud reporting centre. See: www.actionfraud.police.uk
advance fee fraud	A fraud where people are persuaded to hand over money, typically characterised as a 'fee', in the expectation that they will then be able to gain access to a much larger sum which does not actually exist.
AML	Anti-money laundering. See 'money laundering'.
Annex I financial institution	The *Money Laundering Regulations* give the *FCA* responsibility for supervising the anti-money laundering controls of 'Annex I financial institutions' (a reference to Annex I to the Capital Requirements Directive, where they are listed). In practice, this includes businesses that offer finance leases, commercial lenders and providers of safe deposit boxes. Where an authorised firm offers such services, we are responsible for overseeing whether these activities are performed in a manner that complies with the requirements of the *Money Laundering Regulations*. Authorised firms are not formally required to inform us that they perform these activities, although some may choose to do so for the sake of transparency. Where these businesses are not authorised, we are responsible for supervising their activities. For more information on this, see the *FCA's* website: https://www.fca.org.uk/firms/money-laundering-terrorist-financing/registration
beneficial owner	The natural person who ultimately owns or controls the customer. An entity may have more than one beneficial owner. 'Beneficial owner' is defined in Regulations 5 and 6 of the *Money Laundering Regulations*.
boiler room	See 'share sale fraud'.
bribery	Bribery is the offering or acceptance of an undue advantage in exchange for the improper performance of a function or activity. Statutory offences of bribery are set out more fully in the Bribery Act 2010.
Bribery Act 2010	The Bribery Act came into force in July 2011. It outlaws offering and receiving bribes, at home and abroad, as well as creating a corporate offence of failure to prevent bribery. The Ministry of Justice has issued guidance about procedures which firms can put in place to prevent bribery: https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf
business-wide risk assessment	A business-wide risk assessment means the identification and assessment of the financial crime risks to which a firm is exposed as a result of, for example, the products and services it offers, the jurisdictions it operates in, the types of customer it attracts, the com-

Term	Meaning
	plexity and volume of transactions, and the distribution channels it uses to service its customers.
carbon credit scams	Firms may sell carbon credit certificates or seek investment directly in a 'green' project that generates carbon credits as a return. Carbon credits can be sold and traded legitimately and there are many reputable firms operating in the sector. We are, however, concerned an increasing number of firms are using dubious, high-pressure sales tactics and targeting vulnerable consumers. See: https://www.fca.org.uk/scamsmart/carbon-credit-scams
CDD	See 'customer due diligence'.
CIFAS	CIFAS is the UK's fraud prevention service with over 250 members across the financial industry and other sectors. See CIFAS's website for more information: www.cifas.org.uk
Defence against Money Laundering	A 'Defence Against Money Laundering (DAML)' can be requested from the NCA where a firm has a suspicion that property they intend to deal with is in some way criminal, and that by dealing with it they risk committing one of the principal money laundering offences under the Proceeds of Crime Act 2002 (POCA). A person does not commit one of those offences if they have received 'appropriate consent' (aka a "DAML") from the NCA. The NCA is empowered to provide these criminal defences in law under s335 of POCA. More information is available from the NCA, http://www.nationalcrimeagency.gov.uk/publications/902-defence-against-money-laundering-faq-may-2018/file
Consolidated List	OFSI maintains a Consolidated List of financial sanctions targets designated by the United Nations, the European Union and the United Kingdom. It is available from the Treasury's website: www.hm-treasury.gov.uk/fin_sanctions_index.htm
corruption	Corruption is the abuse of public or private office to obtain an undue advantage. Corruption includes not only bribery but also other forms of misconduct or improper behaviour. This behaviour may or may not be induced by the prospect of obtaining an undue advantage from another person.
Counter-Terrorism Act 2008	The Treasury has powers under Schedule 7 to the Counter-Terrorism Act 2008 to require financial firms to take specified actions in relation to a country of concern, or counterparties based in that country. Use of this power can be triggered if a) the risk of money laundering or terrorist financing activities is identified in a country, or b) the government believes a country has a nuclear, chemical, radiological or biological weapons programme that threatens the UK. The directions can require enhanced due diligence and ongoing monitoring, the systematic reporting of transactions, or the cessation of business. This offers the government flexibility that was not available in the traditional financial sanctions regime. We are responsible for monitoring authorised firms' and certain financial institutions' compliance with these directions.
cover payment	Where payments between customers of two banks in different countries and currencies require settlement by means of matching inter-bank payments, those matching payments are known as 'cover payments'. International policymakers have expressed concern that cover payments can be abused to hide the origins of flows of funds. In response to this, changes to the SWIFT payment messaging system now allow originator and beneficiary information to accompany cover payments.
CPS	See 'Crown Prosecution Service'

Term	Meaning
Crown Prosecution Service (CPS)	The Crown Prosecution Service prosecutes crime, money laundering and terrorism offences in England and Wales. The Procurator Fiscal and Public Prosecution Service of Northern Ireland play similar roles in Scotland and Northern Ireland respectively. See the CPS website for more information: www.cps.gov.uk
CTF	Combating terrorist financing/countering the finance of terrorism.
customer due diligence (CDD)'	Customer due diligence' describes measures firms have to take to identify, and verify the identity of, customers and their beneficial owners. Customer due diligence also includes measures to obtain information on the purpose and intended nature of the business relationship. See Regulation 7 of the *Money Laundering Regulations*. 'Customer due diligence' and 'Know Your Customer' (KYC) are sometimes used interchangeably.
dual use goods	Items that can have legitimate commercial uses, while also having applications in programmes to develop weapons of mass destruction. Examples may be alloys constructed to tolerances and thresholds sufficiently high for them to be suitable for use in nuclear reactors. Many such goods are listed in EU regulations which also restrict their unlicensed export.
Data Protection Act 1998 (DPA)	The DPA imposes legal obligations on those who handle individuals' personal information. Authorised firms are required to take appropriate security measures against the loss, destruction or damage of personal data. Firms also retain responsibility when data is passed to a third party for processing.
ECCTA	The Economic Crime and Corporate Transparency Act 2023
economic sanctions	Restrictions on trade or financial flows imposed by the government in order to achieve foreign policy goals. See: 'financial sanctions regime', 'trade sanctions', and 'proliferation finance'.
EEA firms	Firms from the European Economic Area (EEA) which passport into the UK are authorised persons. This means, generally speaking, EEA firms who carry on relevant business from a UK branch will be subject to the requirements of the *Handbook* and of the *Money Laundering Regulations*. However, an EEA firm that only provides services on a cross-border basis (and so does not have a UK branch) will not be subject to the *Money Laundering Regulations*, unless it carries on its business through representatives who are temporarily located in the UK.
Egmont Group	A forum for financial intelligence units from across the world. See the Egmont Group's website for more information: www.egmontgroup.org
embargos	See 'trade sanctions'.
e-money	The Electronic Money Regulations 2011 (SI 2011/99) define electronic money as electronically (including magnetically) stored monetary value, represented by a claim on the issuer, which is issued on receipt of funds for the purpose of making payment transactions, and which is accepted by a person other than the electronic money issuer. The E-money Regulations specify who can issue e-money; this includes credit institutions and e-money institutions.
e-money institutions (EMIs)	E-money institutions are a specific category of financial institutions authorised or registered to issue e-money under the Electronic Money Regulations 2011, rather than FSMA. The *FCA's* financial crime *Handbook* provisions do not apply to e-money institutions, but the *FCA* supervises e-money institutions for compliance with their obligations under the *Money Laundering Regulations*. They must also satisfy us that they have robust governance, effective risk procedures and adequate internal control mechanisms.

Term	Meaning
	This incorporates their financial crime systems and controls. For more information, see our payment services and e-money approach document: https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf
enhanced due diligence (EDD)	Regulations 33-35 of the *Money Laundering Regulations* require firms to apply additional, 'enhanced' customer due diligence measures in higher risk situations (see FCG 3.2.7G to FCG 3.2.9G).
equivalent jurisdiction	A jurisdiction (other than an EEA state) whose law contains equivalent provisions to those contained in the Fourth Money Laundering Directive. The JMLSG has prepared guidance for firms on how to identify which jurisdictions are equivalent. Equivalent jurisdictions are significant because it is a factor that a firm may consider when deciding whether to apply 'simplified due diligence' to financial institutions from these places. Firms can also rely on the customer due diligence checks undertaken by certain introducers from these jurisdictions (see 'reliance').
export controls	UK exporters must obtain a licence from the government before exporting certain types of goods, primarily those with military applications. Exporting these goods without a licence is prohibited by the Export Control Order 2008 (SI 2008/3231). If an authorised financial firm were to finance or insure these illegal exports, it would arguably have been used to further financial crime.
family member of a PEP	Regulation 35(12)(b) of the *Money Laundering Regulations* defines a family member of a PEP as including a spouse or civil partner of a PEP; children of the PEP and the spouses or civil partners of the PEP's children; and the parents of a PEP. The *FCA's* Finalised Guidance 'FG17/16: The treatment of politically exposed persons for anti-money laundering purposes' provides further guidance on this definition.
FATF	See 'Financial Action Task Force'.
FATF Recommendations	Forty Recommendations issued by the FATF on the structural, supervisory and operational procedures that countries should have in place to combat money laundering. These were revised in February 2012, and now incorporate the nine Special Recommendations on the prevention of terrorist financing that were previously listed separately. The Forty Recommendations can be downloaded from the FATF's website: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html
FATF-style regional bodies	Regional international bodies such as Moneyval and the Asia-Pacific Group which have a similar form and functions to those of the FATF. The FATF seeks to work closely with such bodies.
FI	See 'Financial Investigator'.
Financial Action Task Force (FATF)	An intergovernmental body that develops and promotes anti-money laundering and counter terrorist financing standards worldwide. Further information is available on its website: www.fatf-gafi.org
Financial Conduct Authority (*FCA*)	The *Financial Conduct Authority* has statutory objectives under FSMA that include protecting and enhancing the integrity of the UK financial system. The integrity of the UK financial system includes its not being used for a purpose connected with financial crime. We have supervisory responsibilities under the *Money Laundering Regulations* for authorised firms and businesses such as leasing companies and providers of safe deposit boxes. We also have functions under other legislation such as Schedule 7 to the Counter-Terrorism Act 2008.

Term	Meaning
financial crime	Financial crime is any crime involving money. More formally, the Financial Services and Markets Act 2000 defines financial crime 'to include any offence involving (a) fraud or dishonesty; (b) misconduct in, or misuse of information relating to, a financial market; or (c) handling the proceeds of crime'. The use of the term 'to include' means financial crime can be interpreted widely to include, for example, corruption or funding terrorism.
financial intelligence unit (FIU)	The IMF uses the following definition: 'a central national agency responsible for receiving, analyzing, and transmitting disclosures on suspicious transactions to the competent authorities.' The NCA has this role in the UK.
Financial Investigator (FI)	Financial Investigators are accredited people able under the relevant legislation to investigate financial offences and recover the proceeds of crime.
financial sanctions regime	This prohibits firms from providing funds and other economic resources (and, in the case of designated terrorists, financial services) to individuals and entities on a Consolidated List maintained OFSI. OFSI is responsible for ensuring compliance with the UK's financial sanctions regime; our role is to ensure firms have appropriate systems and controls to enable compliance.
Financial Services and Markets Act 2000 (FSMA)	The Financial Services and Markets Act 2000 sets out the objectives, duties and powers of the Financial Conduct Authority and the Prudential Regulation Authority.
Financial Services Authority (*FSA*)	The Financial Services Authority was the previous financial services regulator. It had statutory objectives under FSMA that included the reduction of financial crime. The *FSA* had supervisory responsibilities under the *Money Laundering Regulations* for authorised firms and businesses such as leasing companies and providers of safe deposit boxes. It also had functions under other legislation such as the Transfer of Funds (Information on the Payer) Regulations 2007, in relation to the EU Wire Transfer Regulation, and schedule 7 to the Counter-Terrorism Act 2008.
FIU	See 'financial intelligence unit'.
four-eyes procedures	Procedures that require the oversight of two people, to lessen the risk of fraudulent behaviour, financial mismanagement or incompetence going unchecked.
Fourth Money Laundering Directive (4MLD)	The Fourth Money Laundering Directive (2015/849/EC). The UK has implemented this Directive mainly through the *Money Laundering Regulations*.
fraud (types of)	Fraud can affect firms and their customers in many ways. The following are examples of fraud: • a firm is defrauded by customers (e.g. mortgage fraud); • a firm is defrauded by employees or contractors ('insiders') (e.g. a staff member steals from his employer and amends records to cover-up the theft); • a firm's customers are defrauded by an insider (e.g. a staff member steals customers' money); • a firm's customers are defrauded after a third party misleads the firm (e.g. criminals evade security measures to gain access to a customer's account); • a firm's customers are defrauded by a third party because of the firm's actions (e.g. the firm loses sensitive personal data allowing the customer's identity to be stolen);

Term	Meaning
	• a customer is defrauded, with a firm executing payments connected to this fraud on the customer's instruction (e.g. a customer asks his bank to transfer funds to what turns out to be a share sale scam). See also: 'advance fee fraud', 'boiler room', 'carbon credit scams', 'investment fraud', 'land banking scams', 'long firm fraud', 'mass-marketing fraud', 'Missing Trader Inter-Community fraud', 'Ponzi and pyramid schemes', 'share sale fraud'.
Fraud Act 2006	The Fraud Act 2006 sets out a series of fraud offences such as fraud by false representation, fraud by failing to disclose information and fraud by abuse of position.
FSA	See 'Financial Services Authority'.
FSMA	See 'Financial Services and Markets Act 2000'.
FSRB	See 'FATF-style regional bodies'.
fuzzy matching	The JMLSG suggests the term 'fuzzy matching' 'describes any process that identifies non-exact matches. Fuzzy matching software solutions identify possible matches where data – whether in official lists or in firms' internal records – is misspelled, incomplete, or missing. They are often tolerant of multinational and linguistic differences in spelling, formats for dates of birth, and similar data. A sophisticated system will have a variety of settings, enabling greater or less fuzziness in the matching process'. See Part III of the JMLSG's guidance: http://www.jmlsg.org.uk/download/10007
Funds Transfer Regulation	This EU Regulation is formally titled 'Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds'. It implements FATF's Recommendation 16 in the EU and requires firms to accompany the transfer of funds with specified information identifying the payer and the payee. We are given supervisory and enforcement powers for compliance with this regulation by the *Money Laundering Regulations*.
high-value dealer	A firm trading in goods (e.g. cars, jewellery and antiques) that accepts cash of €10,000 or more in payment (whether in one go or in several payments that appear to be linked). HMRC is the supervisory authority for high value dealers. A full definition is set out in Regulation 14(1)(a) of the *Money Laundering Regulations*.
HM Revenue and Customs (HMRC)	HM Revenue and Customs has supervisory responsibilities under the *Money Laundering Regulations*. It oversees money service businesses, dealers in high value goods, estate agents and trust or company service providers, amongst others. See HMRC's website for more information: https://www.gov.uk/topic/business-tax/money-laundering-regulations
HMRC	See 'HM Revenue and Customs'.
HMT	See 'Treasury'.
ICO	See 'Information Commissioner's Office'.
ID	Identification (or Identity Documents).
identification	The JMLSG's definition is: 'ascertaining the name of, and other relevant information about, a customer or beneficial owner'.
IFB	Insurance Fraud Bureau.
Information Commissioner's Office (ICO)	The Information Commissioner's Office is tasked with protecting the public's personal information. See the ICO's website for further information: www.ico.org.uk

Term	Meaning
Information From Lenders (IFL)	The Information From Lenders scheme enables mortgage lenders to inform the *FCA* of suspected fraud by mortgage brokers. Details are here: https://www.fca.org.uk/firms/fraud/report-mortgage-fraud-advisers
insider fraud	Fraud against a firm committed by an employee or group of employees. This can range from junior staff to senior management, directors, etc. Insiders seeking to defraud their employer may work alone, or with others outside the firm, including organised criminals.
Institute of Chartered Accountants in England and Wales (ICAEW)	The Institute of Chartered Accountants in England and Wales has supervisory responsibility for its members under the *Money Laundering Regulations*, as do other professional bodies for accountants and book-keepers. See the ICAEW's website for further information:www.icaew.com
integration	See 'placement, layering, integration'.
investment fraud	UK-based investors lose money every year to share sale frauds and other scams including, but not limited to, land-banking frauds, Ponzi schemes, and rogue carbon credit schemes. See *FCA's* scamsmart, http://scamsmart.fca.org.uk/
JMLSG	See 'Joint Money Laundering Steering Group'.
Joint Money Laundering Steering Group (JMLSG)	This industry body is made up of financial sector trade bodies. It produces guidance on compliance with legal and regulatory requirements related to money laundering. See the JMLSG's website for more information: www.jmlsg.org.uk
Know Your Customer (KYC)	This term is often used as a synonym for 'customer due diligence' checks. The term can also refer to suitability checks related to the regulated sales of financial products. The *Money Laundering Regulations* refer to 'customer due diligence' and not to KYC.
known close associate of a PEP	Regulation 35(12)(c) of the *Money Laundering Regulations* defines a known close associate of a PEP as being either an individual known to have joint beneficial ownership of a legal entity or a legal arrangement or any other close business relations with a PEP or an individual who has sole beneficial ownership of a legal entity or a legal arrangement which is known to have been set up for the benefit of a PEP.
KYC	See 'Know Your Customer'.
land banking scams	Land banking companies divide land into smaller plots to sell it to investors on the basis that once it is available for development it will soar in value. However, the land is often in rural areas, with little chance of planning permission being granted. See: https://www.fca.org.uk/consumers/land-banking-investment-schemes
layering	See 'placement, layering, integration'.
long firm fraud	A fraud where an apparently legitimate company is established and, over a period of time, builds up a good credit record with wholesalers, paying promptly for modest transactions. Correspondence from bankers may be used by them as evidence of good standing. The company then places a large order, takes delivery, but disappears without paying. This type of fraud is not limited to wholesalers of physical goods: financial firms have been victim to variants of this scam.
MLRO	See 'Money Laundering Reporting Officer'.
mass-marketing fraud	Action Fraud (the UK's national fraud reporting centre) says "Mass marketing fraud is when you receive an uninvited contact by email, letter, phone or adverts, making false promises to con you out of money." Share sale fraud is a type of mass marketing fraud.

Term	Meaning
	See: www.actionfraud.police.uk/types-of-fraud/mass-marketing-fraud
Missing Trader Inter-Community (MTIC) fraud	This fraud exploits the EU system for rebating Value Added Tax payments in situations where goods have moved across borders within the EU. National authorities are misled into giving rebates to import-export companies that are not entitled to them.
money laundering	The process by which the proceeds of crime are converted into assets which appear to have a legitimate origin, so that they can be retained permanently, or recycled to fund further crime.
Money Laundering Directive	See 'Fourth Money Laundering Directive'.
Money Laundering Reporting Officer (MLRO)	The MLRO is responsible for ensuring that measures to combat money laundering within the firm are effective. The MLRO is also usually the 'nominated officer' under the Proceeds of Crime Act (POCA). The MLRO is a 'controlled function' under the Approved Persons Regime and a 'senior management function' under the Senior Managers and Certification Regime.
Market Abuse Regulation (MAR)	MAR, short for Market Abuse Regulation (EU No.596/2014), entered into force on 3 July 2016. It contains the civil offences of insider dealing, unlawful disclosure of inside information and market manipulation, in addition to provisions to prevent and detect these offences.
Money Laundering Regulations	The Money Laundering Regulations 2007 (SI 2007/2157) transposed the Third Money Laundering Directive into UK law. The Regulations require firms to take specified steps to detect and prevent both money laundering and terrorist financing. The Money Laundering Regulations 2007 were revoked and replaced by the Money Laundering Regulations 2017.
Money Laundering Regulations 2017	The Money Laundering Regulations 2017 (SI 2017/692) transpose the requirements of the Third Fourth Money Laundering Directive into UK law. The Regulations require firms to take specified steps to detect and prevent both money laundering and terrorist financing. The Regulations identify the firms we supervise and impose on us a duty to take measures to secure those firms' compliance with the Regulations' requirements.
Money Laundering Reporting Officer (MLRO)	The MLRO is responsible for ensuring that measures to combat money laundering within the firm are effective. The MLRO is also usually the 'nominated officer' under the Proceeds of Crime Act (POCA). The MLRO is a 'controlled function' under the Approved Persons Regime and a 'senior management function' under the Senior Managers and Certification Regime.
money service business (MSB)	An undertaking that by way of business operates a currency exchange office, transmits money (or any representations of monetary value) by any means or which cashes cheques which are made payable to customers. (See Regulation 3(1) of the *Money Laundering Regulations*.) Firms authorised under FSMA must inform us if they provide MSB services. For more information about this, see: https://www.fca.org.uk/firms/money-laundering-terrorist-financing/reporting HM Revenue and Customs supervises the AML controls of money service businesses that are not authorised under FSMA. More information about registration with HMRC can be found on its website:https://www.gov.uk/topic/business-tax/money-laundering-regulations

Term	Meaning
mortgage brokers, general insurers and general insurance intermediaries	Mortgage brokers, general insurers (including managing agents and the Society of Lloyd's) and general insurance intermediaries are subject to the high-level regulatory requirement to counter financial crime set out in SYSC 3.2.6R. However, they are not subject to the *Money Laundering Regulations* or the provisions of the *Handbook* that specifically relate to money laundering (SYSC 3.2.6AR –SYSC 3.2.6JG). Firms offering these services alongside other products that are subject to the *Money Laundering Regulations* (such as banking and stock broking services) can therefore apply different customer due diligence checks in both situations. But in practice, many will choose to apply a consistent approach for the sake of operational convenience.
MSB	See 'money service business'.
MTIC	See 'Missing Trader Inter-Community Fraud'.
National Crime Agency (NCA)	The NCA leads the UK's fight against serious and organised crime. It became operational, replacing the Serious Organised Crime Agency, in October 2013. For more information see the NCA's website:http://www.nationalcrimeagency.gov.uk/ .
NCA	See 'National Crime Agency'.
NCCT	See 'non-cooperative countries or territories'.
nominated officer	Regulation 3(1) of the *Money Laundering Regulations* defines this as "a person who is nominated to receive disclosures under Part 3 (terrorist property) of the Terrorism Act 2000 or Part 7 (money laundering) of the Proceeds of Crime Act 2002". See section 330 of POCA, Part 3 of the Terrorism Act 2000, and Regulation 21(3) of the *Money Laundering Regulations* which requires all firms to appoint a nominated officer.
non-cooperative countries and territories	FATF can designate certain countries and territories as being non-cooperative. This indicates severe weaknesses in anti-money laundering arrangements in those jurisdictions. An up-to-date statement can be found on the FATF website. The JMLSG has prepared guidance for firms on how to judge the risks of conducting business in different countries.
occasional transaction	Any transaction (carried out other than as part of a business relationship) amounting to €15,000 or more, whether the transaction is carried out in a single operation or several operations which appear to be linked. (See Regulation 27(2) of the *Money Laundering Regulations*.) Any transaction that amounts to a transfer of funds within the meaning of article 3(9) of the Funds Transfer Regulation exceeding €1,000.
Office of Financial Sanctions Implementation (OFSI)	The Office of Financial Sanctions Implementation within HM Treasury is responsible for the implementation and administration of the UK sanctions regime. See: https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation for more.
ongoing monitoring	The *Money Laundering Regulations* require ongoing monitoring of business relationships. This means that the transactions performed by a customer, and other aspects of their behaviour, are scrutinised throughout the course of their relationship with the firm. The intention is to spot where a customer's actions are inconsistent with what might be expected of a customer of that type, given what is known about their business, risk profile etc. Where the risk associated with the business relationship is increased, firms must enhance their ongoing monitoring on a risk-sensitive

Term	Meaning
	basis. Firms must also update the information they hold on customers for anti-money laundering purposes.
payment institutions	A 'payment institution' is a UK firm which is required under the Payment Services Regulations 2017 (SI 2017/752) to be authorised or registered in order to provide payment services in the UK. This term is not used to describe payment service providers that are already authorised by us because they carry out regulated activities (such as banks and e-money institutions) or that are exempt under the Payment Services Regulations (such as credit unions). For more information, see our publication. For the *FCA's* approach to Payment institutions and e-money institutions under the *Payment Services Regulations* and the *Electronic Money Regulations*, see https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf.
PEP	See 'politically exposed person'.
placement, layering, integration	The three stages in a common model of money laundering. In the placement stage, money generated from criminal activity (e.g. funds from the illegal import of narcotics) is first introduced to the financial system. The layering phase sees the launderer entering into a series of transactions (e.g. buying, and then cancelling, an insurance policy) designed to conceal the illicit origins of the funds. Once the funds are so far removed from their criminal source that it is not feasible for the authorities to trace their origins, the integration stage allows the funds to be treated as ostensibly 'clean' money.
POCA	See 'Proceeds of Crime Act 2002'.
politically exposed person (PEP)	A person entrusted with a prominent public function. See Regulation 35 of the *Money Laundering Regulations* and Finalised Guidance 'FG17/16: The treatment of politically exposed persons for anti-money laundering purposes' https://www.fca.org.uk/publications/finalised-guidance/fg17-6-treatment-politically-exposed-persons-peps-money-laundering.
Ponzi and pyramid schemes	Ponzi and pyramid schemes promise investors high returns or dividends not usually available through traditional investments. While they may meet this promise to early investors, people who invest in the scheme later usually lose their money; these schemes collapse when the unsustainable supply of new investors dries up. Investors usually find most or all of their money is gone, and the fraudsters who set up the scheme have disappeared.
Proceeds of Crime Act 2002 (POCA)	POCA criminalises all forms of money laundering and creates other offences such as failing to report a suspicion of money laundering and 'tipping off'.
Production Order	The Proceeds of Crime Act 2002 allows Financial Investigators to use production orders to obtain information from financial firms about an individual's financial affairs.
Proliferation finance	Funding the proliferation of weapons of mass destruction in contravention of international law.
pyramid schemes	See 'Ponzi and pyramid schemes'.
Recognised investment exchanges, and recognised clearing houses	To be recognised under FSMA, exchanges and clearing houses must, among other things, adopt appropriate measures to: • reduce the extent to which their facilities can be used for a purpose connected with market abuse or financial crime; and • monitor the incidence of market abuse or financial crime, and facilitate its detection.

Term	Meaning
	Measures should include the monitoring of transactions. This is set out *REC*, which contains our guidance on our interpretation of the recognition requirements. It also explains the factors we may consider when assessing a recognised body's compliance with the requirements. Regulation 7(1)(a)(vii) of the *Money Laundering Regulations* confers supervisory functions on the *FCA* to oversee recognised investment exchanges' compliance with requirements imposed on them by those regulations.
reliance	The *Money Laundering Regulations* allow a firm to rely on customer due diligence checks performed by others. However, there are many limitations on how this can be done. First, the relying firm remains liable for any failure to apply these checks. Second, the firm being relied upon must give its consent. Third, the law sets out exactly what kinds of firms may be relied upon. See Regulation 39 of the *Money Laundering Regulations* and the JMLSG guidance for more detail.
safe deposit boxes	The *FCA* is responsible for supervising anti-money laundering controls of safe custody services; this includes the provision of safe deposit boxes.
sanctions	See 'financial sanctions regime'.
SAR	See 'Suspicious Activity Report'.
Senior Management Arrangements, Systems and Controls sourcebook	See '*SYSC*'.
share sale fraud	Share scams are often run from 'boiler rooms' where fraudsters cold-call investors offering them often worthless, overpriced or even non-existent shares. While they promise high returns, those who invest usually end up losing their money. We have found victims of boiler rooms lose an average of £20,000 to these scams, with as much as £200m lost in the UK each year. Even seasoned investors have been caught out, with the biggest individual loss recorded by the police being £6m. We receive almost 5,000 calls each year from people who think they are victims of boiler room fraud. See: http://scamsmart.fca.org.uk
simplified due diligence (SDD)	Regulation 37 of the *Money Laundering Regulations* allows firms, where they assess that a business relationship or transaction presents a low degree of risk of money laundering or terrorist financing. This regulation sets out a series of factors firms should consider when determining this risk. SDD does not exempt firms from applying CDD measures but permits them to adjust the extent, timing or type of the measures it undertakes to reflect the lower risk it has assessed. A firm is required to carry out sufficient monitoring of any business relationships or transactions which are subject to those measures to enable it to detect any unusual or suspicious transactions.
Solicitors Regulation Authority (SRA)	The Solicitors Regulation Authority has supervisory responsibility for solicitors under the *Money Laundering Regulations*. The Bar Council and other professional bodies for the legal sector perform a similar role for their members. See www.sra.org.uk for more information.
Special Recommendations	See 'FATF Special Recommendations'.
source of funds and source of wealth	'Source of wealth' describes how a customer or beneficial owner acquired their total wealth. 'Source of funds' refers to the origin of the funds involved in the business relationship or occasional transaction. It refers to the activity that generated the funds, for example salary payments or

Term	Meaning
	sale proceeds, as well as the means through which the customer's or beneficial owner's funds were transferred.
SRA	See 'Solicitors Regulation Authority'.
STOR	See 'Suspicious Transaction and Order Report'.
Suspicious Activity Report (SAR)	A report made to the NCA about suspicions of money laundering or terrorist financing. This is commonly known as a 'SAR'. See also 'Suspicious Transaction Report'.
Suspicious Transaction and Order Report (STOR)	A report made to the *FCA* in accordance with articles 16(1) and 16(2) of the *Market Abuse Regulation* about any suspicious order or transaction. For more see: https://www.fca.org.uk/markets/market-abuse/suspicious-transaction-order-reports/stor-supervisory-priorities
SWIFT	SWIFT (the Society for Worldwide Interbank Financial Telecommunication) provides the international system used by banks to send the messages that effect interbank payments.
SYSC	*SYSC* is the Senior Management Arrangements, Systems and Controls sourcebook of the *Handbook*. It sets out the responsibilities of directors and senior management. *SYSC* includes rules and guidance about firms' anti-financial crime systems and controls. These impose obligations to establish and maintain effective systems and controls for countering the risk that the firm might be used to further financial crime' (see SYSC 6.1.1R, or for insurers, managing agents and Lloyd's, SYSC 3.2.6R). SYSC 6.3 contains anti-money laundering specific rules and guidance. These provisions are also set out in SYSC 3.2.6AR to SYSC 3.2.6JG as they apply to certain insurers, managing agents and Lloyd's. These money laundering specific provisions of *SYSC* do not apply to mortgage brokers, general insurers and general insurance intermediaries.
terrorist finance	The provision of funds or other assets to support a terrorist ideology, a terrorist infrastructure or individual operations. It applies to domestic and international terrorism.
TF	Terrorist financing (also 'CTF').
third party	'Third party' is a term often used to refer to entities that are involved in a business or other transaction but are neither the firm nor its customer. Where a third party acts on a firm's behalf, it might expose the firm to financial crime risk.
tipping off	The offence of tipping off is committed where a person discloses that: • any person has made a report under the Proceeds of Crime Act 2002 to the Police, HM Revenue and Customs or the NCA concerning money laundering, where that disclosure is likely to prejudice any investigation into the report; or • an investigation into allegations that an offence of money laundering has been committed, is being contemplated or is being carried out. See section 333A of the Proceeds of Crime Act 2002. A similar offence exists in relation to terrorism (including terrorism financing) by virtue of section 21D of the Terrorism Act 2000.
trade sanctions	Government restrictions on the import or export of certain goods and services, often to or from specific countries, to advance foreign policy objectives. See 'economic sanctions'.

Term	Meaning
Treasury	The Treasury is the UK government's AML policy lead. It also implements the UK's financial sanctions regime through OFSI.
trust or company service provision	A formal legal definition of 'trust or company service provider' is given in Regulation 12(2) of the *Money Laundering Regulations*. A simple definition might be 'an enterprise whose business creates, or enables the creation of, trusts and companies on behalf of others for a fee'. International standard setters have judged that such services can be abused by those seeking to set up corporate entities designed to disguise the true origins of illicit funds. The firms we authorise must inform us if they provide trust or company services. For more information about this, see: https://www.fca.org.uk/firms/money-laundering-terrorist-financing/reporting Trust or company service providers that are not authorised by us have their anti-money laundering controls supervised by HM Revenue and Customs. More information can be found at its website: https://www.gov.uk/topic/business-tax/money-laundering-regulations
verification	Making sure the customer or beneficial owner is who they claim to be. Regulation 28 of the *Money Laundering Regulations* requires the customer's identity to be verified on the basis of documents or information in either case obtained from a reliable source which is independent of the person whose identity is being verified. This includes documents issued or made available by an official body even if they are provided or made available to the firm by or on behalf of the customer. It also refers to checking any beneficial owner in a way that the firm is satisfied that it knows who the beneficial owner is; see Regulation 5 of the *Money Laundering Regulations*.
Wolfsberg Group	An association of global banks, including UK institutions, which aims to 'develop financial services industry standards, and related products, for Know Your Customer, Anti-Money Laundering and Counter Terrorist Financing policies'. See its website for more: www.wolfsberg-principles.com

FCG Annex : Common terms