Financial Conduct Authority

Financial crime: a guide for firms

Part 1: A firm's guide to preventing financial crime

April 2015

Contents

About the Guide:

- This Guide consolidates FCA guidance on financial crime. It does not contain rules and its contents are not binding.
- It provides guidance to firms on steps they can take to reduce their financial crime risk.
- The Guide aims to enhance understanding of FCA expectations and help firms to assess the adequacy of their financial crime systems and controls and remedy deficiencies.
- It is designed to help firms adopt a more effective, risk-based and outcomes-focused approach to mitigating financial crime risk.
- The Guide does not include guidance on all the financial crime risks a firm may face. The self-assessment questions and good and poor practice we use in the Guide are not exhaustive.
- The good practice examples present ways, but not the only ways, in which firms might comply with applicable rules and requirements.
- Similarly, there are many practices we would consider poor that we have not identified as such in the Guide. Some poor practices may be poor enough to breach applicable requirements.
- The Guide is not the only source of guidance on financial crime. Firms are reminded that other bodies produce guidance that may also be relevant and useful.
- Guidance in the Guide should be applied in a risk-based, proportionate way. This includes taking into account the size, nature and complexity of a firm when deciding whether a certain example of good or poor practice is appropriate to its business.
- This Guide is not a checklist of things that all firms must do or not do to reduce their financial crime risk, and should not be used as such by firms or FCA supervisors.

1. Introduction

1.1 This Guide 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 FSA thematic reviews, with some additional material included to reflect other aspects of our financial crime remit. The Guide does not cover market misconduct, detailed rules and guidance on which are contained in the Market Conduct (MAR) sourcebook.

1.2 Effective systems and controls can help firms to detect, prevent and deter financial crime. Part 1 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 Part 1 is a list of common and useful terms. The Annex is provided for reference purposes only and is not a list of 'defined terms'. The Guide does not use the Handbook Glossary of definitions unless otherwise indicated.

1.3 Part 2 provides summaries of, and links to, FSA 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.

1.4 We will keep the Guide 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.

1.5 The material in the Guide 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 prevent 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 2.1.2P; and
- in relation to guidance on money laundering, the rules in SYSC 3.2.6AR to SYSC 3.2.6JG and SYSC 6.3 (Financial crime).

Where the Guide 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 2009 and the Electronic Money Regulations 2011.

1.6 Direct references in Part 1 to requirements set out in our rules or other legal provisions include a cross reference to the relevant provision.

1.7 The Guide contains 'general guidance' as defined in section 158 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.

1.8 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 this Guide. 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*, p.24; paragraph 6.2.1G (4) of the Decision Procedures and Penalties (DEPP) manual of the Handbook and paragraphs 2.22 – 2.27 of our Enforcement Guide (EG).

1.9 The Guide also contains guidance on how firms can meet the requirements of the Money Laundering Regulations 2007 and the EU Wire Transfer Regulation. This guidance is not 'relevant guidance' as described in Regulations 42(3) or 45(2) of the Money Laundering Regulations, or Regulation 14 of the Transfer of Funds (Information on the Payer) Regulations 2007 (which gives the FCA powers and responsibilities to supervise firms' compliance with the EU Wire Transfer Regulation). This means that a decision maker is not required to consider whether a person followed the guidance when it is deciding whether that person has breached these regulations, although they may choose to do so.

1.10 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' under these regulations. As confirmed in DEPP 6.2.3G, EG 12.2 and EG 19.82 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.

1.11 The Guide 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 the Guide 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.

How to use this Guide

1.12 Throughout the Guide, material is set out as follows:

Who should read this chapter? This box 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.

Content: This box lists the sections in each chapter.

1.13 Each section discusses how firms tackle a different type of financial crime. Sections open with a short passage giving context to what follows. In this Guide, 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.

1.14 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 Box 2.1 (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 Box 3.5 (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 Box 4.1 (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.

Box 1.1: Financial crime: a guide for firms

The Guide 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 box provides **illustrative** examples of **good practices.** • Good practice examples are drawn from **conduct seen** in firms during thematic work in relation to financial crime. • We would draw comfort from seeing **evidence** that these practices take place. • 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.	• This box provides **illustrative** examples of **poor practices**. • Poor practice examples are also drawn from **conduct seen** during thematic work. • 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**. • These **do not identify all cases** where conduct may give rise to regulatory breaches or criminal offences.

Boxes like this list obligations directly referred to in the text.

Box 1.2: Case studies and other information

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.

1.15 Where to find out more:

- Most sections close with some sources of further information.
- This includes cross-references to relevant guidance in Part 2 of the Guide.
- It also includes links to external websites and materials. Although the external links are included to assist readers of the Guide, we are not responsible for the content of these, as we neither produce nor maintain them.

2.
Financial crime systems and controls

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.

The **Annex 1 financial institutions** which we supervise for compliance with their obligations under the Money Laundering Regulations 2007 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.

Content: This chapter contains sections on:

SYSC 6.1.1R
SYSC 3.2.6R

2.1 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.

Box 2.1: Governance

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.

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

- Senior management **set the right tone** and demonstrate leadership on financial crime issues.
- A firm takes **active steps** to prevent criminals taking advantage of its services.
- We would draw comfort from seeing evidence that these practices take place.
- There are clear criteria for **escalating** financial crime issues.

Examples of poor practice

- There is little evidence of senior staff **involvement** and **challenge** in practice.
- A firm concentrates on **narrow compliance** with **minimum regulatory standards** and has little engagement with the issues.
- Financial crime issues are dealt with on a purely **reactive** basis.
- There is **no meaningful record** or evidence of senior management considering financial crime risks.

Box 2.1A: Management Information (MI)

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 customer-facing staff, the compliance department, internal audit, the MLRO or the nominated officer.

Box 2.2: Structure

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. • Management responsible for financial crime are **sufficiently senior** as well as being credible, independent, and experienced. • A firm has considered how counter-fraud and anti-money laundering efforts can **complement** each other. • 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.	• The firm makes no effort to understand or address **gaps** in its financial crime defences. • Financial crime officers are relatively **junior** and lack access to senior management. They are often **overruled** without documented justification. • Financial crime departments are **under-resourced** and senior management are reluctant to address this.

Box 2.3: Risk assessment

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

SYSC 3.2.6R
SYSC 6.1.1R

Box 2.4: Policies and procedures

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. • Policies and procedures are **regularly reviewed** and **updated**. • **Internal audit** or another independent party monitors the effectiveness of policies, procedures, systems and controls.	• A firm has no **written policies** and **procedures**. • The firm **does not tailor** externally produced policies and procedures to suit its business. • 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**.

Box 2.5: Staff recruitment, vetting, training, awareness and remuneration

SYSC 3.1.6R
SYSC 5.1.1R

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**. • **Temporary staff** in higher risk roles are subject to the same level of vetting as permanent members of staff in similar roles. • Where **employment agencies** are used, the firm periodically satisfies itself that the agency is adhering to the agreed vetting standard. • **Tailored** training is in place to ensure staff knowledge is adequate and up to date. • New staff in **customer-facing** positions receive financial crime training tailored to their role before being able to interact with customers. • Training has a strong **practical** dimension (e.g. case studies) and some form of testing. • The firm satisfies itself that staff **understand** their responsibilities (e.g. computerised training contains a test). • **Whistleblowing** procedures are clear and accessible, and respect staff confidentiality.	• Staff are **not competent** to carry out preventative functions effectively, exposing the firm to financial crime risk. • Staff vetting is a **one-off** exercise. • The firm fails to **identify changes** that could affect an individual's integrity and suitability. • The firm **limits enhanced vetting** to senior management roles and fails to vet staff whose roles expose them to higher financial crime risk. • 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.** • Poor compliance records are not reflected in **staff appraisals and remuneration**. • Training dwells unduly on **legislation and regulations** rather than practical examples. • 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.

Box 2.6: Quality of oversight

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. • 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.	• Compliance unit and audit teams **lack experience** in financial crime matters. • Audit findings and compliance conclusions are **not shared** between business units. Lessons are not spread more widely.

2.2 Part 2 of the Guide contains the following additional guidance on **governance**:

- Box 6.1 (Governance), from the *FSA's* thematic review *Data security in Financial Services*
- Box 8.1 (Senior management responsibility) from the *FSA's* thematic review *Financial services firms' approach to UK financial sanctions*
- Box 9.1 (Governance and management information) from the *FSA's* thematic review *Anti-bribery and corruption in commercial insurance broking*
- Box 11.1 (Governance, culture and information sharing) from the *FSA's* thematic review *Mortgage fraud against lenders*

2.3 Part 2 contains the following additional guidance on **risk assessment**:

- Box 8.2 (Risk assessment) from the *FSA's* thematic review *Financial services firms' approach to UK financial sanctions*
- Box 9.2 (Risk assessment and responses to significant bribery and corruption events) from the *FSA's* thematic review *Anti-bribery and corruption in commercial insurance broking*
- Box 10.7 (Responsibilities and risk assessments) from the *FSA's* thematic review *The Small Firms Financial Crime Review*
- Box 12.2 (High-risk customers and PEPs – risk assessment) and Box 12.5 (Correspondent banking – risk assessment of respondent banks) from the *FSA's* thematic review *Banks' management of high money-laundering risk situations*

2.4 Part 2 contains the following additional guidance on **policies and procedures**:

- Box 8.3 (Policies and procedures) from the *FSA's* thematic review *Financial services firms' approach to UK financial sanctions*
- Box 10.1 (Regulatory/legal obligations) from the *FSA's* thematic review *The Small Firms Financial Crime Review*

- Box 12.1 (High-risk customers and PEPs – AML policies and procedures) from the *FSA's* thematic review *Banks' management of high money-laundering risk situations*

2.5 Part 2 contains the following additional guidance on **staff recruitment, vetting, training and awareness**:

- Box 6.2 (Training and awareness) and Box 6.3 (Staff recruitment and vetting) from the *FSA's* thematic review *Data security in Financial Services*
- Box 8.4 (Staff training and awareness) from the *FSA's* thematic review *Financial services firms' approach to UK financial sanctions*
- Box 9.5 (Staff recruitment and vetting) and Box 9.6 (Training and awareness) from the *FSA's* thematic review *Anti-bribery and corruption in commercial insurance broking*
- Box 10.6 (Training) from the *FSA's* thematic review *The Small Firms Financial Crime Review*
- Box 11.6 (Staff recruitment and vetting) and Box 11.8 (Staff training and awareness) from the *FSA's* thematic review *Mortgage fraud against lenders laundering risk situations*

2.6 Part 2 contains the following additional guidance on **quality of oversight**:

- Box 6.15 (Internal audit and compliance monitoring) from the *FSA's* thematic review *Data security in Financial Services*
- Box 9.9 (The role of compliance and internal audit) from the *FSA's* thematic review *Anti-bribery and corruption in commercial insurance broking*
- Box 11.5 (Compliance and internal audit) from the *FSA's* thematic review *Mortgage fraud against lenders*

2.7 For firms' obligations in relation to whistleblowers see:

- the Public Interest Disclosure Act 1998: www.legislation.gov.uk/ukpga/1998/23/contents

3.
Money laundering and terrorist financing

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 2007** (referred to in this chapter as 'the ML Regulations').

This guidance does not apply to **payment institutions**, which are supervised for compliance with the ML 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 ML Regulations.

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.

Box 3.2 (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**.

Box 3.12 (Customer payments) applies to **banks** subject to **SYSC 6.3**.

Content: This chapter contains sections on:

3.1 The guidance in this chapter relates both to our interpretation of requirements of the ML 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.

3.2 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. The Guide is not intended to replace, compete or conflict with the JMLSG's guidance, which should remain a key resource for firms.

3.3 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.

Box 3.1: Governance

The guidance in **Box 2.1** 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.

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

- **Reward structures** take account of any failings related to AML compliance.
- 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.
- 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.

Examples of poor practice

- 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.
- 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.
- The board **never considers** MLRO reports.
- A *UK branch or subsidiary* uses group policies which **do not comply** fully with UK AML legislation and regulatory requirements.

SYSC 3.2.6IR
SYSC 6.3.9R

Box 3.2: The Money Laundering Reporting Officer (MLRO)

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.

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 has a direct reporting line to executive management or the board.	• The MLRO lacks credibility and authority, whether because of inexperience or lack of seniority. • 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.

Box 3.3: Risk assessment

The guidance in **Box 2.3** on risk assessment in relation to financial crime also applies to AML.

The assessment of money-laundering risk is at the core of the firm's AML effort and is essential to the development of effective AML policies and procedures.

ML Reg 20
SYSC 3.2.6AR
SYSC 6.3.1R

Firms must therefore put in place systems and controls to identify, assess, monitor and manage money- laundering 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.

ML Reg 20;
SYSC 3.2.6CR
SYSC 6.3.3R

Self-assessment questions:

- Which parts of the business present **greater risks** of money laundering? (Has your firm identified the risks associated with different types of customer or beneficial owner, product, business line, geographical location and delivery channel (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?)

Examples of good practice

- There is evidence that the firm's risk assessment **informs** the **design** of anti-money laundering controls.
- The firm has identified **good sources of information** on money-laundering risks, such as FATF mutual evaluations and typology reports, NCA alerts, press reports, court judgements, reports by non-governmental organisations and commercial due diligence providers.
- Consideration of money-laundering 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;
  - sector risk; and
  - involvement in public contracts.
- 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.

Examples of poor practice

- An inappropriate **risk classification system** makes it almost impossible for a relationship to be classified as 'high risk'.
- Higher-risk countries are allocated low-risk scores to **avoid enhanced due diligence** measures.
- Relationship managers are able to **override customer risk scores** without sufficient evidence to support their decision.
- 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.

Box 3.4: Customer due diligence (CDD) checks

ML Regs 5, 6 and 7

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.

ML Reg 14

In situations where the money-laundering risk associated with the business relationship is increased, for example, where the customer is a PEP, banks must carry out additional, enhanced due diligence (EDD). **Box 3.7** below considers enhanced due diligence.

ML Reg 11

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.

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)?

Examples of good practice

- A firm which uses, e.g. **electronic verification checks** or **PEPs databases** understands their capabilities and limitations.
- The firm can cater for **customers who lack common forms of ID** (such as the socially excluded, 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 obtains information about the purpose and nature of the business relationship sufficient to be satisfied that it **understands** the **associated money-laundering risk**.
- Staff who approve new or ongoing business relationships satisfy themselves that the firm has obtained **adequate CDD** information before doing so.

Examples of poor practice

- Procedures are not **risk-based**: the firm applies the same CDD measures to products and customers of varying risk.
- The firm has **no method for tracking** whether checks on customers are complete.
- The firm allows **language difficulties** or **customer objections** to get in the way of proper questioning to obtain necessary CDD information.
- Staff do **less CDD** because a customer is referred by senior executives or influential people.
- The firm has **no procedures** for dealing with situations requiring enhanced due diligence. **This breaches the ML Regulations**.
- The firm fails to consider **both**:
  - any individuals who ultimately control more that 25% of shares or voting rights of; **and**
  - any individuals who exercise control over the management over

  a corporate customer when identifying and verifying the customer's beneficial owners. **This breaches the ML Regulations**.

Box 3.5: Ongoing monitoring

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 **Box 3.4**).

ML Reg 8(1)

MLR 8(2)(b)

ML Reg 7(1)(d)

Where the risk associated with the business relationship is increased, firms must carry out enhanced ongoing monitoring of the business relationship. **Box 3.8** provides guidance on enhanced ongoing monitoring.

ML Reg 14

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?

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. • Where a firm uses automated transaction monitoring systems, it understands their **capabilities** and **limitations**. • *Small firms* are able to apply credible **manual procedures** to scrutinise customers' behaviour. • The '**rules**' underpinning monitoring systems are understood by the relevant staff and updated to reflect new trends. • The firm uses **monitoring results** to review whether CDD remains adequate. • The firm takes advantage of **customer contact** as an opportunity to update due diligence information. • **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 firm fails to take adequate measures to understand the risk associated with the business relationship and is therefore **unable to conduct meaningful monitoring**. • The MLRO can provide **little evidence** that **unusual transactions** are brought to their attention. • Staff **always accept a customer's explanation** for unusual transactions at face value and do not probe further. • The firm does not take risk-sensitive measures to ensure CDD information is **up to date. This is a breach of the ML Regulations**.

ML Reg 8(2)(b)

Box 3.5A Source of wealth and source of funds

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 8 and Regulation 14 of the Money Laundering Regulations 2007 and of this Guide. Nothing in this Guide prevents the use of 'source of funds as evidence' in situations where this is appropriate.

Box 3.6: Handling higher-risk situations

ML Reg 20
ML Reg 14

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.

The ML Regulations also set out three scenarios in which specific enhanced due diligence measures have to be applied:

ML Reg 14(2)

- **Non-face-to-face CDD**: this is where the customer has not been physically present for identification purposes, perhaps because business is conducted by telephone or on the internet. ML Reg 7

ML Reg 14(3)

- **Correspondent banking**: where a correspondent bank is outside the EEA, the UK bank should thoroughly understand its correspondent's business, reputation, and the quality of its defences against money laundering and terrorist financing. Senior management must give approval to each new correspondent banking relationship.

ML Reg 14(4)

- **Politically exposed persons (PEPs)**: a PEP is a person entrusted with a prominent public function in a foreign state, an EU institution or an international body; their immediate family members; and known close associates. A senior manager at an appropriate level of authority must approve the initiation of a business relationship with a PEP. This includes approving the continuance of a relationship with an existing customer who becomes a PEP after the relationship has begun.

ML Reg 7(3)(b)

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.

Box 3.7: Handling higher-risk situations – enhanced due diligence (EDD)

ML Reg 14

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. **Box 3.3** 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. • The firm establishes the legitimacy of, and documents, the **source of wealth** and **source of funds** used in high-risk business relationships. • Where money laundering risk is very high, the firm obtains **independent** internal or external **intelligence reports**. • When assessing EDD, the firm **complements staff knowledge** of the customer or beneficial owner with more objective information. • 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 *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 proactively **follows up gaps in, and updates**, CDD of higher-risk customers. • A *correspondent bank* seeks to **identify PEPs** associated with their respondents. • 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 *correspondent bank* gathers information about **respondent banks' procedures** for sanctions screening, PEP identification and management, account monitoring and suspicious activity reporting.	• Senior management **do not give approval** for taking on high-risk customers. **If the customer is a PEP or a non-EEA correspondent bank, this breaches the ML Regulations.** • The firm fails to consider whether a customer's **political connections** mean that they are high risk despite falling outside the ML Regulations' definition of a PEP. • The firm **does not distinguish** between the customer's source of funds and their source of wealth. • The firm relies entirely on a **single source** of information for its enhanced due diligence. • 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. • The firm considers the **credit risk** posed by the customer, but not the **money-laundering risk**. • The firm **disregards** allegations of the customer's or beneficial owner's **criminal activity** from reputable sources repeated over a sustained period of time. • The firm ignores adverse allegations simply because customers hold a UK **investment visa**. • A firm grants **waivers** from establishing source of funds, source of wealth or other due diligence without good reason. • A *correspondent bank* conducts inadequate due diligence on **parents** and **affiliates** of respondents. • A *correspondent bank* **relies exclusively** on the Wolfsberg Group AML questionnaire.

ML Reg 14(4)(a); ML Reg 14(3)(d)

Box 3.8: Handling higher-risk situations – enhanced ongoing monitoring

ML Reg 14

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

- Key AML staff have a **good understanding** of, and **easy access** to, information about a bank's highest-risk customers.
- New higher-risk clients are more closely monitored to confirm or amend **expected account activity**.
- **Alert thresholds** on automated monitoring systems are lower for PEPs and other higher-risk customers. Exceptions are **escalated** to more senior staff.
- 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.

Examples of poor practice

- The firm treats annual reviews as a **tick-box exercise** and copies information from previous reviews without thought.
- *A firm in a group* relies on others in the group to carry out monitoring **without understanding** what they did and what they found.
- There is **insufficient challenge** to explanations from relationship managers and customers about unusual transactions.
- 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).

Box 3.9: Liaison with law enforcement

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 the Annex 1 list of common terms for more information about nominated officers and Suspicious Activity Reports.)

ML Reg 20(2)(d)

s.331 POCA

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 Annex 1: Common terms).

s.330 POCA

ML Reg 20(2)(d)(iii)

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?

Examples of good practice

- All staff **understand procedures for escalating suspicions** and follow them as required.
- 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).
- 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.
- There is a clear process for **documenting** decisions.
- A firm's processes for dealing with suspicions reported to it by **third party administrators** are clear and effective.

Examples of poor practice

- 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 nominated officer **dismisses concerns** escalated by staff without reasons being documented.
- 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.
- The nominated officer **turns a blind eye** where a SAR might harm the business. **This could be a criminal offence**.

s.331 POCA

- A firm provides extraneous and irrelevant detail in response to a **Production Order**.

Box 3.10: Record keeping and reliance on others

ML Reg 19
ML Reg 19(4)
ML Reg 7(3)(b)

Firms must keep copies or references to the evidence of the customer's identity for **five years** after the business relationship ends; and transactional documents for five years from the completion of the transaction. Where a firm is **relied on by others** to do due diligence checks, it must keep its records of those checks for five years from the date it was relied on. 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.

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 Annex 1), is this within the limits permitted by the ML Regulations? How does it satisfy itself that it can rely on these firms?

Examples of good practice

- Records of customer ID and transaction data can be **retrieved quickly and without delay**.
- 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.

Examples of poor practice

- 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.
- A firm cannot access CDD and related records for which it has relied on a third party. **This breaches the ML Regulations**. ML Reg 19(6)
- 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. ML Reg 7(3)(b)

Box 3.11: Countering the finance of terrorism

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 **Box 3.9**)

Examples of good practice

- The firm has and uses an effective **process** for liaison with the authorities.
- A firm identifies **sources of information** on terrorist financing risks: e.g. press reports, NCA alerts, Financial Action Task Force typologies, court judgements, etc.
- This information informs the design of **transaction monitoring systems**.
- Suspicions raised within the firm inform its own **typologies**.

Examples of poor practice

- Financial crime **training** does not mention terrorist financing.
- A *firm doing cross-border business* has not assessed terrorism-related risks in **countries** in which it has a presence or does business.
- A firm has not considered if its approach to **customer due diligence** is able to capture information relevant to the risks of terrorist finance.

Box 3.12: Customer payments

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.[1]

Self-assessment questions:

- How does your firm ensure that customer payment instructions contain **complete payer 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?

Examples of good practice

- Although **not required by EU Regulation 1781/2006 on information on the payer accompanying transfers of funds (the Wire Transfer Regulation)**, the following are examples of good practice:
  - Following processing, ***banks*** conduct **risk-based sampling** for inward payments to identify inadequate payer information.
  - An intermediary *bank* chases up **missing** information.
  - A *bank* sends dummy messages to test the effectiveness of filters.
  - 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.
- The quality of payer information in payment instructions from **respondent banks** is taken into account in the *bank's* ongoing review of correspondent banking relationships.
- The firm actively engages in **peer discussions** about taking appropriate action against banks which persistently fail to provide complete payer information.

Examples of poor practice

- A *bank* fails to make use of the correct **SWIFT message type** for cover payments.
- 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 Wire Transfer Regulation:

- International customer payment instructions sent by the payer's *bank* **lack meaningful payer information**.
- An *intermediary* bank **strips** payer information from payment instructions before passing the payment on.
- The *payee bank* does not check any **incoming payments** to see if they include complete and meaningful data about the ultimate transferor of the funds.

1 The Wire Transfer Regulation requires banks to attach information about their customers (such as names and addresses, or, if a payment moves within the EU, a unique identifier like an account number) 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 Annex 1: Common terms) 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.

Box 3.13: Case study – poor AML controls

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 *FSA's* press release for more information:
www.fsa.gov.uk/pages/Library/Communication/PR/2010/077.shtml

Box 3.14: Case studies – wire transfer failures

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.

Box 3.15: Case study – poor AML controls: PEPs and high risk customers

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 *FSA's* press release for more information:
www.fsa.gov.uk/library/communication/pr/2012/032.shtml

Box 3.16: Poor AML controls: risk assessment

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

Habib 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 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 *FSA's* press release for more information:
www.fsa.gov.uk/library/communication/pr/2012/055.shtml

3.4 Part 2 of the Guide contains the following additional AML guidance:

- Chapter 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*
- Chapter 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)*

- Chapter 10 summarises the findings of the *Small Firms Financial Crime Review*. It contains guidance directed at *small firms* on:
  - Regulatory/legal obligations (Box 10.1)
  - Account opening procedures (Box 10.2)
  - Monitoring activity (Box 10.3)
  - Suspicious activity reporting (Box 10.4)
  - Records (Box 10.5)
  - Responsibilities and risk assessments (Box 10.7)
- Chapter 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 (Box 12.1)
  - High-risk customers and PEPs – risk assessment (Box 12.2)
  - High-risk customers and PEPs – Customer take-on (Box 12.3)
  - High-risk customers and PEPs – enhanced monitoring of high-risk relationships (Box 12.4)
  - Correspondent banking – risk assessment of respondent banks (Box 12.5)
  - Correspondent banking – customer take-on (Box 12.6)
  - Correspondent banking – ongoing monitoring of respondent accounts (Box 12.7)
  - Wire transfers – paying banks (Box 12.8)
  - Wire transfers – intermediary banks (Box 12.9)
  - Wire transfers – beneficiary banks (Box 12.10)
  - Wire transfers – implementation of SWIFT MT202COV (Box 12.11)
- Part 2 also summarises the findings of the following thematic reviews:
  - Chapter 3: *Review of private banks' anti-money laundering systems and controls*
  - Chapter 7: *Review of financial crime controls in offshore centres*
  - Chapter 15: *Banks' control of financial crime risks in trade finance (2013)*

3.5 To find out more on **anti money laundering**, see:

- The Money Laundering Regulations 2007: www.legislation.gov.uk/uksi/2007/2157/contents/made

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

- 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

- Our AML self-assessment fact sheet for financial advisers: www.fca.org.uk/static/documents/fsa-aml-tool-factsheet.pdf

- The *FCA's* one-minute guide on AML for smaller firms: www.fca.org.uk/firms/being-regulated/meeting-your-obligations/firm-guides

3.6 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

- FATF's February 2008 report on terrorist financing: www.fatf-gafi.org/dataoecd/28/43/40285899.pdf

3.7 To find out more on **customer payments**, see:

- Chapter 1 of Part III (Transparency in electronic payments (Wire transfers)) of the JMLSG's guidance, which will be banks' chief source of guidance on this topic: www.jmlsg.org.uk

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

- The Wolfsberg Group's April 2007 statement on payment message standards: www.wolfsberg-principles.com/pdf/

- The Wire Transfer Regulation (EU Regulation 1781/2006 on information on the payer accompanying transfers of funds): eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006R1781:en:NOT

- Transfer of Funds (Information on the Payer) Regulations 2007: www.legislation.gov.uk/uksi/2007/3298/contents/made

4. Fraud

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:

- section 4.2 applies only to **mortgage lenders** within our supervisory scope;
- section 4.3 applies to **mortgage intermediaries** only; and
- section 4.5 applies to **retail deposit takers** only.

Content: This chapter contains sections on:

4.1 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.

4.2 The contents of the Guide'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 **paragraph 4.5**.

Box 4.1: General – preventing losses from fraud

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 **Chapter 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

- The firm takes a view on what areas of the firm are most **vulnerable** to fraudsters, and tailors defences accordingly.
- Controls adapt to **new fraud threats**.
- 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.
- **Fraud response plans and investigation procedures** set out how the firm will respond to incidents of fraud.
- **Lessons** are learnt from incidents of fraud.
- **Anti-fraud good practice** is shared widely within the firm.
- 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 Annex 1 for common terms) are in place.
- **Enhanced due diligence** is performed on higher-risk customers (e.g. commercial customers with limited financial history. See 'long firm fraud' in Annex 1).

Examples of poor practice

- Senior management appear **unaware** of fraud incidents and trends. No management information is produced.
- **Fraud losses are buried** in bad debts or other losses.
- There is no clear and consistent **definition** of fraud across the business, so reporting is haphazard.
- Fraud risks are not explored when **new products** and **delivery channels** are developed.
- 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).
- **Sales incentives** act to encourage staff or management to turn a blind eye to potential fraud.
- *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.
- **Remuneration structures** may incentivise behaviour that increases the risk of mortgage fraud.

Box 4.2: Mortgage fraud – lenders

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

- A firm's underwriting process can **identify** applications that may present a **higher risk** of mortgage fraud.
- Membership of a *lender's* **panels** of brokers, conveyancers and valuers is subject to ongoing review. Dormant third parties are identified.
- A *lender* **reviews existing mortgage books** to identify and assess mortgage fraud indicators.
- A *lender* verifies that funds are being dispersed in **line with instructions** before it releases them.
- A *lender* **promptly discharges** mortgages that have been redeemed and checks whether conveyancers register charges with the **Land Registry** in good time.

Examples of poor practice

- A *lender* fails to report relevant information to the *FCA's* **Information from Lenders** (IFL) scheme as per *FCA* guidance on IFL referrals.
- A *lender* **lacks a clear definition** of mortgage fraud, undermining data collection and trend analysis.
- A *lender's* panels of conveyancers, brokers and valuers are **too large to be manageable**.
- The *lender* does no work to identify **dormant parties**.
- A *lender* relies solely on the Financial Services Register when **vetting brokers**.
- Underwriters' demanding work targets **undermine** efforts to contain mortgage fraud.

Box 4.3: Mortgage fraud – intermediaries

This section applies to *mortgage intermediaries*.

Self-assessment questions:

- How 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. • Using the *FCA's* **Information from Brokers** scheme to report intermediaries it suspects of involvement in mortgage fraud.	• Failing to undertake due diligence on **introducers**. • Accepting all applicant information at **face value**. • Treating due diligence as the **lender's responsibility**.

Box 4.4: Enforcement action against mortgage brokers

Since the *FSA* began regulating mortgage brokers in October 2004, the *FSA* have banned over 100 mortgage brokers. Breaches 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 *FSA* have referred numerous cases to law enforcement, a number of which have resulted in criminal convictions.

Box 4.5: Investment fraud

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 contacts customers if it suspects a payment is being made to an investment fraudster. • A bank has transaction monitoring rules designed to detect specific types of investment fraud. Investment fraud subject matter experts help set these rules.	• A bank has performed no risk assessment that considers the risk to customers from investment fraud. • A bank fails to use actionable, credible information it has about known or suspected perpetrators of investment fraud in its financial crime prevention systems. • 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.

4.3 Part 2 of the Guide contains the following additional material on fraud:

- Chapter 10 summarises the findings of the *Small Firms Financial Crime Review*. It contains guidance directed at *small firms* on:
  - Monitoring activity (Box 10.3)
  - Responsibilities and risk assessments (Box 10.7)
  - General fraud (Box 10.13)
  - Insurance fraud (Box 10.14)
  - Investment fraud (Box 10.15)

- Mortgage fraud (Box 10.16)
- Staff/internal fraud (Box 10.17)

- Chapter 11 summarises the findings of the *FSA's* thematic review *Mortgage fraud against lenders*. It contains guidance on:
  - Governance, culture and information sharing (Box 11.1)
  - Applications processing and underwriting (Box 11.2)
- Chapter 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 (Box 14.1)
  - Risk assessment (Box 14.2)
  - Detecting perpetrators (Box 14.3)
  - Automated monitoring (Box 14.4)
  - Protecting victims (Box 14.5)
  - Management reporting and escalation of suspicions (Box 14.6)
  - Staff awareness (Box 14.7)
  - Use of industry intelligence (Box 14.8)
  - Mortgage fraud prevention, investigations and recoveries (Box 11.3)
  - Managing relationships with conveyancers, brokers and valuers (Box 11.4)
  - Compliance and internal audit (Box 11.5)
  - Staff recruitment and vetting (Box 11.6)
  - Remuneration structures (Box 11.7)
  - Staff training and awareness (Box 11.8)

  Part 2, Chapter 2 summarises the *FSA's* thematic review *Firms' high-level management of fraud risk*.

4.4 To find out more about what FCA is doing about fraud, see:

- Details of the FCA's Information from Lenders scheme: www.fca.org.uk/about/what/protecting/financial-crime/fraud/mortgage
- Details of the FCA's Information from Brokers scheme: www.fca.org.uk/firms/firm-types/mortgage-brokers-and-home-finance-lenders/report

- Our fact sheet for mortgage brokers on mortgage fraud:
  www.fsa.gov.uk/smallfirms/resources/factsheets/pdfs/mortgage_fraud.pdf

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

- The National Fraud Authority, which works with the counter-fraud community to make fraud more difficult to commit in and against the UK:
  www.homeoffice.gov.uk/agencies-public-bodies/nfa/

- The National Fraud Authority's cross-sector strategy, Fighting Fraud Together. The strategy, which the FCA endorses, aims to reduce fraud:
  www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/fightrging-fraud-tog/fighting-fraud-together

- Action Fraud, which is the UK's national fraud reporting centre:
  www.actionfraud.org.uk/

- The City of London Police, which has 'lead authority' status in the UK for the investigation of economic crime, including fraud:
  www.cityoflondon.police.uk/CityPolice/Departments/ECD/Fraud/

- The Fraud Advisory Panel, which acts as an independent voice and supporter of the counter fraud community:
  www.fraudadvisorypanel.org/

5.
Data security

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.

Content: This chapter contains sections on:

5.1 Customers routinely entrust financial firms with important personal data; if this falls into criminal hands, fraudsters can attempt to undertake financial 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.

s.4 and Sch 1 Data Protection Act 1998

Box 5.1: Governance

The guidance in **Box 2.1** 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

- There is a clear **figurehead** championing the issue of data security.
- Work, including by internal audit and compliance, is **coordinated** across the firm, with compliance, audit, HR, security and IT all playing a role.
- 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 firm **monitors accounts** following a data loss to spot unusual transactions.
- The firm looks at **outsourcers'** data security practices before doing business, and monitors compliance.

Examples of poor practice

- The firm does not **contact customers** after their data is lost or compromised.
- Data security is treated as an **IT** or **privacy issue**, without also recognising the financial crime risk.
- A '**blame culture**' discourages staff from reporting data losses.
- The firm is unsure how its **third parties**, such as suppliers, protect customer data.

Box 5.2: Five fallacies of data loss and identity fraud

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.

Box 5.3: Controls

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

- **Access** to sensitive areas (call centres, server rooms, filing rooms) is restricted.
- The firm has **individual user accounts** for all systems containing customer data.
- The firm conducts risk-based, **proactive monitoring** to ensure employees' access to customer data is for a genuine business reason.
- IT equipment is disposed of responsibly, e.g. by using a contractor **accredited** by the British Security Industry Association.
- Customer data in electronic form (e.g. on USB sticks, CDs, hard disks, etc), is always **encrypted** when taken off-site.
- The firm understands what checks are done by **employment agencies** it uses.

Examples of poor practice

- Staff and third-party suppliers can access **data they do not** need for their role.
- Files are not **locked away**.
- Password standards are not robust and individuals **share passwords**.
- The firm **fails to monitor** superusers or other staff with access to large amounts of customer data.
- Computers are disposed of or transferred to new users without data being **wiped**.
- 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.

Box 5.4: Case study – protecting customers' accounts from criminals

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 *FSA's* press release:
www.fsa.gov.uk/pages/Library/Communication/PR/2007/130.shtml

Box 5.5: Case study – data security failings

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

- 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 *FSA's* press release has more details:
www.fsa.gov.uk/pages/Library/Communication/PR/2010/134.shtml

5.2 Part 2 of the Guide contains the following additional material on data security:

- Chapter 6 summarises the findings of the FSA's thematic review of *Data security in Financial Services* and includes guidance on:
  - Governance (Box 6.1)
  - Training and awareness (Box 6.2)
  - Staff recruitment and vetting (Box 6.3)
  - Controls – access rights (Box 6.4)
  - Controls – passwords and user accounts (Box 6.5)
  - Controls – monitoring access to customer data (Box 6.6)
  - Controls – data back-up (Box 6.7)
  - Controls – access to the internet and email (Box 6.8)
  - Controls – key-logging devices (Box 6.9)
  - Controls – laptop (Box 6.10)
  - Controls – portable media including USB devices and CDs (Box 6.11)
  - Controls – physical security (Box 6.12)
  - Controls – disposal of customer data (Box 6.13)
  - Managing third-party suppliers (Box 6.14)
  - Internal audit and compliance monitoring (Box 6.15)
- Chapter 10 summarises the findings of the *Small Firms Financial Crime Review*, and contains guidance directed at *small firms* on:
  - Records (Box 10.5)
  - Responsibilities and risk assessments (Box 10.7)
  - Access to systems (Box 10.8)
  - Outsourcing (Box 10.9)
  - Physical controls (Box 10.10)
  - Data disposal (Box 10.11)
  - Data compromise incidents (Box 10.12)

5.3 To find out more, see:

- The website of the Information Commissioner's Office: www.ico.gov.uk
- A one-minute guide for small firms on data security: www.fca.org.uk/firms/being-regulated/meeting-your-obligations/firm-guides/information-gathering/data-security

6.
Bribery and corruption

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.

Content: This chapter contains sections on:

6.1 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.

6.2 The FCA does not enforce or give guidance on the Bribery Act. But:

SYSC 3.2.6R
SYSC 6.1.1R

- 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 Reg 6
Payment Service Reg 6

- e-money institutions and payment institutions must satisfy us that they have robust governance, effective risk procedures and adequate internal control mechanisms.

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.

PRIN 2.1.1R: Principle 1

6.3 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.

Box 6.1: Governance

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

- The firm is committed to carrying out business fairly, honestly and openly.
- Senior management lead by example in complying with the firm's anti-corruption policies and procedures
- 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 reference and senior management membership who reports ultimately to the board.
- 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.

Examples of poor practice

- There is a lack of awareness of, or engagement in, anti-bribery and corruption at senior management or board level.
- An 'ask no questions' culture sees management turn a blind eye to how new business is generated.
- 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 relationships or payments; the systems and controls to mitigate those risks; the effectiveness of these systems and controls; and legal and regulatory developments.

Box 6.2: Risk assessment

The guidance in **Box 2.3** 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

- Corruption risks are assessed in **all jurisdictions** where the firm operates and across all business channels.
- 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.

Examples of poor practice

- Departments responsible for identifying and assessing bribery and corruption risk are ill equipped to do so.
- 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**.

Box 6.3: Policies and procedures

The guidance in **Box 2.4** on policies and procedures in relation to financial crime and in Box 2.5 on staff recruitment, vetting, training, awareness and remuneration also applies to bribery and corruption.

SYSC 3.2.6R
SYSC 6.1.1R

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 standalone 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. • Risk-based, appropriate additional monitoring and due diligence are undertaken for jurisdictions, sectors and business relationships identified as **higher risk**. • Staff responsible for implementing and monitoring anti-bribery and corruption policies and procedures have adequate levels of **anti-corruption expertise**. • 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. • **Political and charitable donations** are subject to appropriate due diligence and are approved at an appropriate management level, with compliance input. • 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 **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**. • A firm relies on passages in the staff code of conduct that prohibit improper payments, but has no other **controls**. • The firm does not **record** corporate hospitality given or received. • The firm **does not respond** to external events that may highlight weaknesses in its anti-corruption systems and controls. • 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**. • The firm fails to maintain **records of incidents and complaints**.

Box 6.4: Dealing with third parties

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

- Where a firm uses third parties to generate business, these relationships are subject to **thorough due diligence** and management oversight.
- 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**.
- Third parties are paid **directly** for their work.
- The firm includes **specific anti-bribery and corruption clauses** in contracts with third parties.
- The firm provides **anti-bribery and corruption training** to third parties where appropriate.
- The firm **reviews and monitors** payments to third parties. It records the purpose of third-party payments.
- There are higher or extra levels of due diligence and approval for **high-risk third-party relationships**.
- 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.

Examples of poor practice

- *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 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?
- The firm is **unable to produce a list** of approved third parties, associated due diligence and details of payments made to them.
- The firm does not discourage the giving or receipt of **cash gifts**.
- There is **no checking** of compliance's operational role in approving new third-party relationships and accounts.
- A firm **assumes** that long-standing third-party relationships present no bribery or corruption risk.
- A firm relies exclusively on **informal** means to assess the bribery and corruption risks associated with third parties, such as staff's personal knowledge of the relationship with the overseas third parties.

Box 6.5: Case study – corruption risk

In January 2009, Aon Limited, an insurance intermediary based in the UK, was fined £5.25m for failures in its anti-bribery systems and controls.

The firm made suspicious payments totalling $7m to overseas firms and individuals who helped generate business in higher-risk jurisdictions. Weak controls surrounding these payments to third parties meant the firm failed to question their nature and purpose when it ought to have been reasonably obvious to it that there was a significant corruption risk.

- Aon Limited failed properly to assess the risks involved in its dealings with overseas third parties and implement effective controls to mitigate those risks.
- Its payment procedures did not require adequate levels of due diligence to be carried out.
- Its authorisation process did not take into account the higher levels of risk to which certain parts of its business were exposed in the countries in which they operated.
- After establishment, neither relationships nor payments were routinely reviewed or monitored.
- Aon Limited did not provide relevant staff with sufficient guidance or training on the bribery and corruption risks involved in dealings with overseas third parties.
- It failed to ensure that the committees it appointed to oversee these risks received relevant management information or routinely assessed whether bribery and corruption risks were being managed effectively.

See the *FSA's* press release:
www.fsa.gov.uk/pages/Library/Communication/PR/2009/004.shtml

Box 6.6: Case study – inadequate anti-bribery and corruption systems and controls

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 *FSA's* press release:
www.fsa.gov.uk/pages/Library/Communication/PR/2011/066.shtml.

6.4 Part 2 of the Guide contains the following additional material on bribery and corruption:

- Chapter 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 (Box 9.1)
  - Risk assessment and responses to significant bribery and corruption events (Box 9.2)
  - Due diligence on third-party relationships (Box 9.3)
  - Payment controls (Box 9.4)
  - Staff recruitment and vetting (Box 9.5)
  - Training and awareness (Box 9.6)
  - Risk arising from remuneration structures (Box 9.7)
  - Incident reporting (Box 9.8)
  - The role of compliance and internal audit (Box 9.9)
- Chapter 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 (MI) (Box 13.1)
  - Assessing bribery and corruption risk (Box 13.2)
  - Policies and procedures (Box 13.3)
  - Third-party relationships and due diligence (Box 13.4)
  - Payment controls (Box 13.5)
  - Gifts and hospitality (GH) (Box 13.6)
  - Staff recruitment and vetting (Box 13.7)
  - Training and awareness (Box 13.8)
  - Remuneration structures (Box 13.9)
  - Incident reporting and management (Box 13.10)

6.5 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: www.justice.gov.uk/downloads/guidance/making-reviewing-law/bribery-act-2010-guidance.pdf (full version)

  www.justice.gov.uk/downloads/guidance/making-reviewing-law/bribery-act-2010-quick-start-guide.pdf (quick-start guide)

- Our one-minute guide for smaller firms on anti-bribery and corruption: http://www.fca.org.uk/firms/being-regulated/meeting-your-obligations/firm-guides/systems/anti-bribery

7.
Sanctions and asset freezes

Who should read this chapter? All firms are required to comply with the UK's financial sanctions regime. 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** within our supervisory scope.

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 FSA-supervised firms. **Box 7.5**, which looks at weapons proliferation, applies to **banks carrying out trade finance business** and those engaged in other activities, such as **project finance** and **insurance**, for whom the risks are greatest.

Sanctions against Iran[2] will impose requirements on **all firms conducting business linked to that country**.

Content: This chapter contains sections on:

7.1 The UK's financial sanctions regime, which freezes the UK assets of certain individuals and entities, is one aspect of the government's wider approach to economic sanctions. Other elements include export controls (see the Annex 1 list of common terms) and measures to prevent the proliferation of weapons of mass destruction.

7.2 The **UK financial sanctions** regime lists individuals and entities that are subject to financial sanctions. These can be based in the UK, elsewhere in the EU or the rest of the world. In general

2 Current sanctions against Iran stem from concerns over its proliferation activity. As well as imposing asset freezes, they prevent firms we regulate from, among other things, dealing with Iranian banks, establishing subsidiaries in Iran, buying Iranian bonds, making loans to Iranian oil companies, and insuring Iranian organisations (but not individuals). Fund transfers involving Iran over €10,000 in value need to be notified to the Treasury, or, in some cases, submitted to them for approval.

terms, the law requires firms not to provide funds or, in the case of the Terrorism Order[3], financial services, to those on the list, unless a licence is obtained from the Treasury's dedicated Asset Freezing Unit.[4] The Treasury maintains a Consolidated List of financial sanctions targets designated by the United Nations, the European Union and the United Kingdom, which is available from its website. If firms become aware of a breach, they must notify the Asset Freezing Unit in accordance with the relevant provisions.

7.3 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.[5]

Box 7.1: Governance

The guidance in **Box 2.1** on governance in relation to financial crime also applies to sanctions.

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

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.)

Examples of good practice	Examples of poor practice
• An individual of **sufficient authority** is responsible for overseeing the firm's adherence to the sanctions regime. • 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). • There is **appropriate escalation** of actual target matches and breaches of UK sanctions. Notifications are timely.	• The firm believes payments to sanctioned individuals and entities are **permitted** when the sums are small. Without a licence from the Asset Freezing Unit, this could be a **criminal offence**. • No **internal audit** resource is allocated to monitoring sanctions compliance. • Some business units in a *large organisation* think they are **exempt**.

The offence will depend on the sanctions provisions breached.

3 The Terrorism (United Nations Measures) Order 2009 (SI 2009/1747)

4 General licences are in place to allow individuals subject to financial sanctions to access basic financial services, for example to insure themselves, and to allow insurers to provide services for short periods following a claim (e.g. a hire car after a motor accident). The Treasury must be informed promptly.

5 Aiding proliferators 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 Annex 1) to direct financial firms to, say, cease business with certain customers involved in proliferation activity.

Box 7.2: Risk assessment

The guidance in **Box 2.3** on risk assessment in relation to financial crime also applies to sanctions.

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.

Self-assessment questions:

- Does your firm have a **clear view** on where within the firm 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?

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**. • *A small firm* is **aware** of the sanctions regime and where it is most vulnerable, even if risk assessment is only informal.	• There is **no process** for updating the risk assessment. • The firm assumes financial sanctions **only apply to money transfers** and so has not assessed its risks.

Box 7.3: Screening against sanctions lists

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 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 the sanctions regime. (Some firms may knowingly continue to retain customers who are listed under UK sanctions: this is permitted if the Asset Freezing Unit has granted a licence.)

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?)

Examples of good practice

- The firm has considered what **mixture** of manual and automated screening is most appropriate.
- There are quality control checks over **manual screening**.
- 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 screens customers' **directors** and known **beneficial owners** on a risk-sensitive basis.
- Where the firm maintains an account for a listed individual, the status of this account is **clearly flagged** to staff.
- A firm only places faith in **other firms' screening** (such as outsourcers or intermediaries) after taking steps to satisfy themselves this is appropriate.

Examples of poor practice

- The firm assumes that an intermediary has screened a customer, but **does not check** this.
- 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.
- An *insurance company* **only screens when claims are made** on a policy.
- Screening of customer databases is a **one-off** exercise.
- Updating from the Consolidated List is **haphazard**. Some business units use out-of-date lists.
- The firm has **no means** of monitoring payment instructions.

Box 7.4: Matches and escalation

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

- Sufficient resources are available to identify '**false positives**'.
- After a breach, as well as meeting its formal obligation to notify the **Asset Freezing Unit**, the firm considers whether it should report the breach to the **FCA**.[6]

Examples of poor practice

- The firm **does not report a breach** of the financial sanctions regime to the Asset Freezing Unit: **this could be a criminal offence**.
- 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.
- **No audit trail** of decisions where potential target matches are judged to be false positives.

The offence will depend on the sanctions provisions breached.

The offence will depend on the sanctions provisions breached.

6 Chapter 15.3 of the Supervision manual (SUP) of the Handbook 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.

Box 7.5: Weapons proliferation

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 should address the proliferation risks they face.

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

- 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.
- Where **doubt exists**, the *bank* asks the customer to **demonstrate** that appropriate assurances have been gained from relevant government authorities.
- The firm has considered **how to respond** if the government takes action under the Counter-Terrorism Act 2008 against one of its customers.

Examples of poor practice

- 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.
- An insurer has not identified whether **EU Regulation 961/2010** affects its relationship with its customers.
- 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.

Box 7.6: Case study – deficient sanctions systems and controls

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

7.4 Part 2 of the Guide contains the following additional material on sanctions and assets freezes:

- Chapter 8 summarises the findings of the *FSA's* thematic review *Financial services firms' approach to UK financial sanctions* and includes guidance on:
  - Senior management responsibility (Box 8.1)
  - Risk assessment (Box 8.2)
  - Policies and procedures (Box 8.3)
  - Staff training and awareness (Box 8.4)
  - Screening during client take-on (Box 8.5)
  - Ongoing screening (Box 8.6)
  - Treatment of potential target matches (Box 8.7)
- Chapter 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 (Box 15.7)
  - Dual-use goods (Box 15.8)

7.5 To find out more on financial sanctions, see:

- The website of the Treasury's Asset Freezing Unit:
  www.hm-treasury.gov.uk/fin_sanctions_afu.htm
- The Treasury also provides information on general licences:
  www.hm-treasury.gov.uk/fin_sanctions_general_licences.htm

- Part III of the Joint Money Laundering Steering Group's guidance, which is a chief source of guidance for firms on this topic:
  www.jmlsg.org.uk

- Our fact sheet on financial sanctions aimed at small firms:
  http://www.fca.org.uk/static/fca/documents/fas-sanctions2.pdf

7.6 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' (see the Annex 1 list of common terms). For Iran, the website also lists goods that require a licence for that destination, and provides guidance on end users of concern. See:
  www.businesslink.gov.uk/bdotg/action/layer?r.s=tl&r.l1=1079717544&r.lc=en&r.l2=1084228483&topicId=1084302974

- The BIS Iran List, which shows, among other things, entities in Iran who have had export licenses declined:
  www.bis.gov.uk/policies/export-control-organisation/eco-notices-exporters

- The NCA's website, which contains guidelines on how to report suspicions related to weapons proliferation:
  www.nationalcrimeagency.gov.uk/publications/46-guidelines-for-counter-proliferation-financing-reporting/file

- EU Regulation 961/2010, which sets out restrictive measures against Iran:
  http://tinyurl.com/961-2011

- The FATF website. In June 2008, FATF launched a 'Proliferation Financing Report' that includes case studies of past proliferation cases, including some involving UK banks. This was followed up with a report in February 2010:
  www.fatf-gafi.org/dataoecd/14/21/41146580.pdf
  www.fatf-gafi.org/dataoecd/32/40/45049911.pdf.

Annex 1: 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 the Guide. This annex does not provide guidance on rules or amend corresponding references in the Handbook's Glossary of definitions.

Term	Meaning
Action Fraud	The UK's national fraud reporting centre. See: www.actionfraud.police.uk/home
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.
AFU	See 'Asset Freezing Unit'.
AML	Anti-money laundering. See 'money laundering'.
Annex I financial institution	The Money Laundering Regulations 2007 give the *FCA* responsibility for supervising the anti-money laundering controls of 'Annex I financial institutions' (a reference to Annex I to the Banking Consolidation 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 2007. 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: www.fsa.gov.uk/pages/About/What/financial_crime/money_laundering/3mld/regis tered/index.shtml
asset freezing	See 'financial sanctions regime'.

Term	Meaning
Asset Freezing Unit (AFU)	The Asset Freezing Unit of the Treasury is responsible for the implementation and administration of the UK sanctions regime. See: www.hm-treasury.gov.uk/fin_sanctions_afu.htm for more.
Banking Consolidation Directive (BCD)	Directive 2006/48/EC, which first set out the list of 'Annex I Financial Institutions' that was subsequently used to define the scope of the Third Money Laundering Directive.
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 Regulation 6 of the Money Laundering Regulations 2007.
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: www.justice.gov.uk/downloads/guidance/making-reviewing-law/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 complexity 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: www.fsa.gov.uk/consumerinformation/scamsandswindles/investment_scams/carbon_credit
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

Term	Meaning
consent	If a firm is concerned that it may be assisting in the laundering of funds it can file a Suspicious Activity Report and apply to the NCA for consent to continue the transaction. The Proceeds of Crime Act 2002 gives the NCA seven working days to respond. The NCA will either agree that the transaction can go ahead or it will refuse consent. In the latter case the NCA has 31 calendar days in which to take further action: for example, to seek a court order to restrain the assets in question.
Consolidated List	The Treasury 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'
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.

Term	Meaning
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 2007. '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.
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 2007. 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 2007, 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 E-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.

Term	Meaning
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 2007. They must also satisfy us that they have robust governance, effective risk procedures and adequate internal control mechanisms. This incorporates their financial crime systems and controls. For more information, see our e-money approach document: www.fsa.gov.uk/pubs/international/approach_emoney.pdf
enhanced due diligence (EDD)	The Money Laundering Regulations 2007 require firms to apply additional, 'enhanced' customer due diligence measures in higher-risk situations (see Boxes 3.6 to 3.8).
equivalent jurisdiction	A jurisdiction (other than an EEA state) whose law contains equivalent provisions to those contained in the Third Money Laundering Directive. The JMLSG has prepared guidance for firms on how to identify which jurisdictions are equivalent. Equivalent jurisdictions are significant because a firm is able 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.
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: www.fatf-gafi.org/dataoecd/7/40/34849567.PDF
FATF Special Recommendations	Nine Recommendations on the prevention of terrorist financing were introduced by the FATF in October 2001. These were incorporated into the revised 40 Recommendations in February 2012 and are no longer separately listed.
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'.

Term	Meaning
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 2007 for authorised firms and businesses such as leasing companies and providers of safe deposit boxes. We also have 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.
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 by the Asset Freezing Unit of the Treasury. The Asset Freezing Unit 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.*

Term	Meaning
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 2007 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.
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); • 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'.

Term	Meaning
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: www.jmlsg.org/download/7323
high-value dealer	A firm trading in goods (e.g. cars, jewellery and antiques) that accepts cash of €15,000 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 3(12) of the Money Laudering Regulations 2007.
HM Revenue and Customs (HMRC)	HM Revenue and Customs has supervisory responsibilities under the Money Laundering Regulations 2007. It oversees money service businesses, dealers in high-value goods and trust or company service providers, amongst others. See HMRC's website for more information: www.hmrc.gov.uk/index.htm
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.gov.uk
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: www.fsa.gov.uk/pages/doing/regulated/supervise/mortgage_fraud.shtml
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 2007, as do other professional bodies for accountants and book-keepers. See the ICAEW's website for further information: www.icaew.com

Term	Meaning
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: www.fsa.gov.uk/consumerinformation/scamsandswindles/investment_scams
integration	See 'placement, layering, integration'.
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 2007 refer to 'customer due diligence' and not to KYC.
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: www.fsa.gov.uk/consumerinformation/scamsandswindles/investment_scams/land_ banking
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.
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. 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.
LRO	See 'Money Laundering Reporting Officer'.
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.

Term	Meaning
Money Laundering Directive	See 'Third Money Laundering Directive'.
Money Laundering Regulations 2007	The Money Laundering Regulations 2007 (SI 2007/2157) transpose the requirements of 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 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.
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 2(1) of the Money Laundering Regulations 2007.) Firms authorised under FSAMA must inform us if they provide MSB services. For more information about this, see: www.fsa.gov.uk/pages/About/What/financial_crime/money_laundering/3mld/authorised/index.shtml 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: www.hmrc.gov.uk/mlr
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 2007 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'.

Term	Meaning
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/.
National Fraud Authority (NFA)	The National Fraud Authority is responsible for devising and implementing a national fraud strategy. See the NFA's website for more information: www.homeoffice.gov.uk/agencies-public-bodies/nfa
NCA	See 'National Crime Agency'.
NCCT	See 'non-cooperative countries or territories'.
NFA	See 'National Fraud Authority'.
nominated officer	A person in a firm nominated to receive disclosures from others within the firm who know or suspect that a person is engaged in money laundering or terrorist financing. See section 330 of POCA, Part 3 of the Terrorism Act 2000, and Regulation 20(2)(d) of the Money Laundering Regulations 2007.
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 2(1) of the Money Laundering Regulations 2007.)
ongoing monitoring	The Money Laundering Regulations 2007 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 basis. Firms must also update the information they hold on customers for anti-money laundering purposes.

Term	Meaning
payment institutions	A 'payment institution' is a UK firm which is required under the Payment Services Regulations 2009 (SI 2009/209) 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 *The FSA's role under the Payment Services Regulations.*
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 in a foreign state, an EU institution or an international body; their immediate family members; and known close associates. PEPs are associated with an increased money laundering risk as their position makes them vulnerable to corruption. A formal definition is set out in Regulation 14(5) and Schedule 2 of the Money Laundering Regulations 2007. Business relationships with PEPs must be subject to greater scrutiny. (See also Regulation 14(4) of the Money Laundering Regulations 2007.)
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 scheme 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 claimed.
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.

Term	Meaning
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. Measures should include the monitoring of transactions. This is set out in the Recognised Investment Exchanges and Recognised Clearing Houses (REC) module of the Handbook, 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. The guidance in REC 2.10.4G provides that the Money Laundering Regulations 2007, among other laws, apply to recognised bodies.
reliance	The Money Laundering Regulations 2007 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 17 of the Money Laundering Regulations 2007 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: www.fsa.gov.uk/consumerinformation/scamsandswindles/investment_scams/boiler_room

Term	Meaning
simplified due diligence (SDD)	The Money Laundering Regulations 2007 allow firms, in certain specific situations which present a low money-laundering risk, not to apply customer due diligence measures to their customers and, where applicable, their beneficial owners. See Regulation 13 of the Money Laundering Regulations 2007 for more detail. Applying simplified due diligence does not exempt the firm from the need for ongoing monitoring of the customer relationship, and a firm will have to obtain sufficient information to have a meaningful basis for monitoring. Firms also need to report any suspicious transactions. Also, in practice, firms may have other reasons to satisfy themselves that a customer is who they purport to be: for example, in order to control fraud or credit losses.
Solicitors Regulation Authority (SRA)	The Solicitors Regulation Authority has supervisory responsibility for solicitors under the Money Laundering Regulations 2007. 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 sale proceeds, as well as the means through which the customer's or beneficial owner's funds were transferred.
SRA	See 'Solicitors Regulation Authority'.
STR	See 'Suspicious Transaction 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 Report (STR)	When applied to money laundering reporting, the term 'Suspicious Transaction Report' is used commonly outside of the UK in place of 'Suspicious Activity Report'. Both terms have substantially the same meaning. In the UK, the term 'Suspicious Transaction Report' (STR) tends to be used in connection with market abuse reporting.
SWIFT	SWIFT (the Society for Worldwide Interbank Financial Telecommunication) provides the international system used by banks to send the messages that effect interbank payments.

Term	Meaning
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 Money Laundering Directive (3MLD)	The Third Money Laundering Directive (2005/60/EC), adopted in 2005, translated the FATF's Recommendations into EC legislation. The UK has implemented this Directive chiefly through the Money Laundering Regulations 2007.
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
Transfer of Funds (Information on the Payer) Regulation 2007	The Transfer of Funds (Information on the Payer) Regulations 2007 (SI 2007/3298) allow the FSA to place penalties on banks that fail to include data about the payer in payment instructions, as is required by the EU Wire Transfer Regulation. See also 'Wire Transfer Regulation'.
Treasury	The Treasury is the UK government's AML policy lead. It also implements the UK's financial sanctions regime through its Asset Freezing Unit.
trust or company service provision	A formal legal definition of 'trust or company service provider' is given in Regulation 3(10) of the Money Laundering Regulations 2007. 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: www.fsa.gov.uk/pages/About/What/financial_crime/money_laundering/3mlaaauthorised/index.shtml 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: www.hmrc.gov.uk/mlr
verification	Making sure the customer or beneficial owner is who they claim to be. The Money Laundering Regulations 2007 require the customer's identity to be identified on the basis or reliable and independent information, and the beneficial owner's in a way that the firm is satisfied that it knows who the beneficial owner is. See Regulation 5 of the Money Laundering Regulations 2007.
Wire Transfer Regulation	This EU Regulation is formally titled 'Regulation 1781/2006 on information on the payer accompanying transfers of funds'. It implements FATF's 'Special Recommendation VII' in the EU and requires firms to accompany the transfer of funds with specified information identifying the payer. We were given enforcement powers under this regulation by the Transfer of Funds (Information on the Payer) Regulations 2007. The Wire Transfer Regulation is also known as the Payer Information Regulation or the Payment Regulation and should not be confused with the Payment Services Directive.
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

Financial Conduct Authority

25 The North Colonnade Canary Wharf
London E14 5HS
Telephone: +44 (0)20 7066 1000
Fax: +44 (0)20 7066 1099
Website: www.fca.org.uk