FINANCIAL CRIME GUIDE INSTRUMENT 2011

Powers exercised

A. The Financial Services Authority makes this instrument in the exercise of its powers under:

(1) section 157(1) (Guidance) of the Financial Services and Markets Act 2000;
(2) Regulation 93(1) (Guidance) of the Payment Services Regulations 2009; and
(3) Regulation 60(1) (Guidance) of the Electronic Money Regulations 2011.

Commencement

B. This instrument comes into force on 9 December 2011.

New Regulatory Guide

C. The Financial Services Authority makes 'Financial Crime: a guide for firms' to form a Regulatory Guide in accordance with Annex A to this instrument. The Regulatory Guide does not form part of the Handbook.

Amendments to the Handbook

D. The Glossary of definitions is amended in accordance with Annex B to this instrument.

E. The Senior Management Arrangements, Systems and Controls sourcebook (SYSC) is amended in accordance with Annex C to this instrument.

Citation

F. This instrument may be cited as the Financial Crime Guide Instrument 2011.

By order of the Board
8 December 2011

Annex A

Financial crime: a guide for firms

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

Contents

About the Guide:

- **This Guide consolidates FSA 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 FSA 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 FSA supervisors.**

1 Introduction

1.1 This Guide provides practical assistance and information for firms of all sizes and across all FSA-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 FSA 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 FSA 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 FSA 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 FSA 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. We use the word 'must' to indicate a legal obligation under applicable legislation or a regulatory requirement in the FSA's Handbook.

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 FSA 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 we have 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**	• This box provides **illustrative** examples of **poor practices**. • Poor practice examples are also drawn from **conduct we have 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

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

lacking it may not be a problem. The FSA would consider whether a firm has taken other measures to meet its obligations.	**criminal offences.** • These do not identify all cases where conduct may give rise to regulatory breaches or criminal offences.

Box 1.2: Case studies and other information

Most sections contain case studies outlining occasions when a person's conduct fell short of the FSA's 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:

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.

SYSC 6.1.1R
SYSC 3.2.6R

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?
- What **drives** the firm's financial crime efforts? What outcomes does it seek to achieve?

Examples of good practice	Examples of poor 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. • A firm has a **strategy** for self-improvement on financial crime. • There are clear criteria for **escalating** financial crime issues.	• 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 2.2: 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.	• The firm makes no effort to understand or address **gaps** in its financial crime defences. • Financial crime officers are

• 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. • 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.	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 systems and controls.

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.	• 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

• The firm actively considers the **impact of crime** on customers. • The firm considers financial crime risk when **designing new products** and **services**.	suffer (e.g. fraud against customers).

Box 2.4: Policies and procedures

SYSC 3.2.6R
SYSC 6.1.1R

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 (including 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 takes **inadequate steps** to **communicate** policies and procedures to relevant staff. • 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 and awareness

SYSC 3.1.6R
SYSC 5.1.1R

Firms must employ staff with 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.

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

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

- Box 8.2 (Risk assessment) from our thematic review *Financial services firms' approach to UK financial sanctions*
- Box 9.2 (Risk assessment and responses to significant bribery and corruption events) from our thematic review *Anti-bribery and corruption in commercial insurance broking*
- Box 10.7 (Responsibilities and risk assessments) from our 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 our 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 our thematic review *Financial services firms' approach to UK financial sanctions*
- Box 10.1 (Regulatory/Legal obligations) from our thematic review *The Small Firms Financial Crime Review*
- Box 12.1 (High risk customers and PEPs - AML policies and procedures) from our 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 our thematic review *Data security in Financial Services*
- Box 8.4 (Staff training and awareness) from our 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 our thematic review *Anti-bribery and corruption in commercial insurance broking*
- Box 10.6 (Training) from our thematic review *The Small Firms Financial Crime Review*
- Box 11.6 (Staff recruitment and vetting) and Box 11.8 (Staff training and awareness) from our thematic review *Mortgage fraud against lenders*

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

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

2.7 For firms' obligations in relation to whistleblowers see:

- the Public Interest Disclosure Act 1998: http://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 Her Majesty's 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	Examples of poor 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	• 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

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.	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

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.

SYSC 3.2.6IR
SYSC 6.3.9R

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 question:

- 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, and makes appropriate use of, 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	Examples of poor 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, SOCA alerts, press reports, court judgements, reports by non-governmental	• 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

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.
	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	Examples of poor 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.
	• 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**.
		ML Reg 14
		ML Reg 6(1)(a)
		ML Reg 6(1)(b)
		ML Reg 7

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 the 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	• 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

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.	CDD information is **up to date**. **This is a breach of the ML Regulations.** •

ML Reg 8(2)(b)

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:

- **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 14(2)

- **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(3)

- **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 14(4)

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.

ML Reg 7(3)(b)

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.

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	• 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-**

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

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.	**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.

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	Examples of poor practice
• Key AML staff have a **good understanding** of, and **easy access** to, information about a bank's highest risk customers.	• The firm treats annual reviews as a **tick-box exercise** and copies information from previous reviews without thought.

• New higher-risk clients are more closely monitored to confirm or amend **expected account activity**. • **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.	• *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

ML Reg 20(2)(d)
s.331 POCA

Firms must have a **nominated officer**. The nominated officer has a legal obligation to **report any knowledge or suspicions** of money laundering to the Serious Organised Crime Agency (SOCA) 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.)

s.330 POCA
ML Reg 20(2)(d)(iii)

Staff must report their concerns and may do so to the firm's nominated officer, who must then consider whether a report to SOCA 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).

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	Examples of poor 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.	• The nominated officer **passes all internal reports** to SOCA 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.** • A firm provides extraneous and irrelevant detail in response to a **Production Order**.

s.331 POCA

Box 3.10: Record keeping and reliance on others

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.

ML Reg 19

ML Reg 19(4)

ML Reg 7(3)(b)

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	Examples of poor practice
• Records of customer ID and transaction data can be **retrieved quickly and without delay**. • Where the firm routinely relies on	• The firm keeps customer records and related information in a way that **restricts** the **firm's access** to these records

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.	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.** • 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 Reg19(6)

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	Examples of poor 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, SOCA alerts, Financial Action Task Force typologies, court judgements, etc. • This information informs the design of **transaction monitoring systems**. • Suspicions raised within the firm	• 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.

inform its own **typologies**.	

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),** we have seen the following good practices:
  - 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,

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**. — Art.5 EU Reg 1781/2006
- An *intermediary bank* **strips** payer information from payment instructions before passing the payment on. — Art.12 EU Reg 1781/2006
- The *payee bank* does not check any **incoming payments** to see if they include complete and — Art.8 EU Reg 1781/2006

[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 FSA 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.

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.	meaningful data about the ultimate transferor of the funds.

Box 3.13: Case study – poor AML controls

We 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 our 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 FSA 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.

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, our thematic review of *Automated Anti-Money Laundering Transaction Monitoring Systems*
- Chapter 5 summarises the findings of, and consolidates good and poor practice from, our *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 our 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*

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
- SOCA's website, which contains information on how to report suspicions of money laundering: www.soca.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.fsa.gov.uk/smallfirms/resources/factsheets/pdfs/aml_tool.pdf
- Our one-minute guide on AML for smaller firms: www.fsa.gov.uk/smallfirms/resources/one_minute_guides/info_gathering/anti_money.shtml

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/download/6130
- 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 financial institutions are at risk of being defrauded. The main types of fraud are described in our Annex 1 entry for 'fraud'.

4.2 The contents of the Guide's fraud chapter reflect our 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 FSA 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	Examples of poor 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).	• 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 our supervisory scope.

Self-assessment questions:

- Are systems and controls to detect and prevent mortgage fraud **coordinated across the firm**, with resources allocated on the basis of an

assessment of where they can be used to best effect?

- How does your firm contain the fraud risks posed by corrupt **conveyancers, brokers and valuers**?
- How and when does your firm engage with **cross-industry information-sharing** exercises?

Examples of good practice	Examples of poor practice
• A firm's underwriting process can **identify** applications that may present a **higher risk** of mortgage fraud. • 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.	• A *lender* fails to report relevant information to the FSA's **Information from Lenders** (IFL) scheme as per FSA 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 FSA 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	• Failing to undertake due diligence

this is required by lenders. • Using the FSA's **Information from Brokers** scheme to report intermediaries it suspects of involvement in mortgage fraud.	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 we began regulating mortgage brokers in October 2004, we 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.

We have referred numerous cases to law enforcement, a number of which have resulted in criminal convictions.

Box 4.5: Investment fraud

This section applies to *retail deposit takers*.

UK consumers lose over £500m a year to share sale fraud (sometimes referred to as 'boiler room fraud') and other investment scams, e.g. involving land banking and unauthorised deposit taking. Fraudsters are increasingly receiving the proceeds of these crimes in 'collection accounts' held with UK high-street banks. There is a common pattern of activity for such accounts. They typically receive large numbers of relatively small incoming payments from individuals before substantial, regular outgoing payments are then made to other accounts, usually based overseas, as the criminals disperse their proceeds.

Firms have obligations under the Proceeds of Crime Act 2002, the Money Laundering Regulations 2007 and our rules to:

- identify customers (including understanding the nature of the business relationship);
- monitor account activity;
- report suspicious activity to the Serious Organised Crime Agency; and
- have policies and procedures in place to prevent activities related to money laundering and to counter the risk of being used to further financial crime.

Chapter 3 on anti-money laundering provides guidance to help firms fulfil these obligations.

Firms should be vigilant in identifying and reporting transactions where there are suspicions of financial crime. By doing so, they can prevent consumer loss by enabling the relevant authorities to identify quickly the proceeds of unauthorised business and, where appropriate, freeze funds.

What procedures does your firm have in place to avoid facilitating payments to investment fraudsters such as boiler rooms or unauthorised deposit takers?

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 our 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)
  - 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 our thematic review *Firms' high-level management of fraud risk.*

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

- Details of the FSA's Information from Lenders scheme:

  www.fsa.gov.uk/pages/doing/regulated/supervise/mortgage_fraud.shtml
- Details of the FSA's Information from Brokers scheme:

  www.fsa.gov.uk/smallfirms/your_firm_type/mortgage/fraud/report.shtml
- 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 FSA 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: http://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	Examples of poor practice
• There is a clear **figurehead** championing the issue of data security.	• The firm does not **contact customers** after their data is lost or compromised.
• Work, including by internal audit and compliance, is **coordinated** across the firm, with compliance,	• Data security is treated as an **IT** or **privacy issue**, without also recognising the financial crime

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.	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 that 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 is **access** to the premises and sensitive areas of the business **controlled**?
- When are **staff access rights** reviewed? (It is good practice to review them at least on recruitment, when staff change roles, and when they leave the firm.)
- Is there enhanced **vetting** of staff with access to lots of data?
- How are staff made aware of **data security risks**?

Examples of good practice	Examples of poor practice
• **Access** to sensitive areas (call centres, server rooms, filing rooms) is restricted. • 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	• 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

(e.g. on USB sticks, CDs, hard disks etc) is always **encrypted** when taken offsite. • The firm understands what checks are done by **employment agencies** it uses.	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, we fined Norwich Union Life £1.26m for failings in its anti-fraud systems and controls.

- 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 our press release:
www.fsa.gov.uk/pages/Library/Communication/PR/2007/130.shtml

Box 5.5: Case study - data security failings

In August 2010, we 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.

Our 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 our 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)
  - Physical security (Box 6.12)
  - 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.fsa.gov.uk/smallfirms/resources/one_minute_guides/info_gathering/data_security.shtml

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 FSA does not enforce or give guidance on the Bribery Act. But:

- firms which are subject to our rules SYSC 3.2.6R and SYSC 6.1.1R are under a separate, regulatory obligation to establish and maintain effective systems and controls to mitigate financial crime risk; and

SYSC 3.2.6R; SYSC 6.1.1R

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

E-Money Reg 6; Payment Service Reg 6

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

The guidance in Box 2.1 on governance in relation to financial crime also applies to bribery and corruption.

A firm's senior management should take steps to ensure 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.

Self-assessment questions:

- What **role** do senior management play in the firm's anti-bribery and corruption effort? Do they approve and periodically review the strategies and policies for managing, monitoring and mitigating this risk? What steps do they take to ensure staff are aware of their interest in this area?
- Can your firm's board and senior management **demonstrate** a good understanding of the bribery and corruption risks faced by the firm, the materiality to its business and how to apply a risk-based approach to anti-bribery and corruption?
- How are **integrity** and **compliance** with relevant anti-corruption legislation considered when discussing **business opportunities**?
- What **information** do senior management receive in relation to bribery and corruption, and how frequently? Is it sufficient for senior management effectively to fulfil their functions in relation to anti-bribery and corruption?

Examples of good practice	Examples of poor practice
• The firm is **committed** to carrying out business fairly, honestly and openly. • Responsibility for anti-bribery and corruption systems and controls is **clearly documented** and apportioned to a single senior manager with appropriate terms of reference 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.	• 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 higher-risk third-party relationships or payments.

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 it cover corrupt behaviour not captured by the Bribery Act definition?
- 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?
- Could **remuneration structures** increase the risk of bribery and corruption?

Examples of good practice	Examples of poor practice
• Corruption risks are assessed in **all jurisdictions** where the firm operates and across all business channels. • The firm assesses and manages the risk of **remuneration structures** rewarding staff for taking unacceptable corruption and bribery risks to generate business.	• Compliance departments are **ill equipped** to identify and assess corruption risk. • For fear of harming the business, the firm classifies as **low risk** a jurisdiction generally associated with **high risk**.

Box 6.3: Policies and procedures

The guidance in Box 2.4 on policies and procedures in relation to financial crime 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:

- How do you satisfy yourself that your anti-bribery and 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.	• The firm **does not assess** the extent to which staff comply with its anti-corruption policies and

• 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**.	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 respond** to internal or external events that may highlight weaknesses in its anti-corruption systems and controls.

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 **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 due diligence information kept **up to date**? How?

Examples of good practice	Examples of poor practice
• Where a firm uses third parties to generate business, these relationships are subject to **thorough due diligence** and management oversight. • 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.	• *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

• 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.	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 our 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, we 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 review 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.

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

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.fsa.gov.uk/smallfirms/resources/one_minute_guides/insurance_intermed/anti_bribery.shtml

7 Sanctions and asset freezes

Who should read this chapter? All firms are required to comply with the UK's financial sanctions regime. The FSA'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 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

[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.

[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.

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.

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.

[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.

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 customers 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, for a variety of reasons, 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	Examples of poor practice
• The firm has considered what **mixture** of manual and automated screening is most	• The firm assumes that an intermediary has screened a customer, but **does not check**

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.	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 FSA, and giving consideration to a Suspicious Activity Report.)

Examples of good practice	Examples of poor 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 **FSA.** [6]	• 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.

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

[6] Chapter 15.3 of the Supervision manual (SUP) of the FSA 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.

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, we 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 our 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 our 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)

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/download/6130
- Our fact sheet on financial sanctions aimed at small firms:
  www.fsa.gov.uk/smallfirms/resources/pdfs/Sanctions.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/download/6130
- 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
- SOCA's website, which contains guidelines on how to report suspicions related to weapons proliferation:
  www.soca.gov.uk/about-soca/library/doc_download/297-guidelines-for-counter-proliferation-financing-reporting.doc

- 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 FSA Handbook's Glossary of definitions.

Term	Meaning
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 FSA responsibility for supervising the anti-money laundering controls of 'Annex I financial institutions' (a reference to Annex I to the Banking Consolidation Directive). In practice, this includes businesses that offer finance leases, commercial lenders and providers of safe deposit boxes. Where a firm we authorise 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 by us, we are responsible for supervising their AML activities. For more information on this, see our website: www.fsa.gov.uk/pages/About/What/financial_crime/money_laundering/3mld/registered/index.shtml
asset freezing	See 'financial sanctions regime'.
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 sets out (in its Annex I) the list of activities subject to mutual recognition which, in turn, help define the scope of the Third Money Laundering Directive.
beneficial owner	The natural person who ultimately owns the customer or exercises management control over it. An entity may have more than one beneficial owner. 'Beneficial owner' is defined in Regulation 6 of the Money Laundering Regulations 2007.
boiler room	An unauthorised firm that defrauds the public by using hard-sell tactics, usually over the telephone, to sell shares as an investment opportunity while knowing that the shares are worthless or fictional.

	www.fsa.gov.uk/Pages/consumerinformation/scamsandswindles/index.shtml
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, and creates a corporate offence of failing to prevent bribery. The Ministry of Justice has issued guidance about procedures that firms can put in place to prevent bribery: www.justice.gov.uk/downloads/guidance/making-reviewing-law/bribery-act-2010-guidance.pdf.
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.
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 SOCA for consent to continue the transaction. The Proceeds of Crime Act 2002 gives SOCA seven working days to respond. SOCA will either agree that the transaction can go ahead or it will refuse consent. In the latter case SOCA 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
corruption	Corruption is the abuse of public or private office to obtain an undue advantage. Corruption includes bribery.
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.
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 include alloys that are 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) that passport into the UK are generally authorised persons. Generally speaking, EEA firms who carry on relevant business from a UK branch will be subject to the Money Laundering Regulations 2007 and the financial crime-related requirements in the FSA Handbook. 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.
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 FSA's financial crime Handbook provisions do not apply to e-money institutions, but the FSA 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: http://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 a financial firm authorised by us 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. 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. The Nine Special Recommendations can be downloaded from FATF's website: www.fatf-gafi.org/dataoecd/8/17/34849466.pdf
FATF-style	Regional international bodies such as Moneyval and the Asia-Pacific

regional bodies	Group which have a similar form and functions to those of the FATF. The FATF seeks to work closely with such bodies.
FI	See 'Financial Investigator'.
Financial Action Task Force (FATF)	An intergovernmental body that develops and promotes anti-money laundering and counter terrorist financing standards worldwide. Further information is available on its website: www.fatf-gafi.org
financial 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.' SOCA 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 Services Authority.
Financial Services Authority (FSA)	The Financial Services Authority has statutory objectives under FSMA that include the reduction of 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.
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', 'long firm fraud', and 'Missing Trader Inter-Community fraud'.
Fraud Act 2006	The Fraud Act 2006 sets out a series of fraud offences such as fraud by false representation, fraud by failing to disclose information and fraud by abuse of position.
FSA	See 'Financial Services Authority'.
FSMA	See 'Financial Services and Markets Act 2000'.
FSRB	See 'FATF-style regional bodies'.
fuzzy matching	The JMLSG suggests the term 'fuzzy matching' 'describes any process that identifies non-exact matches. Fuzzy matching software solutions identify possible matches where data - whether in official lists or in firms' internal records - is misspelled, incomplete, or missing. They are often tolerant of multinational and linguistic differences in spelling, formats for dates of birth, and similar data. A sophisticated system will have a variety of settings, enabling greater or less fuzziness in the matching process'. See Part III of the JMLSG's guidance: www.jmlsg.org/download/6130.
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 Laundering Regulations 2007.
HM Revenue and Customs (HMRC)	HM Revenue and Customs (HMRC) 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 FSA 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.
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’.
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.
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.
MLRO	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.
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 FSA's 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 that are authorised by the FSA 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 FSA Handbook that specifically relate to money laundering (SYSC 3.2.6AR – SYSC 3.2.6JG). Firms offering these services alongside other products that are subject to the Money Laundering Regulations (such as banking and stock broking services) can therefore apply different customer due diligence checks in both situations. But in practice, many will choose to apply a consistent approach for the sake of operational convenience.
MSB	See 'money service business'.
MTIC	See 'Missing Trader Inter-Community Fraud'.
National 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.
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.)
Office of Fair Trading (OFT)	The Office of Fair Trading has responsibilities under the Money Laundering Regulations 2007 to supervise many lenders and estate agents.
OFT	See 'Office of Fair Trading'.
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.
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 to 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.)
Proceeds of Crime Act 2002 (POCA)	POCA criminalises all forms of money laundering and creates other offences such as failing to report a suspicion of money laundering and 'tipping off'.
Production Order	The Proceeds of Crime Act 2002 allows Financial Investigators to use production orders to obtain information from financial firms about an individual's financial affairs.
proliferation finance	Funding the proliferation of weapons of mass destruction in contravention of international law.

recognised investment exchanges, and recognised clearing houses	To be recognised by the FSA, 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, • 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 FSA 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 FSA 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'.
Serious Organised Crime Agency (SOCA):	Created in 2006, SOCA brought together various agencies including the National Crime Squad, National Criminal Intelligence Service and HMRC's investigative branches. As the UK's financial intelligence unit it receives suspicious activity reports about money laundering and terrorist financing. See SOCA's website for more information: www.soca.gov.uk.
simplified due diligence (SDD)	The Money Laundering Regulations 2007 allow firms, in certain specific situations that 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.
SOCA	See 'Serious Organised Crime Agency'.
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	As part of their customer due diligence and monitoring obligations, firms should establish that the source of wealth and source of funds involved in a business relationship or occasional transaction is legitimate. They are required to do so when the customer is a PEP. 'Source of wealth' describes how a customer acquired their total wealth, while 'source of funds' refers to the origin of the funds involved in the business relationship or occasional transaction.
SRA	See 'Solicitors Regulation Authority'.
STR	See 'Suspicious Transaction Report'.
Suspicious Activity Report (SAR)	A report made to SOCA 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 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.
SYSC	SYSC is the Senior Management Arrangements, Systems and Controls sourcebook of the FSA's 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.
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 SOCA 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'.
Transfer of Funds (Information on the Payer) Regulations 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'.
The 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_launderi

	ng/3mld/authorised/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 of 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 crime:
a guide for firms

Part 2: Financial crime thematic reviews

Contents

1 Introduction

1.1 Part 2 of *Financial crime: a guide for firms* contains summaries of, and links to, FSA thematic reviews of various financial crime risks. It includes the consolidated examples of good and poor practice that were included with the reviews' findings. Each chapter includes a statement about those to whom it is most relevant and, where good and poor practice is included, to whom that guidance applies. We have suggested where material may be of interest and use to a broader range of firms, but we will only take guidance as applying to those types of firms to whom we have directly applied it. Each chapter also includes cross references to relevant chapters in Part 1.

1.2 The statements of our expectations and the examples of good and poor practice in the body of Part 2 have the same status as in Part 1: they are "general guidance" as defined by section 158 of the Financial Services and Markets Act 2000. The guidance in Part 2 is not binding and imposes no requirements on firms. Please refer to Chapter 1 of Part 1 for more information about guidance in the Guide.

1.3 As with Part 1, Part 2 contains 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).

Chapters 4, 5, and 12 also contain guidance on how firms can meet the requirements of the Money Laundering Regulations 2007; Chapter 12 also contains guidance on the EU Wire Transfer Regulation[7].

1.4 Not all thematic reviews contain consolidated examples of good and poor practice. All reports do, however, discuss what we found about the practices in place at the firms we visited. This information is not guidance, but firms interested in comparing themselves against their peers' systems and controls and policies and procedures in the areas covered by the reviews can find more information on this in the original reports.

[Editor's note: changes from the original published thematic reports are indicated by underlining (for additions) and striking through (for deletions).]

[7] EU Regulation 1781/2006 on information on the payer. See Part 1 Annex 1 of common terms for more information.

2 Firms' high-level management of fraud risk (2006)

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

2.1 In February 2006 we reviewed a sample of 16 firms (predominantly larger financial services groups) to assess how firms' senior management were managing fraud risk.

2.2 The findings of the review reflected our overall expectation that firms' senior management should be proactive in taking responsibility for identifying and assessing fraud risk and the adequacy of existing controls, and ensure that, if necessary, appropriate additional controls are put in place. We expect a firm to consider the full implications of the fraud risks it faces, which may have wider effects on its reputation, its customers and the markets in which it operates.

2.3 The report emphasised that fraud is more than just a financial crime issue for firms; it is also a reputational one for the industry as a whole. The report concluded that while there had been some improvement in the management of fraud there was still more that firms could be doing to ensure fraud risk was managed effectively.

2.4 The contents of this report are reflected in Chapter 2 (Financial crime systems and controls) and Chapter 4 (Fraud) of Part 1 of this Guide.

Our findings

2.5 You can read the findings of the FSA's thematic review here:

http://www.fsa.gov.uk/pubs/other/fraud_risk.pdf

Consolidated examples of good and poor practice

2.6 This report did not contain consolidated examples of good and poor practice.

3 Review of private banks' anti-money laundering systems and controls (2007)

Who should read this chapter? This chapter is relevant to **private banks** (firms which provide banking and investment services in a closely managed relationship to high net-worth clients) and **other firms conducting business with customers, such as PEPs, who might pose a higher risk of money laundering**. It may also be of interest to other firms we supervise under the Money Laundering Regulations 2007.

3.1 In July 2007 we undertook a review of the anti-money laundering (AML) systems and controls at several FSA-regulated private banks. The review was conducted in response to a report by our Intelligence team, which had highlighted the high risk of money laundering within private banking.

3.2 This sector is particularly susceptible to money laundering and firms are expected to have high-standard AML systems and controls in place in order to mitigate these risks. The review focused on firms' policies and procedures for identifying, assessing, monitoring and managing the risks with a strong focus on high-risk clients and Politically Exposed Persons (PEPs).

3.3 The key areas examined in depth were a consideration of senior managements' risk appetite and the level of customer due diligence that took place.

3.4 Overall we found that the private banks covered by our review acknowledged the relatively high risk of money laundering within their business activities and recognised the need to develop and implement strong AML systems and controls. The report also emphasised that private banks should obtain and keep up-to-date information on clients.

3.5 The contents of this report are reflected in Chapter 2 (Financial crime systems and controls) and Chapter 3 (Money laundering and terrorist financing) of Part 1 of this Guide.

Our findings

3.6 You can read the findings of the FSA's thematic review here:

http://www.fsa.gov.uk/pubs/other/money_laundering/systems.pdf

Consolidated examples of good and poor practice

3.7 This report did not contain consolidated examples of good and poor practice.

4 Automated Anti-Money Laundering Transaction Monitoring Systems (2007)

Who should read this chapter? This chapter is relevant, and its statements of good and poor practice apply, to **all firms** for whom we are the supervisory authority under the Money Laundering Regulations 2007.

The extent to which we expect a firm to use automated anti-money laundering transaction monitoring (AML TM) systems depends on considerations such as the nature and scale of its business activities. There may be firms, particularly, **smaller firms**, that monitor credibly and effectively using manual procedures. This chapter will not apply to such firms where they do not, and are not intending to, use AML TM systems, although it may still be of interest to them.

4.1 We wrote a short report on automated Anti-Money Laundering Transaction Monitoring Systems in July 2007. This was in anticipation of the fact that transaction monitoring would become compulsory following the implementation of the Money Laundering Regulations 2007.

4.2 The report explains that we did not anticipate that there would be major changes in firms' practice, as the new framework expressed in law what firms were already doing. Instead, it is to be read as feedback on good practice to assist firms in complying with the Money Laundering Regulations 2007.

4.3 The report confirms our expectation that senior management should be in a position to monitor the performance of transaction monitoring (TM) systems, particularly at firms that experience operational or performance issues with their systems, to ensure issues are resolved in a timely fashion. Particular examples of good practice include transaction monitoring and profiling; especially ensuring unusual patterns of customer activity are identified.

4.4 The contents of this report are reflected in Chapter 2 (Financial crime systems and controls) and Chapter 3 (Money laundering and terrorist financing) of Part 1 of this Guide.

Our findings

4.5 You can read the findings of the FSA's thematic review here:

http://www.fsa.gov.uk/pubs/other/money_laundering/aml_system.pdf

Consolidated examples of good and poor practice

4.6 This report contained the following examples of good practice:

Box 4.1: Statement of good practice
• Depending on the nature and scale of a firm's business activities, automated AML TM

Box 4.1: Statement of good practice
systems may be an important component of an effective overall AML control environment.
Methodologies
• TM systems use profiling and/or rules-based monitoring methods.
• Profiling identifies unusual patterns of customer activity by applying statistical modelling techniques. These compare current patterns of activity to historical activity for that customer or peer group.
• Rules-based monitoring compares customer activity to fixed pre-set thresholds or patterns to determine if it is unusual.
Development and implementation
• A clear understanding of what the system will deliver and what constraints will be imposed by the limitations of the available data (including any issues arising from data cleanliness or legacy systems).
• Consideration of whether the vendor has the skills, resources and ability to deliver the promised service and provide adequate ongoing support.
• Maintenance of good working relations with the vendor, e.g. when collaborating to agree detailed system configuration.
• Use of recommended hardware, not necessarily a firm's own standard, to reduce processing problems, or otherwise finding a solution that is a good fit with a firm's existing infrastructure.
• A full understanding of the data being entered into the system and of the business's requirements.
• Regular housekeeping and database maintenance (operational resilience is vital to ensure that queries do not back up).
• Careful consideration of the risks of commissioning a bespoke vendor system, which may be incompatible with future standard product upgrades.
• Continued allocation of sufficient resources to ensure~~ing~~ manual internal suspicion reporting is effective, as TM can supplement, but not replace, human awareness in day-to-day business.
Effectiveness
• Analyse system performance at a sufficiently detailed level, for example on a rule-by-rule basis, to understand the real underlying drivers of the performance results.
• Set systems so they do not generate fewer alerts simply to improve performance statistics. There is a risk of 'artificially' increasing the proportion of alerts that are ultimately reported as suspicious activity reports without generating an improvement in the quality and quantity

Box 4.1: Statement of good practice
of the alerts being generated.
• Deploy analytical tools to identify suspicious activity that is currently not being flagged by existing rules or profile-based monitoring.
• Allocate adequate resources to analysing and assessing system performance, in particular to define how success is measured and produce robust objective data to analyse performance against these measures.
• Consistently monitor from one period to another, rather than on an intermittent basis, to ensure that performance data is not distorted by, for example, ad hoc decisions to run particular rules at different times.
• Measure performance as far as possible against like-for-like comparators, e.g. peers operating in similar markets and using similar profiling and rules.
Oversight
• Senior management should be in a position to monitor the performance of TM systems, particularly at firms that are experiencing operational or performance issues with their systems, so that issues are resolved in a timely fashion.
• Close involvement of the project management process by major business unit stakeholders and IT departments is an important component of successful system implementation.
Reporting & review
• There should be a clear allocation of responsibilities for reviewing, investigating and reporting details of alerts generated by TM systems. Those responsible for this work should have appropriate levels of skill and be subject to effective operational control and quality assurance processes.

5 Review of firms' implementation of a risk-based approach to anti-money laundering (AML) (2008)

Who should read this chapter? This chapter is relevant, and its statements of good and poor practice apply, to **all firms** for whom we are the supervisory authority under the **Money Laundering Regulations 2007**.

5.1 In March 2008 we conducted a review of firms' implementation of a risk-based approach to anti-money laundering. This followed the move to a more principles-based regulatory strategy from August 2006, when we replaced the detailed rules contained in the Money Laundering sourcebook with high-level rules in the Senior Management Arrangements, Systems and Controls sourcebook (SYSC) of our Handbook.

5.2 We visited 43 firms in total and gathered additional information from approximately 90 small firms with a survey. The report explored in depth a number of key areas that required improvement, including a review of staff training and the need to ensure staff are aware that it is a constant requirement to ensure AML policies and procedures are up to date and effective.

5.3 Due to the wide range of firms we visited, there were a number of different findings. There were many examples of good practice, particularly in the way the larger firms had fully embraced the risk-based approach to AML and senior management's accountability for effective AML. We also recognised that smaller firms, which generally represent lower risk, had fewer resources to devote to money laundering risk assessment and mitigation.

5.4 The contents of this report are reflected in Chapter 2 (Financial crime systems and controls) and Chapter 3 (Money laundering and terrorist financing) of Part 1 of this Guide.

Our findings

5.5 You can read the findings of the FSA's thematic review here:

http://www.fsa.gov.uk/pubs/other/jmlsg_guidance.pdf

Consolidated examples of good and poor practice

Box 5.1: Firms' implementation of a risk-based approach to AML	
Examples of good practice:	**Examples of poor practice:**
• One large firm's procedures required it to undertake periodic Know your Customer (KYC)/Customer Due Diligence (CDD) reviews of existing clients. The depth of the review is determined by the risk ranking assigned to the client. Clients rated A and B are reviewed every three years; Cs every two years; and Ds and Es are reviewed annually. For lower risk (A-	• Some firms did not have a robust approach to classifying the money laundering risk associated with their clients. For example, one wholesale small firm classified all its clients as low or medium risk, despite the fact that most of them were based in Eastern Europe, North Africa and the Middle East. Another firm's risk-assessment

Box 5.1: Firms' implementation of a risk-based approach to AML

Examples of good practice:	Examples of poor practice:
C) clients, the review may amount to no more than refreshing the client's file to take account of: significant changes in ownership or capitalisation; changes in the client's line of business; addition of a Politically Exposed Person (PEP) to shareholders or senior management; or any negative news on the client's owners or senior managers. For high risk (D or E) clients, visits to the client are necessary to provide an extra layer of comfort. Such visits would typically cover: review of client's client take-on procedures; sample testing of KYC documentation on underlying clients; and, obtaining answers to outstanding queries on, e.g., annual AML certification, transaction queries, and potential PEP or sanctions hits. • One building society undertook a comprehensive policy review following the publication of the 2006 JMLSG guidance, in order to identify which parts of the business were affected and what action was needed. It identified eight core business areas, which represented the key operational areas exposed to risk from money laundering. These business areas were ranked in order of risk and formed into workstreams. The local managers from each workstream business area were then trained by the Compliance Policy Team, using a series of presentations and individual workshops, to understand the impact of the risk-based approach, their individual responsibilities and the appropriate customer due diligence policies. These managers were then required to apply this awareness and their existing knowledge of their workstreams' business activities to create documented risk profiles covering customers, products, delivery channels and	procedures provided that the Compliance Officer or MLRO[9] would determine the risk category for each client and would record the basis of the assessment for each client. However, a file review showed no evidence that risk assessments had actually been carried out. • Some small firms had produced inadequate annual MLRO reports, which failed to demonstrate to their governing body and senior management that the firms' AML systems and controls were operating effectively. In one case, the MLRO stated categorically that there had been no perceived deficiencies in the suspicious activity reporting process. However, he was unable even to describe that process to us, so it was highly unlikely that he had ever reviewed the SAR[10] process for possible deficiencies. • In one small firm, the MLRO was clearly not fully engaged in his role. For example, he was unaware that we had removed the Money Laundering sourcebook and he was still using an outdated (2003) edition of the JMLSG Guidance. It was not entirely clear whether this arose from a lack of interest in his MLRO function or from inadequate compliance resources at the firm, which left him with insufficient time to keep up to date with AML matters, or a combination of both. • We found some cases of medium-sized and smaller firms documenting their client take-on procedures but not regularly updating those procedures and not always following them. For example, one firm told us that CDD information on clients was refreshed every time clients

[9] Money Laundering Reporting Officer. See Part 1 Annex 1 for common terms.

[10] Suspicious Activity Report. See Part 1 Annex 1 for common terms.

Box 5.1: Firms' implementation of a risk-based approach to AML

Examples of good practice:	Examples of poor practice:
geography. The risk profiles were graded as Red, Amber and Green and customer due diligence and monitoring requirements set at appropriate levels. • In response to the SYSC changes, one major bank decided to appoint the MLRO's line manager as the designated director with overarching responsibility for AML controls. This director was seen as the obvious choice for the role, given that his portfolio of responsibilities included fraud, risk and money laundering. The bank's decision formally to appoint a Board-level senior manager to this position was viewed as reinforcing the importance of having in place a robust AML control framework. Following his appointment, the director decided that the management information (MI) on AML issues he had hitherto received was too ad hoc and fragmented. So the SYSC/ JMLSG[8] changes proved to be a catalyst for the bank establishing more organised MI and a Group-level Financial Risk Committee to consider relevant issues. (In the past, various Risk Committees had considered such issues.) The new Committee's remit covered fraud, money laundering and sanctions issues; however, its primary focus was AML. • One large bank judged that staff AML training and awareness were suitable for the development of a risk-based approach. It saw a need to differentiate between AML requirements in various business units, so that training could be adapted to the needs of the job. So in Retail, training had been re-designed to produce a more balanced package. Accordingly, staff were required to undertake one training module per quarter, with the emphasis on a different area in each module and a test taken every quarter. The aim was to see	applied for a new product or service. However, a file review showed no evidence that this had been done. • A number of medium-sized and small firms were unaware that it was illegal for them to deal with individuals or entities named on the Treasury's Financial Sanctions list. As a result, no screening of clients or transactions was being undertaken against that list. • One firm said that it did not routinely check the Financial Sanctions list, because it did not deal with the type of client who might appear on the list. • Some medium-sized and small firms admitted that staff AML training was an area where improvement was needed. One firm told us that training was delivered as part of an induction programme but not refreshed at regular intervals throughout the employee's career. Another firm said that it provided AML induction training only if a new joiner specifically requested it and no new employee had actually made such a request. The firm's MLRO took the view that most new employees came from the regulated sector, so should already be aware of their AML obligations. Such employees were merely required to sign a form to confirm that they were aware of the firm's AML procedures, but their understanding was never tested.

[8] Joint Money Laundering Steering Group. See Part 1 Annex 1 for common terms

Box 5.1: Firms' implementation of a risk-based approach to AML	
Examples of good practice:	**Examples of poor practice:**
what impact this constant 'drip feed' of training had on suspicious activity reporting. At the time of our visit, this bank was also in the throes of merging its anti-fraud and AML training. The overall objective was to make it more difficult for criminals to do business with the bank undetected.	

6 Data security in Financial Services (2008)

Who should read this chapter? This chapter is relevant, and its statements of good and poor practice apply, 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 In April 2008 we published the findings of our thematic review on how financial services firms in the UK were addressing the risk that customer data may be lost or stolen and used to commit fraud or other financial crime. We visited 39 firms, including retail and wholesale banks, investment firms, insurance companies, financial advisers and credit unions. We also took into account our experience of data loss incidents dealt with by our Financial Crime Operations Team: during 2007, the team dealt with 56 cases of lost or stolen data from financial services firms.

6.2 We found a wide variation between good practices demonstrated by firms that were committed to ensuring data security and weakness in firms that were not taking adequate steps. Overall, we found that data security in financial services firms needed to be improved significantly.

6.3 The report concluded that poor data security was a serious, widespread and high-impact risk, and that firms were often failing to consider the wider risks of identity fraud which could occur from cases of significant data loss and the impact of this on consumers. We

found that firms lacked a clear understanding of these risks and were therefore failing properly to inform customers, resulting in a lack of transparency.

6.4 The contents of this report are reflected in Chapter 2 (Financial crime systems and controls) and Chapter 5 (Data security) of Part 1 of this Guide.

Our findings

6.5 You can read the findings of the FSA's thematic review here:

http://www.fsa.gov.uk/pubs/other/data_security.pdf

Consolidated examples of good and poor practice

Box 6.1: Governance

Examples of good practice:	**Examples of poor practice:**
• Identification of data security as a key specific risk, subject to its own governance, policies and procedures and risk assessment. • A senior manager with overall responsibility for data security, specifically mandated to manage data security risk assessment and communication between the key stakeholders within the firm such as: senior management, information security, Human Resources, financial crime, security, IT, compliance and internal audit. • A specific committee with representation from relevant business areas to assess, monitor and control data security risk, which reports to the firm's Board. As well as ensuring coordinated risk management, this structure sends a clear message to all staff about the importance of data security. • Written data security policies and procedures that are proportionate, accurate and relevant to staff's day-to-day work. • An open and honest culture of communication with pre-determined reporting mechanisms that make it easy for all staff and third parties to report data	• Treating data security as an IT issue and failing to involve other key staff from across the business in the risk assessment process. • No written policies and procedures on data security. • Firms do not understand the need for knowledge-sharing on data security. • Failing to take opportunities to share information with, and learn from, peers and others about data security risk and not recognising the need to do so. • A 'blame culture' that discourages staff from reporting data security concerns and data losses. • Failure to notify customers affected by data loss in case the details are picked up by the media.

Box 6.1: Governance	
Examples of good practice: security concerns and data loss without fear of blame or recrimination. • Firms seeking external assistance if they feel they do not have the necessary expertise to complete a data security risk assessment themselves. • Firms liaising with peers and others to increase their awareness of data security risk and the implementation of good systems and controls. • Detailed plans for reacting to a data loss including when and how to communicate with affected customers. • Firms writing to affected customers promptly after a data loss, telling them what has been lost and how it was lost. • Firms offering advice on protective measures against identity fraud to consumers affected by data loss and, where appropriate, paying for such services to be put in place.	**Examples of poor practice:**

Box 6.2: Training and awareness	
Examples of good practice: • Innovative training and awareness campaigns that focus on the financial crime risks arising from poor data security, as well as the legal and regulatory requirements to protect customer data. • Clear understanding among staff about why data security is relevant to their work and what they must do to comply with relevant policies and procedures. • Simple, memorable and easily digestible guidance for staff on good data security practice. • Testing of staff understanding of data security policies on induction and once a year after that. • Competitions, posters, screensavers and group discussion to raise interest in the subject.	**Examples of poor practice:** • No training to communicate policies and procedures. • Managers assuming that employees understand data security risk without any training. • Data security policies which are very lengthy, complicated and difficult to read. • Reliance on staff signing an annual declaration stating that they have read policy documents without any further testing. • Staff being given no incentive to learn about data security.

Box 6.3: Staff recruitment and vetting	
Examples of good practice: • Vetting staff on a risk-based approach, taking into account data security and other fraud risk. • Enhanced vetting – including checks of credit records, criminal records, financial sanctions lists and the CIFAS Staff Fraud Database – for staff in roles with access to large amounts of customer data. • Liaison between HR and Financial Crime to ensure that financial crime risk indicators are considered during the vetting process. • A good understanding of vetting conducted by employment agencies for	**Examples of poor practice:** • Allowing new recruits to access customer data before vetting has been completed. • Temporary staff receiving less rigorous vetting than permanently employed colleagues carrying out similar roles. • Failing to consider continually whether staff in higher-risk positions are becoming vulnerable to committing fraud or being coerced by criminals.

Box 6.3: Staff recruitment and vetting	
Examples of good practice: temporary and contract staff. • Formalised procedures to assess regularly whether staff in higher-risk positions are becoming vulnerable to committing fraud or being coerced by criminals.	**Examples of poor practice:**

Box 6.4: Controls - Access rights	
Examples of good practice: • Specific IT access profiles for each role in the firm, which set out exactly what level of IT access is required for an individual to do their job. • If a staff member changes roles or responsibilities, all IT access rights are deleted from the system and the user is set up using the same process as if they were a new joiner at the firm. The complexity of this process is significantly reduced if role-based IT access profiles are in place – the old one can simply be replaced with the new. • A clearly-defined process to notify IT of forthcoming staff departures in order that IT accesses can be permanently disabled or deleted on a timely and accurate basis. • A regular reconciliation of HR and IT user records to act as a failsafe in the event of a failure in the firm's leavers process. • Regular reviews of staff IT access rights to ensure that there are no anomalies. • 'Least privilege' access to call recordings and copies of scanned documents obtained for 'know your customer' purposes. • Authentication of customers' identities using, for example, touch-tone telephone before a conversation with a call centre adviser takes place. This limits the amount	**Examples of poor practice:** • Staff having access to customer data that they do not require to do their job. • User access rights set up on a case-by-case basis with no independent check that they are appropriate. • Redundant access rights being allowed to remain in force when a member of staff changes roles. • User accounts being left 'live' or only suspended (i.e. not permanently disabled) when a staff member leaves. • A lack of independent check of changes effected at any stage in the joiners, movers and leavers process.

Box 6.4: Controls - Access rights	
Examples of good practice: of personal information and/or passwords contained in call recordings. • Masking credit card, bank account details and other sensitive data like customer passwords where this would not affect employees' ability to do their job.	**Examples of poor practice:**

Box 6.5: Controls - passwords and user accounts	
Examples of good practice: • Individual user accounts – requiring passwords – in place for all systems containing customer data. • Password standards at least equivalent to those recommended by Get Safe Online – a government-backed campaign group. In July 2011 ~~At present~~, their recommended standard for passwords was ~~is~~ a combination of letters, numbers and keyboard symbols at least ~~seven~~ eight characters in length and changed regularly. • Measures to ensure passwords are robust. These might include controls to ensure that passwords can only be set in accordance with policy and the use of password-cracking software on a risk-based approach. • 'Straight-through processing', but only if complemented by accurate role-based access profiles and strong passwords.	**Examples of poor practice:** • The same user account and password used by multiple users to access particular systems. • Names and dictionary words used as passwords. • Systems that allow passwords to be set which do not comply with password policy. • Individuals share passwords. ~~Password sharing of any kind.~~

Box 6.6: Controls - monitoring access to customer data	
Examples of good practice: • Risk-based, proactive monitoring of staff's access to customer data to ensure it is being accessed and/or updated for a	**Examples of poor practice:** • Assuming that vetted staff with appropriate access rights will always act appropriately. Staff can breach procedures, for example by looking at account information relating

Box 6.6: Controls - monitoring access to customer data	
Examples of good practice: genuine business reason. • The use of software designed to spot suspicious activity by employees with access to customer data. Such software may not be useful in its 'off-the-shelf' format so it is good practice for firms to ensure that it is tailored to their business profile. • Strict controls over superusers' access to customer data and independent checks of their work to ensure they have not accessed, manipulated or extracted data that was not required for a particular task.	**Examples of poor practice:** to celebrities, be tempted to commit fraud themselves or be bribed or threatened to give customer data to criminals. • Failure to make regular use of management information about access to customer data. • Failing to monitor superusers or other employees with access to large amounts of customer data.

Box 6.7: Controls - data back-up	
Examples of good practice: • Firms conducting a proper risk assessment of threats to data security arising from the data back-up process – from the point that back-up tapes are produced, through the transit process to the ultimate place of storage. • Firms encrypting backed-up data that is held off-site, including while in transit. • Regular reviews of the level of encryption to ensure it remains appropriate to the current risk environment. • Back-up data being transferred by secure Internet links. • Due diligence on third parties that handle backed-up customer data so the firm has a good understanding of how it is secured, exactly who has access to it and how staff with access to it are vetted. • Staff with responsibility for holding backed-up data off-site being given assistance to do so securely. For example,	**Examples of poor practice:** • Firms failing to consider data security risk arising from the backing up of customer data. • A lack of clear and consistent procedures for backing up data, resulting in data being backed up in several different ways at different times. This makes it difficult for firms to keep track of copies of their data. • Unrestricted access to back-up tapes for large numbers of staff at third party firms. • Back-up tapes being held insecurely by firm's employees; for example, being left in their cars or at home on the kitchen table.

Box 6.7: Controls - data back-up	
Examples of good practice: firms could offer to pay for a safe to be installed at the staff member's home. • Firms conducting spot checks to ensure that data held off-site is held~~done so~~ in accordance with accepted policies and procedures.	**Examples of poor practice:**

Box 6.8: Controls - access to the internet and email	
Examples of good practice: • Giving internet and email access only to staff with a genuine business need. • Considering the risk of data compromise when monitoring external email traffic, for example by looking for strings of numbers that might be credit card details. • Where proportionate, using specialist IT software to detect data leakage via email. • Completely blocking access to all internet content which allows web-based communication. This content includes web-based email, messaging facilities on social networking sites, external instant messaging and 'peer-to-peer' file-sharing software. • Firms that provide cyber-cafes for staff to use during breaks ensuring that web-based communications are blocked or that data cannot be transferred into the cyber-cafe, either in electronic or paper format.	**Examples of poor practice:** • Allowing staff who handle customer data to have access to the Internet and email if there is no business reason for this. • Allowing access to web-based communication internet sites. This content includes web-based email, messaging facilities on social networking sites, external instant messaging and 'peer-to-peer' file-sharing software.

Box 6.9: Controls - key-logging devices	
Examples of good practice: • Regular sweeping for key-logging devices in parts of the firm where employees have access to large amounts of, or sensitive,	

Box 6.9: Controls - key-logging devices	
Examples of good practice: customer data. (Firms will also wish to conduct sweeps in other sensitive areas. For example, where money can be transferred.) • Use of software to determine whether unusual or prohibited types of hardware have been attached to employees' computers. • Raising awareness of the risk of key-logging devices. The vigilance of staff is a useful method of defence. • Anti-spyware software and firewalls etc in place and kept up to date.	

Box 6.10: Controls - laptop	
Examples of good practice: • The encryption of laptops and other portable devices containing customer data. • Controls that mitigate the risk of employees failing to follow policies and procedures. We have dealt with several cases of lost or stolen laptops ~~in the past year~~ that arose from firms' staff not doing what they should. • Maintaining an accurate register of laptops issued to staff. • Regular audits of the contents of laptops to ensure that only staff who are authorised to hold customer data on their laptops are doing so and that this is for genuine business reasons. • The wiping of shared laptops' hard drives between uses.	**Examples of poor practice:** • Unencrypted customer data on laptops. • A poor understanding of which employees have been issued or are using laptops to hold customer data. • Shared laptops used by staff without being signed out or wiped between uses.

Box 6.11: Controls - portable media including USB devices and CDs	
Examples of good practice: • Ensuring that only staff with a genuine business need can download customer data to portable media such as USB devices and CDs. • Ensuring that staff authorised to hold customer data on portable media can only do so if it is encrypted. • Maintaining an accurate register of staff allowed to use USB devices and staff who have been issued USB devices. • The use of software to prevent and/or detect individuals using personal USB devices. • Firms reviewing regularly and on a risk-based approach the copying of customer data to portable media to ensure there is a genuine business reason for it. • The automatic encryption of portable media attached to firms' computers. • Providing lockers for higher-risk staff such as call centre staff and superusers and restricting them from taking personal effects to their desks.	**Examples of poor practice:** • Allowing staff with access to bulk customer data – for example, superusers – to download to unencrypted portable media. • Failing to review regularly threats posed by increasingly sophisticated and quickly evolving personal technology such as mobile phones.

Box 6.12: Physical security	
Examples of good practice: • Appropriately restricted access to areas where large amounts of customer data ~~is~~ are accessible, such as server rooms, call centres and filing areas. • Using robust intruder deterrents such as keypad entry doors, alarm systems, grilles or barred windows, and closed circuit television (CCTV). • Robust procedures for logging visitors and ensuring adequate supervision of them	**Examples of poor practice:** • Allowing staff or other persons with no genuine business need to access areas where customer data is held. • Failure to check electronic records showing who has accessed sensitive areas of the office. • Failure to lock away customer records and files when the office is left unattended.

Box 6.12: Physical security	
Examples of good practice:	**Examples of poor practice:**
while on-site. • Training and awareness programmes for staff to ensure they are fully aware of more basic risks to customer data arising from poor physical security. • Employing security guards, cleaners etc directly to ensure an appropriate level of vetting and reduce risks that can arise through third-party suppliers accessing customer data. • Using electronic swipe card records to spot unusual behaviour or access to high risk areas. • Keeping filing cabinets locked during the day and leaving the key with a trusted member of staff. • An enforced clear-desk policy.	

Box: 6.13: Disposal of customer data	
Examples of good practice:	**Examples of poor practice:**
• Procedures that result in the production of as little paper-based customer data as possible. • Treating all paper as 'confidential waste' to eliminate confusion among employees about which type of bin to use. • All customer data disposed of by employees securely, for example by using shredders (preferably cross-cut rather than straight-line shredders) or confidential waste bins. • Checking general waste bins for the	• Poor awareness among staff about how to dispose of customer data securely. • Slack procedures that present opportunities for fraudsters, for instance when confidential waste is left unguarded on the premises before it is destroyed. • Staff working remotely failing to dispose of customer data securely. • Firms failing to provide guidance or assistance to remote workers who need to dispose of an obsolete home computer. • Firms stockpiling obsolete computers and

Box: 6.13: Disposal of customer data	
Examples of good practice: accidental disposal of customer data. • Using a third party supplier, preferably one with BSIA[11] accreditation, which provides a certificate of secure destruction, to shred or incinerate paper-based customer data. It is important for firms to have a good understanding of the supplier's process for destroying customer data and their employee vetting standards. • Providing guidance for travelling or home-based staff on the secure disposal of customer data. • Computer hard drives and portable media being properly wiped (using specialist software) or destroyed as soon as they become obsolete.	**Examples of poor practice:** other portable media for too long and in insecure environments. • Firms relying on others to erase or destroy their hard drives and other portable media securely without evidence that this has been done competently.

Box 6.14: Managing third-party suppliers	
Examples of good practice: • Conducting due diligence of data security standards at third-party suppliers before contracts are agreed. • Regular reviews of third-party suppliers' data security systems and controls, with the frequency of review dependent on data security risks identified. • Ensuring third-party suppliers' vetting standards are adequate by testing the checks performed on a sample of staff with access to customer data. • Only allowing third-party IT suppliers access to customer databases for specific tasks on a case-by-case basis. • Third-party suppliers being subject to procedures for reporting data security	**Examples of poor practice:** • Allowing third-party suppliers to access customer data when no due diligence of data security arrangements has been performed. • Firms not knowing exactly which third-party staff have access to their customer data. • Firms not knowing how third-party suppliers' staff have been vetted. • Allowing third-party staff unsupervised access to areas where customer data is held when they have not been vetted to the same standards as employees. • Allowing IT suppliers unrestricted or unmonitored access to customer data.

[11] British Security Industry Association

Box 6.14: Managing third-party suppliers	
Examples of good practice: breaches within an agreed timeframe. • The use of secure internet links to transfer data to third parties.	**Examples of poor practice:** • A lack of awareness of when/how third-party suppliers can access customer data and failure to monitor such access. • Unencrypted customer data being sent to third parties using unregistered post.

Box 6.15: Internal audit and compliance monitoring	
Examples of good practice: • Firms seeking external assistance where they do not have the necessary in-house expertise or resources. • Compliance and internal audit conducting specific reviews of data security which cover all relevant areas of the business including IT, security, HR, training and awareness, governance and third-party suppliers. • Firms using expertise from across the business to help with the more technical aspects of data security audits and compliance monitoring.	**Examples of poor practice:** • Compliance focusing only on compliance with data protection legislation and failing to consider adherence to data security policies and procedures. • Compliance consultants adopting a 'one size fits all' approach to different clients' businesses.

7 Review of financial crime controls in offshore centres (2008)

Who should read this chapter? This chapter is relevant to:

- **all firms** subject to the financial crime rules in SYSC 3.2.6R or SYSC 6.1.1R; and
- **e-money institutions** and **payment institutions** within our supervisory scope

who have or are considering establishing operations in offshore centres.

7.1 In the second half of 2008 we reviewed how financial services firms in the UK were addressing financial crime risks in functions they had moved to offshore centres. The review followed on from our report into data security in financial services (April 2008 – http://www.fsa.gov.uk/pubs/other/data_security.pdf).

7.2 The main financial crime risks we reviewed were: customer data being lost or stolen and used to facilitate fraud; money laundering; and fraud. The review found that, while there were good data security controls in place across the industry, continued effort was required to ensure controls did not break down and that they remained 'valid and risk-based'.

7.3 The review emphasised the importance of appropriate vetting and training of all staff, particularly with regard to local staff who had financial crime responsibilities. An examination revealed that training in this area was often lacking and not reflective of the needs of, and work done by, members of staff. The report emphasised that senior management should ensure that staff operating in these roles were given proper financial crime training as well as ensuring they possessed the appropriate technical know-how. The review also highlighted that, due to high staff turnover, firms needed appropriate and thorough vetting controls to supplement inadequate local electronic intelligence and search systems.

7.4 The contents of this report are reflected in Chapter 2 (Financial crime systems and controls) and Chapter 5 (Data security) of Part 1 of this Guide.

Our findings

7.5 You can read the findings of the FSA's thematic review here:

http://www.fsa.gov.uk/pages/About/What/financial_crime/library/reports/review_offshore.shtml

Consolidated examples of good and poor practice

7.6 This report did not contain consolidated examples of good and poor practice.

8 Financial services firms' approach to UK financial sanctions (2009)

Who should read this chapter? This chapter is relevant, and its statements of good and poor practice apply, 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:

8.1 In April 2009 we published the findings of our thematic review of firms' approach to UK financial sanctions. We received 228 responses to an initial survey from a broad range of firms across the financial services industry, ranging from small firms to major financial groups, both retail and wholesale. Tailored surveys were sent to different types of firms to ensure that the questions were relevant to the nature and scale of the business of each firm. We then selected a sub-sample of 25 firms to visit to substantiate the findings from the surveys.

8.2 The review highlighted areas where there was significant scope across the industry for improvement in firms' systems and controls to comply with the UK financial sanctions regime. We found that, while some firms had robust systems in place that were appropriate to their business need, others, including some major firms, lacked integral infrastructure and struggled with inappropriate systems for their business. In small firms in particular, we found a widespread lack of awareness of the UK financial sanctions regime.

8.3 The report examined a number of key areas of concern which included an in-depth look at whether senior management were aware of their responsibilities and, if so, were responding in an appropriate manner. We also identified issues over the implementation of policies and procedures, particularly those put in place to ensure that staff were adequately trained, were kept aware of changes in this area, and knew how to respond when sanctions were imposed. We also had concerns about firms' screening of clients, both initially and as an ongoing process.

8.4 The contents of this report are reflected in Chapter 2 (Financial crime systems and controls) and Chapter 7 (Sanctions and asset freezes) of Part 1 of this Guide.

Our findings

8.5 You can read the findings of the FSA's thematic review here:

www.fsa.gov.uk/pubs/other/Sanctions_final_report.pdf

Consolidated examples of good and poor practice

Box 8.1: Senior management responsibility	
Examples of good practice: • ~~Full senior~~Senior management ~~and/or Board-level~~ involvement in approving and taking responsibility for policies and procedures. • ~~High~~ A level of senior management awareness of the firm's obligations regarding financial sanctions sufficient to enable them to discharge their functions effectively. • Appropriate escalation ~~Senior management involvement~~ in cases where a potential target match cannot easily be verified. • Adequate and appropriate resources allocated by senior management. • Appropriate escalation of actual target matches and breaches of UK financial sanctions. ~~Senior management notified of all actual matches and, if it should arise, all breaches of UK financial sanctions in an appropriate and timely manner~~.	**Examples of poor practice:** • No senior management involvement or understanding regarding the firm's obligations under the UK financial sanctions regime, or its systems and controls to comply with it. • No, or insufficient, management oversight of the day-to-day operation of systems and controls. • Failure to include assessments of the financial sanctions systems and controls as a normal part of internal audit programmes. • No senior management involvement in any cases where a potential target match cannot easily be verified. • Senior management ~~not~~never being made aware of a target match or breach of sanctions for an existing customer. • Inadequate or inappropriate resources allocated to financial sanctions compliance with our requirements.

Box 8.2: Risk assessment	
Examples of good practice: • Conducting a comprehensive risk assessment, based on a good understanding of the financial sanctions regime, covering the risks that may be posed by clients, transactions, services, products and jurisdictions. • Taking into account associated parties, such as directors and beneficial owners. • A formal documented risk assessment with a clearly documented rationale for the	**Examples of poor practice:** • Not assessing the risks that the firm may face of breaching financial sanctions. • Risk assessments that are based on misconceptions.

approach.	

Box 8.3: Policies and procedures	
Examples of good practice: • Documented policies and procedures in place, which clearly set out a firm's approach to complying with its legal and regulatory requirements in this area. • Group-wide policies for UK financial sanctions screening ~~across the group~~, to ensure that business unit-specific policies and procedures reflect ~~at~~ the ~~very least the minimum~~ standard set out in group policy. • Effective procedures to screen against the Consolidated List[12] ~~Treasury list~~ that are appropriate for the business, covering customers, transactions and services across all products and business lines. • Clear, simple and well understood escalation procedures to enable staff to raise financial sanctions concerns with management. • Regular review and update of policies and procedures. • Regular reviews of the effectiveness of policies, procedures, systems and controls by the firm's internal audit function or another independent party. • Procedures that include ongoing monitoring/screening of clients.	**Examples of poor practice:** • No policies or procedures in place for complying with the legal and regulatory requirements of the UK financial sanctions regime. • Internal audits of procedures carried out by persons with responsibility for oversight of financial sanctions procedures, rather than an independent party.

Box 8.4: Staff training and awareness	
Examples of good practice: • Regularly updated training and awareness programmes that are relevant and	**Examples of poor practice:** • No training on financial sanctions. • Relevant staff unaware of the firm's

[12] See Part 1 Annex 1 for descriptions of common terms

appropriate for employees' particular roles. • Testing to ensure that employees have a good understanding of financial sanctions risks and procedures. • Ongoing monitoring of employees' work to ensure they understand the financial sanctions procedures and are adhering to them. • Training provided to each business unit covering both the group-wide and business unit-specific policies on financial sanctions.	policies and procedures to comply with the UK financial sanctions regime. • Changes to the financial sanctions policies, procedures, systems and controls are not communicated to relevant staff.

Box 8.5: Screening during client take-on	
Examples of good practice:	**Examples of poor practice:**
• An effective screening system appropriate to the nature, size and risk of the firm's business. • Screening against the Consolidated List ~~Treasury list~~ at the time of client take-on before providing any services or undertaking any transactions for a customer. • Screening directors and beneficial owners of corporate customers. • Screening third party payees where adequate information is available. • Where the firm's procedures require dual control (e.g. a 'four eyes' check) to be used, having in place an effective process to ensure this happens. • The use of 'fuzzy matching' where automated screening systems are used. • Where a commercially available automated screening system is implemented, making sure that there is a full understanding of the capabilities and limits of the system.	• ~~Screening retrospectively, rather than at the time of client take-on.~~ • Screening only on notification of a claim on an insurance policy, rather than during client take-on. • Relying on other FSA-authorised firms and compliance consultants to screen clients against the Consolidated List ~~Treasury list~~ without taking reasonable steps to ensure that they are doing so effectively. • Assuming that AML customer due diligence checks include screening against the Consolidated List ~~Treasury~~. • Failing to screen UK-based clients on the assumption that there are no UK-based persons or entities on the Consolidated List ~~Treasury list~~ or failure to screen due to any other misconception. • Large global institutions with millions of clients using manual screening, increasing the likelihood of human error and leading to matches being missed. • IT systems that cannot flag potential

Box 8.5: Screening during client take-on	
Examples of good practice:	**Examples of poor practice:** matches clearly and prominently. • Firms calibrating their screening rules too narrowly or too widely so that they, for example, match only exact names with the Consolidated List ~~Treasury list~~ or generate large numbers of resource intensive false positives. • Regarding the implementation of a commercially available sanctions screening system as a panacea, with no further work required by the firm. • Failing to tailor a commercially available sanctions screening system to the firm's requirements.

Box 8.6: Ongoing screening	
Examples of good practice: • Screening of the entire client base within a reasonable time following updates to the Consolidated List ~~Treasury list~~. • Ensuring that customer data used for ongoing screening is up to date and correct. • Processes that include screening for indirect as well as direct customers and also third party payees, wherever possible. • Processes that include screening changes to corporate customers' data (e.g. when new directors are appointed or if there are changes to beneficial owners). • Regular reviews of the calibration and rules of automated systems to ensure they are operating effectively. • Screening systems calibrated in accordance with the firm's risk appetite, rather than the settings suggested by	**Examples of poor practice:** • No ongoing screening of customer databases or transactions. • Failure to screen directors and beneficial owners of corporate customers and/or third party payees where adequate information is available. • Failure to review the calibration and rules of automated systems, or to set the calibration in accordance with the firm's risk appetite. • Flags on systems that are dependent on staff looking for them. • Controls on systems that can be overridden without referral to compliance.

Box 8.6: Ongoing screening	
Examples of good practice: external software providers. • Systems calibrated to include 'fuzzy matching', including name reversal, digit rotation and character manipulation. • Flags on systems prominently and clearly identified. • Controls that require referral to relevant compliance staff prior to dealing with flagged individuals or entities.	**Examples of poor practice:**

Box 8.7: Treatment of potential target matches	
Examples of good practice: • Procedures for investigating whether a potential match is an actual target match or a false positive. • Procedures for freezing accounts where an actual target match is identified. • Procedures for notifying the Treasury's AFU promptly of any confirmed matches. • Procedures for notifying senior management of target matches and cases where the firm cannot determine whether a potential match is the actual target on the Consolidated List ~~Treasury list~~. • A clear audit trail of the investigation of potential target matches and the decisions and actions taken, such as the rationale for deciding that a potential target match is a false positive.	**Examples of poor practice:** • No procedures in place for investigating potential matches with the Consolidated List ~~Treasury list~~. • Discounting actual target matches incorrectly as false positives due to insufficient investigation. • No audit trail of decisions where potential target matches are judged to be false positives.

9 Anti-bribery and corruption in commercial insurance broking (2010)

Who should read this chapter? This chapter is relevant, and its statements of good and poor practice apply, to:

- **commercial insurance brokers** and **other firms** who are subject to the financial crime rules in SYSC 3.2.6R or SYSC 6.1.1R**;** and
- **e-money institutions** and **payment institutions** within our supervisory scope

except that **Box 9.3** and **Box 9.4** only apply to those **firms or institutions who use third parties to win business**. It may also be of interest to other firms who are subject to SYSC 3.2.6R and SYSC 6.1.1R.

Content: This chapter contains sections on:

9.1 In May 2010 we published the findings of our review into the way commercial insurance broker firms in the UK addressed the risks of becoming involved in corrupt practices such as bribery. We visited 17 broker firms. Although this report focused on commercial insurance brokers, the findings are relevant in other sectors.

9.2 The report examined standards in managing the risk of illicit payments or inducements to, or on behalf of, third parties in order to obtain or retain business.

9.3 The report found that many firms' approach towards high-risk business was not of an acceptable standard and that there was a risk that firms were not able to demonstrate that adequate procedures were in place to prevent bribery from occurring.

9.4 The report identified a number of common concerns including weak governance and a poor understanding of bribery and corruption risks among senior managers as well as very little or no specific training and weak vetting of staff. We found that there was a general failure to implement a risk-based approach to anti-bribery and corruption and very weak due diligence and monitoring of third-party relationships and payments.

9.5 The contents of this report are reflected in Chapter 2 (Financial crime systems and controls) and Chapter 6 (Bribery and corruption) of Part 1 of this Guide.

Our findings

9.6 You can read the findings of the FSA's thematic review here:

www.fsa.gov.uk/pubs/anti_bribery.pdf

Consolidated examples of good and poor practice

Box 9.1: Governance and management information	
Examples of good practice: • Clear, documented responsibility for anti-bribery and corruption apportioned to either a single senior manager or a committee with appropriate Terms of Reference and senior management membership, reporting ultimately to the Board. • Good Board-level and senior management understanding of the bribery and corruption risks faced by the firm, the materiality to their business and how to apply a risk-based approach to anti-bribery and corruption work. • Swift and effective senior management-led response to significant bribery and corruption events, which highlight potential areas for improvement in systems and controls. • Regular MI to the Board and other relevant senior management forums. • MI includes information about third parties including (but not limited to) new third party accounts, their risk classification, higher risk third party payments for the preceding period, changes to third-party bank account details and unusually high commission paid to third parties. • MI submitted to the Board ensures they are adequately informed of any external developments relevant to bribery and corruption. • Actions taken or proposed in response to issues highlighted by MI are minuted and	**Examples of poor practice:** • Failing to allocate official responsibility for anti-bribery and corruption to a single senior manager or appropriately formed committee. • A lack of awareness and/or engagement in anti-bribery and corruption at senior management or Board level. • Little or no MI sent to the Board about higher risk third party relationships or payments. • Failing to include details of wider issues, such as new legislation or regulatory developments in MI. • IT systems unable to produce the necessary MI.

Box 9.1: Governance and management information	
Examples of good practice: acted on appropriately.	**Examples of poor practice:**

Box 9.2: Risk assessment and responses to significant bribery and corruption events	
Examples of good practice: • Regular assessments of bribery and corruption risks with a specific senior person responsible for ensuring this is done, taking into account the country and class of business involved as well as other relevant factors. • More robust due diligence on and monitoring of higher risk third-party relationships. • Thorough reviews and gap analyses of systems and controls against relevant external events, with strong senior management involvement or sponsorship. • Ensuring review teams have sufficient knowledge of relevant issues and supplementing this with external expertise where necessary. • Establishing clear plans to implement improvements arising from reviews, including updating policies, procedures and staff training. • Adequate and prompt reporting to SOCA[13] and us of any inappropriate payments identified during business practice review.	**Examples of poor practice:** • Failing to consider the bribery and corruption risks posed by third parties used to win business. • Failing to allocate formal responsibility for anti-bribery and corruption risk assessments. • A 'one size fits all' approach to third-party due diligence. • Failing to respond to external events which may draw attention to weaknesses in systems and controls. • Taking too long to implement changes to systems and controls after analysing external events. • Failure to bolster insufficient in-house knowledge or resource with external expertise. • Failure to report inappropriate payments to SOCA and a lack of openness in dealing with us concerning any material issues identified.

Box 9.3: Due diligence on third-party relationships	
Examples of good practice: • Establishing and documenting policies with a clear definition of a 'third party'	**Examples of poor practice:** • Failing to carry out or document due

[13] Serious Organised Crime Agency. See Part 1 Annex 1 for common terms.

Box 9.3: Due diligence on third-party relationships

Examples of good practice:	Examples of poor practice:
and the due diligence required when establishing and reviewing third-party relationships. • More robust due diligence on third parties which pose the greatest risk of bribery and corruption, including a detailed understanding of the business case for using them. • Having a clear understanding of the roles clients, reinsurers, solicitors and loss adjusters play in transactions to ensure they are not carrying out higher risk activities. • Taking reasonable steps to verify the information provided by third parties during the due diligence process. • Using third party forms which ask relevant questions and clearly state which fields are mandatory. • Having third party account opening forms reviewed and approved by compliance, risk or committees involving these areas. • Using commercially-available intelligence tools, databases and/or other research techniques such as internet search engines to check third-party declarations about connections to public officials, clients or the assured. • Routinely informing all parties involved in the insurance transaction about the involvement of third parties being paid commission. • Ensuring current third-party due diligence standards are appropriate when business is acquired that is higher risk than existing business. • Considering the level of bribery and corruption risk posed by a third party when	diligence on third-party relationships. • Relying heavily on the informal 'market view' of the integrity of third parties as due diligence. • Relying on the fact that third-party relationships are longstanding when no due diligence has ever been carried out. • Carrying out only very basic identity checks as due diligence on higher risk third parties. • Asking third parties to fill in account opening forms which are not relevant to them (e.g. individuals filling in forms aimed at corporate entities). • Accepting vague explanations of the business case for using third parties. • Approvers of third-party relationships working within the broking department or being too close to it to provide adequate challenge. • Accepting instructions from third parties to pay commission to other individuals or entities which have not been subject to due diligence. • Assuming that third-party relationships acquired from other firms have been subject to adequate due diligence. • Paying high levels of commission to third parties used to obtain or retain higher risk business, especially if their only role is to introduce the business. • Receiving bank details from third parties via informal channels such as email, particularly if email addresses are from webmail (e.g. Hotmail) accounts or do not appear to be obviously connected to the third party.

Box 9.3: Due diligence on third-party relationships	
Examples of good practice: agreeing the level of commission. • Setting commission limits or guidelines which take into account risk factors related to the role of the third party, the country involved and the class of business. • Paying commission to third parties on a one-off fee basis where their role is pure introduction. • Taking reasonable steps to ensure that bank accounts used by third parties to receive payments are, in fact, controlled by the third party for which the payment is meant. For example, broker firms might wish to see the third party's bank statement or have the third party write them a low value cheque. • Higher or extra levels of approval for high risk third-party relationships. • Regularly reviewing third-party relationships to identify the nature and risk profile of third-party relationships. • Maintaining accurate central records of approved third parties, the due diligence conducted on the relationship and evidence of periodic reviews.	**Examples of poor practice:** • Leaving redundant third-party accounts 'live' on the accounting systems because third-party relationships have not been regularly reviewed. • Being unable to produce a list of approved third parties, associated due diligence and details of payments made to them.

Box 9.4: Payment controls	
Examples of good practice: • Ensuring adequate due diligence and approval of third-party relationships before payments are made to the third party. • Risk-based approval procedures for payments and a clear understanding of why payments are made. • Checking third-party payments individually prior to approval, to ensure	**Examples of poor practice:** • Failing to check whether third parties to whom payments are due have been subject to appropriate due diligence and approval. • The inability to produce regular third-party payment schedules for review. • Failing to check thoroughly the nature, reasonableness and appropriateness of

consistency with the business case for that account. • Regular and thorough monitoring of third-party payments to check, for example, whether a payment is unusual in the context of previous similar payments. • A healthily sceptical approach to approving third-party payments. • Adequate due diligence on new suppliers being added to the Accounts Payable system. • Clear limits on staff expenditure, which are fully documented, communicated to staff and enforced. • Limiting third-party payments from Accounts Payable to reimbursements of genuine business-related costs or reasonable entertainment. • Ensuring the reasons for third-party payments via Accounts Payable are clearly documented and appropriately approved. • The facility to produce accurate MI to facilitate effective payment monitoring.	gifts and hospitality. • No absolute limits on different types of expenditure, combined with inadequate scrutiny during the approvals process. • The giving or receipt of cash gifts.

Box 9.5: Staff recruitment and vetting	
Examples of good practice: • Vetting staff on a risk-based approach, taking into account financial crime risk. • Enhanced vetting – including checks of credit records, criminal records, financial sanctions lists, commercially available intelligence databases and the CIFAS Staff Fraud Database – for staff in roles with higher bribery and corruption risk. • A risk-based approach to dealing with adverse information raised by vetting checks, taking into account its seriousness and relevance in the context of the	**Examples of poor practice:** • Relying entirely on an individual's market reputation or market gossip as the basis for recruiting staff. • Carrying out enhanced vetting only for senior staff when more junior staff are working in positions where they could be exposed to bribery or corruption issues. • Failing to consider on a continuing basis whether staff in higher risk positions are becoming vulnerable to committing fraud or being coerced by criminals. • Relying on contracts with employment

individual's role or proposed role. • Where employment agencies are used to recruit staff in higher risk positions, having a clear understanding of the checks they carry out on prospective staff. • Conducting periodic checks to ensure that agencies are complying with agreed vetting standards. • A formal process for identifying changes in existing employees' financial soundness which might make them more vulnerable to becoming involved in, or committing, corrupt practices.	agencies covering staff vetting standards without checking periodically that the agency is adhering to them. • Temporary or contract staff receiving less rigorous vetting than permanently employed colleagues carrying out similar roles.

Box 9.6: Training and awareness	
Examples of good practice: • Providing good quality, standard training on anti-bribery and corruption for all staff. • Additional anti-bribery and corruption training for staff in higher risk positions. • Ensuring staff responsible for training others have adequate training themselves. • Ensuring training covers practical examples of risk and how to comply with policies. • Testing staff understanding and using the results to assess individual training needs and the overall quality of the training. • Staff records setting out what training was completed and when. • Providing refresher training and ensuring it is kept up to date.	**Examples of poor practice:** • Failing to provide training on anti-bribery and corruption, especially to staff in higher risk positions. • Training staff on legislative and regulatory requirements but failing to provide practical examples of how to comply with them. • Failing to ensure anti-bribery and corruption policies and procedures are easily accessible to staff. • Neglecting the need for appropriate staff training in the belief that robust payment controls are sufficient to combat anti-bribery and corruption.

Box 9.7: Risk arising from remuneration structures	
Examples of good practice: • Assessing whether remuneration structures give rise to increased risk of bribery and	**Examples of poor practice:** • Bonus structures for staff in higher risk positions which are directly linked (e.g. by

corruption. • Determining individual bonus awards on the basis of several factors, including a good standard of compliance, not just the amount of income generated. • Deferral and clawback provisions for bonuses paid to staff in higher risk positions.	a formula) solely to the amount of income or profit they produce, particularly when bonuses form a major part, or the majority, of total remuneration.

Box 9.8: Incident reporting	
Examples of good practice: • Clear procedures for whistleblowing and reporting suspicions, and communicating these to staff. • Appointing a senior manager to oversee the whistleblowing process and act as a point of contact if an individual has concerns about their line management. • Respect for the confidentiality of workers who raise concerns. • Internal and external suspicious activity reporting procedures in line with the Joint Money Laundering Steering Group guidance. • Keeping records or copies of internal suspicion reports which are not forwarded as SARs for future reference and possible trend analysis. • Financial crime training covers whistleblowing procedures and how to report suspicious activity.	**Examples of poor practice:** • Failing to report suspicious activity relating to bribery and corruption. • No clear internal procedure for whistleblowing or reporting suspicions. • No alternative reporting routes for staff wishing to make a whistleblowing disclosure about their line management or senior managers. • A lack of training and awareness in relation to whistleblowing the reporting of suspicious activity.

Box 9.9: The role of compliance and internal audit	
Examples of good practice: • Compliance and internal audit staff receiving specialist training to achieve a very good knowledge of bribery and	**Examples of poor practice:** • Failing to carry out compliance or internal audit work on anti-bribery and corruption.

corruption risks. • Effective compliance monitoring and internal audit reviews which challenge not only whether processes to mitigate bribery and corruption have been followed but also the effectiveness of the processes themselves. • Independent checking of compliance's operational role in approving third party relationships and accounts, where relevant. • Routine compliance and/or internal audit checks of higher risk third party payments to ensure there is appropriate supporting documentation and adequate justification to pay.	• Compliance, in effect, signing off their own work, by approving new third party accounts and carrying out compliance monitoring on the same accounts. • Compliance and internal audit not recognising or acting on the need for a risk-based approach.

10 The Small Firms Financial Crime Review (2010)

Who should read this chapter? This chapter is relevant, and its statements of good and poor practice apply, to **small firms** in all sectors who are subject to the financial crime rules in SYSC 3.2.6R or SYSC 6.1.1R and small **e-money institutions** and **payment institutions** within our supervisory scope.

Content: This chapter contains sections on:

10.1 In May 2010 we published the findings of our thematic review into the extent to which small firms across the financial services industry addressed financial crime risks in their business. The review conducted visits to 159 small retail and wholesale firms in a variety of financial sectors. It was the first systematic review of financial crime systems and controls in small firms conducted by the FSA.

10.2 The review covered three main areas: anti-money laundering and financial sanctions; data security; and fraud controls. The review sought to determine whether firms understood clearly the requirements placed on them by the wide range of legislation and regulations to which they were subject.

10.3 We found that firms generally demonstrated a reasonable awareness of their obligations, particularly regarding AML systems and controls. But we found weaknesses across the sector regarding the implementation of systems and controls put in place to reduce firms' broader financial crime risk.

10.4 The review emphasised the key role that the small firms sector often plays in acting as the first point of entry for customers to the wider UK financial services industry; and the importance, therefore, of firms having adequate customer due diligence measures in place. The report flagged up concerns relating to weaknesses in firms' enhanced due diligence procedures when dealing with high-risk customers.

10.5 We concluded that, despite an increased awareness of the risks posed by financial crime and information supplied by the FSA, small firms were generally weak in their assessment and mitigation of financial crime risks.

10.6 The contents of this report are reflected in Chapter 2 (Financial crime systems and controls), Chapter 3 (Money laundering and terrorist financing), Chapter 4 (Fraud), Chapter 5 (Data security) and Chapter 7 (Sanctions and asset freezes) of Part 1 of this Guide.

Our findings

10.7 You can read the findings of the FSA's thematic review here:

www.fsa.gov.uk/smallfirms/pdf/financial_crime_report.pdf

Consolidated examples of good and poor practice

Box 10.1: Regulatory/Legal obligations	
Examples of good practice: • A small IFA used policies and procedures which had been prepared by consultants but the MLRO had tailored these to the firm's business. There was also a risk assessment of customers and products included in an MLRO report which was updated regularly. • One general insurance (GI) intermediary had an AML policy in place which was of a very good standard and included many good examples of AML typologies relevant to GI business. Despite the fact that there is no requirement for an MLRO for a business of this type the firm had appointed an individual to carry out an MLRO function as a point of good practice.	**Examples of poor practice:** • An MLRO at an IFA was not familiar with the JMLSG guidance and had an inadequate knowledge of the firm's financial crime policies and procedures.

Box 10.2: Account opening procedures	
Examples of good practice:	**Examples of poor practice:**

Box 10.2: Account opening procedures	
Examples of good practice: • A discretionary portfolio manager had procedures that required the verification of the identity of all beneficial owners. The firm checked its customer base against sanctions lists and had considered the risks associated with PEPs. Most new customers were visited by the adviser at home and in these cases the advisers would usually ask for identity verification documents on the second meeting with the customer. Where business was conducted remotely, more (three or four) identity verification documents were required and the source of funds exemption was not used.	**Examples of poor practice:** • An IFA commented that they only dealt with investment customers that were well known to the firm or regulated entities. However, the firm had some high risk customers who were subject to very basic due diligence (e.g.: copy of passport). The firm said that they were concerned about the high reputational impact an AML incident could have on their small, young business. The firm stated that they would deal with PEPs but with appropriate care. However, the firm did not have a rigorous system in place to be able to identify PEPs – this was a concern given the nationality and residence of some underlying customers. The firm appeared to have reasonable awareness of the sanctions requirements of both the Treasury and the United States Office of Foreign Assets Control (OFAC), but there was no evidence in the customer files of any sanctions checking. • A venture capital firm had policies in place which required a higher level of due diligence and approval for high-risk customers. However, they had no system in place by which they could identify this type of customer.

Box 10.3: Monitoring activity	
Examples of good practice: • A credit union used a computer-based monitoring system which had been specially designed for business of this type. The system was able to produce a number of exception reports relating to the union's members, including frequency of transactions and defaulted payments. The exceptions reports were reviewed daily. If there had been no activity on an account for 12 months it was suspended. If the customer was to return and request a	

Box 10.3: Monitoring activity	
Examples of good practice: withdrawal they would be required to prove their identity again. • A Personal Pension Operator's procedure for higher risk customers included gathering extra source of funds proof at customer take-on. The firm also conducted manual monitoring and produced valuation statements twice a year. • Within a GI intermediary firm, there was a process where, if a customer made a quick claim after the policy has been taken out, their records were flagged on the firm's monitoring system. This acted as an alert for any possible suspicious claims in the future.	

Box 10.4: Suspicious activity reporting	
	Examples of poor practice: • One MLRO working at an IFA firm commented that he would forward all internal SARs he received to SOCA and would not exercise any judgement himself as to the seriousness of these SARs. • At an IFA the MLRO did not demonstrate any knowledge of how to report a SAR to SOCA, what to report to SOCA, or how to draft a SAR. The firm's policies and procedures contained a pro forma SAR but this was not a document the MLRO was familiar with. • An IFA was unaware of the difference between reporting suspicions to SOCA and sanctions requirements, believing that if he identified a person on the Consolidated List ~~Sanctions list~~ he should carry on as normal and just report it as a SAR to SOCA.

Box 10.5: Records	
Examples of good practice: • An advising-only intermediary firm used a web-based system as its database of leads, contact names and addresses. It also stored telephone and meeting notes there which were accessed by staff using individual passwords. • A home finance broker classified customers as A, B or C for record keeping purposes. A's being Active, B's being 'one-off or infrequent business' who he maintained contact with via a regular newsletter and C's being archived customers~~, the records for which he kept in his loft in the house~~.	**Examples of poor practice:** • A file review at an IFA revealed disorganised files and missing KYC documentation in three of five files reviewed. Files did not always include a checklist. (~~The firm was advised~~ We expect that KYC information should be kept together in the file so that it ~~was~~ is easily identifiable and auditable.)

Box 10.6: Training	
Examples of good practice: • A GI Intermediary used an on-line training website (costing around £100 per employee per year). The firm believed that the training was good quality and included separate modules on financial crime which were compulsory for staff to complete. Staff were also required to complete refresher training. An audit of all training completed was stored on-line. • An IFA (sole trader) carried out on-line training on various financial crime topics. He also participated in conference call training where a trainer talked trainees through various topics while on-line; this was both time and travel efficient.	**Examples of poor practice:** • A GI Intermediary explained that the compliance manager carried out regular audits to confirm staff knowledge was sufficient. However, on inspection of the training files it appeared that training was largely limited to product information and customer service and did not sufficiently cover financial crime. • One credit union, apart from on-the-job training for new staff members, had no regular training in place and no method to test staff knowledge of financial crime issues.

Box 10.7: Responsibilities and risk assessments	
Examples of good practice: • At an IFA there was a clearly documented policy on data security which staff were	**Examples of poor practice:** • At an IFA, a risk assessment had been undertaken by the firm's compliance

Box 10.7: Responsibilities and risk assessments	
Examples of good practice:	**Examples of poor practice:**
tested on annually. The policy contained, but was not limited to, details around clear desks, non-sharing of passwords, the discouraging of the over-use of portable media devices, the secure disposal of data, and the logging of customer files removed and returned to the office. • An IFA had produced a written data security review of its business which had been prompted by their external consultants and largely followed the small firms' factsheet material on data security, provided by the FSA in April 2008. • In a personal pension operator, there was a full and comprehensive anti-fraud strategy in place and a full risk assessment had been carried out which was regularly reviewed. The firm's financial transactions were normally 'four eyed' as a minimum and there were strict mandates on cheque signatures for Finance Director and Finance Manager.	consultant but the firm demonstrated no real appreciation of the financial crime risks in its business. The risk assessment was not tailored to the risks inherent in that business. • An advising-only intermediary had its policies and procedures drawn up by an external consultant but these had not been tailored to the firm's business. The MLRO was unclear about investigating and reporting suspicious activity to SOCA. The firm's staff had not received formal training in AML or reporting suspicious activity to SOCA.

Box 10.8: Access to systems	
Examples of good practice:	**Examples of poor practice:**
• In a Discretionary Investment Management firm, the Chief Executive ensured that he signed off on all data user profiles ensuring that systems accesses were authorised by him. • A discretionary investment manager conducted five year referencing on new staff, verified personal addresses and obtained character references from acquaintances not selected by the candidate. They also carried out annual credit checks, CRB checks and open source Internet searches on staff. ~~They~~ There were role profiles for each job within the firm and these were reviewed	• In a financial advisory firm there was no minimum length for passwords, (although these had to be alpha/numeric) and the principal of the firm plus one other colleague knew all staff members' passwords. • In an advising-only intermediary, staff set their own systems passwords which had no defined length or complexity and were only changed every six months.

Box 10.8: Access to systems	
Examples of good practice: monthly for accuracy. • In a venture capital firm they imposed a minimum ten character (alpha/numeric, upper/lower case) password for systems access which had a 45-day enforced change period.	**Examples of poor practice:**

Box 10.9: Outsourcing	
Examples of good practice: • A discretionary investment manager used an external firm for IT support and had conducted its own on-site review of the IT firm's security arrangements. The same firm also insisted on CRB checks for cleaners. • An IFA had received a request from an introducer to provide names of customers who had bought a certain financial product. The firm refused to provide the data as it considered the request unnecessary and wanted to protect its customer data. It also referred the matter to the Information Commissioner who supported the firm's actions. • A general insurance intermediary employed office cleaners supplied by an agency that conducts due diligence including CRB checks. Office door codes were regularly changed and always if there was a change in staff. • In an authorised professional firm, unauthorised data access attempts by staff were monitored by the IT manager and email alerts sent to staff and management when identified. • In a general insurance intermediary the two directors had recently visited the offsite data storage facility to satisfy	**Examples of poor practice:** • An authorised professional firm employed the services of third-party cleaners, security staff, and an offsite confidential waste company, but had carried out no due diligence on any of these parties. • An IFA allowed a third-party IT consultant full access rights to its customer databank. Although the firm had a service agreement in place that allowed full audit rights between the advisor and the IT company to monitor the security arrangements put in place by the IT company, this had not been invoked by the IFA, in contrast to other firms visited where such audits had been undertaken. • In an authorised professional firm, Internet and Hotmail usage was only monitored if it was for longer than 20 minutes at any one time. There was also no clear-desk policy within the firm. • In an authorised professional firm there had been two incidents where people had walked into the office and stolen staff wallets and laptops.

Box 10.9: Outsourcing	
Examples of good practice: themselves about the security arrangements at the premises.	**Examples of poor practice:**

Box 10.10: Physical controls	
Examples of good practice: • At an IFA, staff email was monitored and monthly MI was produced, which included a monitoring of where emails had been directed to staff home addresses. • At an investment advisory firm, staff were prohibited from using the Internet and Hotmail accounts. USB ports had been disabled on hardware and laptops were encrypted.	**Examples of poor practice:** • In a general insurance intermediary which had poor physical security in terms of shop front access, there were many insecure boxes of historical customer records dotted around the office in no apparent order. The firm had no control record of what was stored in the boxes, saying only that they were no longer needed for the business.

Box 10.11: Data disposal	
Examples of good practice: • An advising and arranging intermediary used a third party company for all paper disposals, using secure locked bins provided by the third party. All paper in the firm was treated as confidential and 'secure paper management' was encouraged throughout the firm, enhanced by a monitored clear-desk policy. The firm was also aware that it needed to consider a process for secure disposal of electronic media as it was due to undergo a systems refit in the near future. • An IFA treated all customer paperwork as confidential and had onsite shredding facilities. For bulk shredding the firm used a third party who provided bags and tags for labelling sensitive waste for removal, and this was collected and signed for by the third party. The firm's directors had visited the third party's premises and	**Examples of poor practice:** • In an IFA there was a clear-desk policy that was not enforced and customer data was stored in unlocked cabinets which were situated in a part of the office accessible to all visitors to the firm.

Box 10.11: Data disposal	
Examples of good practice:	**Examples of poor practice:**
satisfied themselves of their processes. The directors periodically checked office bins for confidential waste being mishandled. PCs which had come to 'end of life' were wiped using reputable software and physically destroyed.	

Box 10.12: Data compromise incidents	
Examples of good practice:	**Examples of poor practice:**
• A general insurance broker had suffered a succession of break-ins to their offices. No data had been lost or stolen but the firm sought the advice of local police over the incidents and employed additional physical security as a result.	• In a general insurance intermediary, the IT manager said he would take responsibility for any data security incidents although there was no procedures in place for how to handle such occurrences. When asked about data security, the compliance officer was unable to articulate the financial crime risks that lax data security processes posed to the firm and said it would be something he would discuss with his IT manager.

Box 10.13: General fraud	
Examples of good practice:	**Examples of poor practice:**
• A small product provider had assessed the fraud risk presented by each product and developed appropriate controls to mitigate this risk based on the assessment. This assessment was then set out in the firm's Compliance Manual and was updated when new information became available. • A credit union did not permit its members to change address details over the telephone. These needed to be submitted in writing/email. The firm also considered ~~considering~~ the feasibility of allocating passwords to their members for accessing their accounts. The union had photographs of all its members which were taken when the account was opened. These were then	• One GI broker ~~customers~~ permitted customers to contact the firm by telephone to inform the firm of any amendments to their personal details (including change of address). To verify the identity of the person they were speaking to, the firm asked security questions. However, all the information that the firm used to verify the customer's identity was available in the public domain.

Box 10.13: General fraud	
Examples of good practice: used to verify the identity of the customer should they wish to withdraw money or apply for a loan from the union. • One discretionary investment manager kept full records of all customer contact including details of any phone calls. When receiving incoming calls from product providers, the firm required the caller to verify where they were calling from and provide a contact telephone number which they were then called back on before any customer details were discussed or instructions taken. • One general insurance intermediary was a member of a local association whose membership included law enforcement and Law Society representatives. This group met in order to share local intelligence to help improve their firms' defences against financial crime.	**Examples of poor practice:**

Box 10.14: Insurance fraud	
Examples of good practice: • A small general insurer had compiled a handbook which detailed indicators of potential insurance fraud. • An IFA had undertaken a risk assessment to understand where his business was vulnerable to insurance fraud. • An IFA had identified where their business may be used to facilitate insurance fraud and implemented more controls in these areas.	**Examples of poor practice:** • An IFA had a procedure in place to aid in the identification of high risk customers. However, once identified, this firm had no enhanced due diligence procedures in place to deal with such customers.

Box 10.15: Investment fraud

Examples of good practice:	Examples of poor practice:
• An IFA had undertaken a risk assessment for all high net worth customers. • A discretionary investment manager referred higher risk decisions (in respect of a high risk customer/value of funds involved) to a specific senior manager. • A personal pension operator carried out a financial crime risk assessment for newly introduced investment products.	• An IFA had a 'one size fits all' approach to identifying the risks associated with customers and investments.

Box 10.16: Mortgage fraud	
Examples of good practice:	**Examples of poor practice:**
• The majority of firms conducted customer fact finds. This allowed them to know their customers sufficiently to identify any suspicious behaviour. CDD[14] (including source of funds information) was also obtained early in the application process before the application was completed and submitted to the lender. • A home finance broker would not conduct any remote business – meeting all customers face-to-face. • An IFA had informally assessed the mortgage fraud risks the business faced and was aware of potentially suspicious indicators. The IFA also looked at the fraud risks associated with how the company approached the firm – e.g. the firm felt that a cold call from a customer may pose a greater risk than those which had been referred by longstanding customers.	• An IFA did not undertake any KYC checks, considering this to be the responsibility of the lender. • An IFA did not investigate source of funds. The firm stated this was because 'a bank would pick it up and report it.' • An IFA did not undertake extra verification of its non face-to-face customers.

Box 10.17: Staff/Internal fraud	
Examples of good practice:	**Examples of poor practice:**

[14] Customer Due Diligence. See Part 1 Annex 1 for common terms.

Box 10.17: Staff/Internal fraud	
Examples of good practice: • An IFA obtained full reference checks (proof of identity, eligibility to work and credit checks) prior to appointment. Original certificates or other original documentation was also requested. • An IFA ensured that staff vetting is repeated by completing a credit reference check on each member of staff. • An IFA set a low credit limit for each of its company credit cards. Bills are sent to the firm and each month the holder has to produce receipts to reconcile their claim. • At one authorised professional firm dual signatory requirements had to be met for all payments made over £5,000.	**Examples of poor practice:** • One general insurance intermediary did not undertake any background checks before appointing a member of staff or authenticate qualifications or references. • Company credit card usage was not monitored or reconciled at an IFA. An IFA had the same computer log-on used by all staff in the office no matter what their role.

11 Mortgage fraud against lenders (2011)

Who should read this chapter? This chapter is relevant, and its statements of good and poor practice apply, to **mortgage lenders** within our supervisory scope**.** It may also be of interest to other firms who are subject to the financial crime rules in SYSC 3.2.6R or SYSC 6.1.1R.

Content: This chapter contains sections on:

11.1 In June 2011 we published the findings of our thematic review into how mortgage lenders in the UK were managing the risks mortgage fraud posed to their businesses. Our project population of 20 banks and building societies was selected to be a representative sample of the mortgage lending market. The firms we visited accounted for 56% of the mortgage market in 2010.

11.2 Our review found the industry had made progress coming to terms with the problem of containing mortgage fraud over recent years. Defences were stronger, and the value of cross-industry cooperation was better recognised. However, we found that many in the industry could do better; we were disappointed, for example, that more firms were not actively participating in our Information From Lenders scheme and other industry-wide initiatives to tackle mortgage fraud. Other areas of concern we identified were to do with the adequacy of firms' resources for dealing with mortgage fraud, both in terms of the number and experience of staff; and we identified scope for significant improvement in the way lenders dealt with third parties such as brokers, valuers and conveyancers.

11.3 The contents of this report are reflected in Chapter 2 (Financial crime systems and controls) and Chapter 4 (Fraud) of Part 1 of this Guide.

Our findings

11.4 You can read the findings of the FSA's thematic review here:

www.fsa.gov.uk/pubs/other/mortgage_fraud.pdf

Consolidated examples of good and poor practice

Box 11.1: Governance, culture and information sharing	
Examples of good practice:	**Examples of poor practice:**
• A firm's efforts to counter mortgage fraud are coordinated, and based on consideration of where anti-fraud resources can be allocated to best effect. • Senior management engage with mortgage fraud risks and receive sufficient management information about incidents and trends. • A firm engages in cross-industry efforts to exchange information about fraud risks. • A firm engages front-line business areas in anti-mortgage fraud initiatives.	• A firm fails to ~~engage with~~ report relevant information to the FSA's Information From Lenders ~~project~~ scheme as per the FSA's guidance on IFL referrals. • A firm fails to define mortgage fraud clearly, undermining efforts to compile statistics related to mortgage fraud trends. • A firm does not allocate responsibility for countering mortgage fraud clearly within the management hierarchy.

Box 11.2: Applications processing and underwriting	
Examples of good practice:	**Examples of poor practice:**
• A firm's underwriting process can identify applications that may, based on a thorough assessment of risk flags relevant to the firm, present a higher risk of mortgage fraud. • Underwriters can contact all parties to the application process (customers, brokers, valuers etc.) to clarify aspects of the application. • The firm verifies that deposit monies for a mortgage transaction are from a legitimate source. • New or inexperienced underwriters receive training about mortgage fraud risks, potential risk indicators, and the firm's approach to tackling the issue.	• A firm's underwriters have a poor understanding of potential fraud indicators, whether through inexperience or poor training. • Underwriters' demanding work targets undermine efforts to contain mortgage fraud. • Communication between the fraud team and mortgage processing staff is weak. • A firm relying on manual underwriting has no checklists to ensure the application process is complete. • A firm requires underwriters to justify all declined applications to brokers.

Box 11.3: Mortgage fraud prevention, investigations and recoveries	
Examples of good practice:	**Examples of poor practice:**
• A firm routinely assesses fraud risks during the development of new mortgage products, with particular focus on fraud when it enters	• A firm's anti-fraud efforts are uncoordinated and under-resourced.

Box 11.3: Mortgage fraud prevention, investigations and recoveries	
Examples of good practice:	**Examples of poor practice:**
new areas of the mortgage market (such as sub-prime or buy-to-let). • A firm reviews existing mortgage books to identify fraud indicators. • Applications that are declined for fraudulent reasons result in a review of pipeline and back book cases where associated fraudulent parties are identified. • A firm has planned how counter-fraud resources could be increased in response to future growth in lending volumes, including consideration of the implications for training, recruitment and information technology. • A firm documents the criteria for initiating a fraud investigation. • Seeking consent from the Serious Organised Crime Agency (SOCA) to accept mortgage payments wherever fraud is identified.	• Fraud investigators lack relevant experience or knowledge of mortgage fraud issues, and have received insufficient training. • A firm's internal escalation procedures are unclear and leave staff confused about when and how to report their concerns about mortgage fraud.

Box 11.4: Managing relationships with ~~solicitor~~ conveyancers, brokers and valuers	
Examples of good practice:	**Examples of poor practice:**
• A firm has identified third parties they will not deal with, drawing on a range of internal and external information. • A third party reinstated to a panel after termination is subject to fresh due diligence checks. • A firm checks that ~~solicitor~~ conveyancers register charges over property with the Land Registry in good time, and chases this up. • Where a ~~solicitor~~ conveyancer is changed during the processing of an application, lenders contact both the original and new ~~solicitor~~ conveyancer to ensure the change is for a legitimate reason. • A firm checks whether third parties maintain	• A firm's scrutiny of third parties is a one-off exercise; membership of a panel is not subject to ongoing review. • A firm's panels are too large to be manageable. No work is undertaken to identify dormant third parties. • A firm solely relies on the FSA Register to check mortgage brokers, while scrutiny of ~~solicitor~~ conveyancers only involves a check of public material from the Law Society or Solicitors Regulation Authority. • A firm that uses divisional sales managers to oversee brokers has not considered how to manage conflicts of interest that may arise.

professional indemnity cover. • A firm has a risk-sensitive process for subjecting property valuations to independent checks. • A firm can detect brokers 'gaming' their systems, for example by submitting applications designed to discover the firm's lending thresholds, or submitting multiple similar applications known to be within the firm's lending policy. • A firm verifies that funds are dispersed in line with instructions held, particularly where changes to the Certificate of Title occur just before completion.	

Box 11.5: Compliance and internal audit	
Examples of good practice: • A firm has subjected anti-fraud measures to 'end-to-end' scrutiny, to assess whether defences are coordinated, rather than solely reviewing adherence to specific procedures in isolation. • There is a degree of specialist anti-fraud expertise within the compliance and internal audit functions.	**Examples of poor practice:** • A firm's management of third party relationships is subject to only cursory oversight by compliance and internal audit. • Compliance and internal audit staff demonstrate a weak understanding of mortgage fraud risks, because of inexperience or deficient training.

Box 11.6: Staff recruitment and vetting	
Examples of good practice: • A firm requires staff to disclose conflicts of interest stemming from their relationships with third parties such as brokers or ~~solicitor~~conveyancers. • A firm has considered what enhanced vetting methods should be applied to different roles (e.g. credit checks, criminal record checks, CIFAS staff fraud database, etc). • A firm adopts a risk-sensitive approach to managing adverse information about an employee or new candidate.	**Examples of poor practice:** • A firm uses recruitment agencies without understanding the checks they perform on candidates, and without checking whether they continue to meet agreed recruitment standards. • Staff vetting is a one-off exercise. • Enhanced vetting techniques are applied only to staff in Approved Persons positions. • A firm's vetting of temporary or contract staff is less thorough than checks on

Box 11.6: Staff recruitment and vetting	
Examples of good practice: • A firm seeks to identify when a deterioration in employees' financial circumstances may indicate increased vulnerability to becoming involved in fraud.	**Examples of poor practice:** permanent staff in similar roles.

Box 11.7: Remuneration structures	
Examples of good practice: • A firm has considered whether remuneration structures could incentivise behaviour that may increase the risk of mortgage fraud. • A firm's bonuses related to mortgage sales will take account of subsequent fraud losses, whether through an element of deferral or by 'clawback' arrangements.	**Examples of poor practice:** • The variable element of a firm's remuneration of mortgage salespeople is solely driven by the volume of sales they achieve, with no adjustment for sales quality or other qualitative factors related to compliance. • The variable element of salespeople's remuneration is excessive. • Staff members' objectives fail to reflect any consideration of mortgage fraud prevention.

Box 11.8: Staff training and awareness	
Examples of good practice: • A firm's financial crime training delivers clear messages about mortgage fraud across the organisation, with tailored training for staff closest to the issues. • A firm verifies that staff understand training materials, perhaps with a test. • Training is updated to reflect new mortgage fraud trends and types. • Mortgage fraud 'champions' offer guidance or mentoring to staff.	**Examples of poor practice:** • A firm fails to provide adequate training on mortgage fraud, particularly to staff in higher-risk business areas. • A firm relies on staff reading up on the topic of mortgage fraud on their own initiative, without providing formal training support. • A firm fails to ensure mortgage lending policies and procedures are readily accessible to staff. • A firm fails to define mortgage fraud in training documents or policies and procedures. • Training fails to ensure all staff are aware of their responsibilities to report

Box 11.8: Staff training and awareness	
Examples of good practice:	**Examples of poor practice:** suspicions, and the channels they should use.

12 Banks' management of high money-laundering risk situations (2011)

Who should read this chapter? This chapter is relevant, and its statements of good and poor practice apply, to **banks** we supervise under the Money Laundering Regulations 2007**.** Boxes 12.1 – 12.4 also apply to other **firms** we supervise under the Money Laundering Regulations **that have customers who present a high money-laundering risk**. It may be of interest to other firms we supervise under the Money Laundering Regulations 2007.

Content: This chapter contains sections on:

12.1 In June 2011 we published the findings of our thematic review of how banks operating in the UK were managing money-laundering risk in higher-risk situations. We focused in particular on correspondent banking relationships, wire transfer payments and high-risk customers including politically exposed persons (PEPs). We conducted 35 visits to 27 banking groups in the UK that had significant international activity exposing them to the AML risks on which we were focusing.

12.2 Our review found no major weaknesses in banks' compliance with the legislation relating to wire transfers. On correspondent banking, there was a wide variance in standards with some banks carrying out good quality AML work, while others, particularly among the smaller banks in our sample, carried out either inadequate due diligence or none at all.

12.3 However, our main conclusion was that around three-quarters of banks in our sample, including the majority of major banks, were not always managing high-risk customers and PEP relationships effectively and had to do more to ensure they were not used for money laundering purposes. We identified serious weaknesses in banks' systems and controls, as well as indications that some banks were willing to enter into very high-risk

business relationships without adequate controls when there were potentially large profits to be made. This meant that we found it likely that some banks were handling the proceeds of corruption or other financial crime.

12.4 The contents of this report are reflected in Chapter 2 (Financial crime systems and controls) and Chapter 3 (Money laundering and terrorist financing) of Part 1 of this Guide.

Our findings

12.5 You can read the findings of the FSA's thematic review here:

www.fsa.gov.uk/pubs/other/aml_final_report.pdf

Consolidated examples of good and poor practice

12.6 In addition to the examples of good and poor practice below, Section 6 of the report also included **case studies** illustrating relationships into which banks had entered which caused us particular concern. The case studies can be accessed via the link in the paragraph above.

Box 12.1: High risk customers and PEPs - AML policies and procedures

Examples of good practice:	**Examples of poor practice:**
• Senior management take money laundering risk seriously and understand what the Money Laundering Regulations are trying to achieve. • Keeping AML policies and procedures up to date to ensure compliance with evolving legal and regulatory obligations. • A clearly articulated definition of a PEP (and any relevant sub-categories) which is well understood by relevant staff. • Considering the risk posed by former PEPs and 'domestic PEPs' on a case-by-case basis. • Ensuring adequate due diligence has been carried out on all customers, even if they have been referred by somebody who is powerful or influential or a senior manager. • Providing good quality training to relevant staff on the risks posed by higher risk customers including PEPs and correspondent banks.	• A lack of commitment to AML risk management among senior management and key AML staff. • Failing to conduct quality assurance work to ensure AML policies and procedures are fit for purpose and working in practice. • Informal, undocumented processes for identifying, classifying and declassifying customers as PEPs. • Failing to carry out enhanced due diligence on customers with political connections who, although they do not meet the legal definition of a PEP, still represent a high risk of money laundering. • Giving waivers from AML policies without good reason. • Considering the reputational risk rather than the AML risk presented by customers. • Using group policies which do not

Box 12.1: High risk customers and PEPs - AML policies and procedures	
Examples of good practice:	**Examples of poor practice:**
• Ensuring RMs[15] and other relevant staff understand how to manage high money laundering risk customers by training them on practical examples of risk and how to mitigate it. • Keeping training material comprehensive and up-to-date, and repeating training where necessary to ensure relevant staff are aware of changes to policy and emerging risks.	comply fully with UK AML legislation and regulatory requirements. • Using consultants to draw up policies which are then not implemented. • Failing to allocate adequate resources to AML. • Failing to provide training to relevant staff on how to comply with AML policies and procedures for managing high-risk customers. • Failing to ensure policies and procedures are easily accessible to staff.

Box 12.2: High risk customers and PEPs - Risk assessment	
Examples of good practice:	**Examples of poor practice:**
• Using robust risk assessment systems and controls appropriate to the nature, scale and complexities of the bank's business. • Considering the money-laundering risk presented by customers, taking into account a variety of factors including, but not limited to, company structures; political connections; country risk; the customer's reputation; source of wealth/funds; expected account activity; sector risk; and involvement in public contracts. • Risk assessment policies which reflect the bank's risk assessment procedures and risk appetite. • Clear understanding and awareness of risk assessment policies, procedures, systems and controls among relevant staff. • Quality assurance work to ensure risk assessment policies, procedures, systems	• Allocating higher risk countries with low risk scores to avoid having to conduct EDD. • MLROs who are too stretched or under resourced to carry out their function appropriately. • Failing to risk assess customers until shortly before an FSA visit. • Allowing RMs to override customer risk scores without sufficient evidence to support their decision. • Inappropriate customer classification systems which make it almost impossible for a customer to be classified as high risk.

[15] Relationship Managers

Box 12.2: High risk customers and PEPs - Risk assessment	
Examples of good practice: and controls are working effectively in practice. • Appropriately-weighted scores for risk factors which feed in to the overall customer risk assessment. • A clear audit trail to show why customers are rated as high, medium or low risk.	**Examples of poor practice:**

Box 12.3: High risk customers and PEPs - Customer take-on	
Examples of good practice: • Ensuring files contain a customer overview covering risk assessment, documentation, verification, expected account activity, profile of customer or business relationship and ultimate beneficial owner. • ~~Having all new PEP or other high-risk relationships checked by the MLRO or the AML team.~~ The MLRO (and their team) have adequate oversight of all high-risk relationships. • Clear processes for escalating the approval of high risk and all PEP customer relationships to senior management or committees which consider AML risk and give appropriate challenge to RMs and the business. • Using, where available, local knowledge and open source internet checks to supplement commercially available databases when researching potential high risk customers including PEPs. • Having clear risk-based policies and procedures setting out the EDD required for higher risk and PEP customers, particularly in relation to source of wealth. • Effective challenge of RMs and business units by banks' AML and compliance	**Examples of poor practice:** • Failing to give due consideration to certain political connections which fall outside the Money Laundering Regulations definition of a PEP (eg wider family) which might mean that certain customers still need to be treated as high risk and subject to enhanced due diligence. • Poor quality, incomplete or inconsistent CDD. • Relying on Group introductions where overseas standards are not UK-equivalent or where CDD is inaccessible due to legal constraints. • Inadequate analysis and challenge of information found in documents gathered for CDD purposes. • Lacking evidence of formal sign-off and approval by senior management of high-risk and PEP customers and failure to document appropriately why the customer was within AML risk appetite. • Failing to record adequately face-to-face meetings that form part of CDD. • Failing to carry out EDD for high risk/PEP customers. • Failing to conduct adequate CDD before

Box 12.3: High risk customers and PEPs - Customer take-on	
Examples of good practice:	**Examples of poor practice:**
teams, and senior management. • Reward structures for RMs which take into account good AML/compliance practice rather than simply the amount of profit generated. • Clearly establishing and documenting PEP and other high-risk customers' source of wealth. • Where money laundering risk is very high, supplementing CDD with independent intelligence reports and fully exploring and reviewing any credible allegations of criminal conduct by the customer. • Understanding and documenting ~~ownership structures~~ complex or opaque ownership and corporate structures and the reasons for them. • Face-to-face meetings and discussions with high-risk and PEP prospects before accepting them as a customer. • Making clear judgements on money-laundering risk which are not compromised by the potential profitability of new or existing relationships. • Recognising and mitigating the risk arising from RMs becoming too close to customers and conflicts of interest arising from RMs' remuneration structures.	customer relationships are approved. • Over-reliance on undocumented 'staff knowledge' during the CDD process. • Granting waivers from establishing a customer's source of funds, source of wealth and other CDD without good reason. • Discouraging business units from carrying out adequate CDD, for example by charging them for intelligence reports. • Failing to carry out CDD on customers because they were referred by senior managers. • Failing to ensure CDD for high-risk and PEP customers is kept up-to-date in line with current standards. • Allowing 'cultural difficulties' to get in the way of proper questioning to establish required CDD records. • Holding information about customers of their UK operations in foreign countries with banking secrecy laws if, as a result the firm's ability to access or share CDD is restricted. • Allowing accounts to be used for purposes inconsistent with the expected activity on the account (e.g. personal accounts being used for business) without enquiry. • Insufficient information on source of wealth with little or no evidence to verify that the wealth is not linked to crime or corruption. • Failing to distinguish between source of funds and source of wealth. • Relying exclusively on commercially-available PEP databases and failure to make use of available open source

Box 12.3: High risk customers and PEPs - Customer take-on	
Examples of good practice:	**Examples of poor practice:** information on a risk-based approach. • Failing to understand the reasons for complex and opaque offshore company structures. • Failing to ensure papers considered by approval committees present a balanced view of money laundering risk. • No formal procedure for escalating prospective customers to committees and senior management on a risk based approach. • Failing to take account of credible allegations of criminal activity from reputable sources. • Concluding that adverse allegations against customers can be disregarded simply because they hold an investment visa. • Accepting regulatory and/or reputational risk where there is a high risk of money laundering.

Box 12.4: High risk customers and PEPs - Enhanced monitoring of high risk relationships	
Examples of good practice: • Transaction monitoring which takes account of up-to-date CDD information including expected activity, source of wealth and source of funds. • Regularly reviewing PEP relationships at a senior level based on a full and balanced assessment of the source of wealth of the PEP. • Monitoring new clients more closely to confirm or amend the expected account activity. • A risk-based framework for assessing the	**Examples of poor practice:** • Failing to carry out regular reviews of high-risk and PEP customers in order to update CDD. • Reviews carried out by RMs with no independent assessment by money laundering or compliance professionals of the quality or validity of the review. • Failing to disclose suspicious transactions to SOCA. • Failing to seek consent from SOCA on suspicious transactions before processing them.

Box 12.4: High risk customers and PEPs - Enhanced monitoring of high risk relationships	
Examples of good practice:	**Examples of poor practice:**
necessary frequency of relationship reviews and the degree of scrutiny required for transaction monitoring. • Proactively following up gaps in, and updating, CDD during the course of a relationship. • Ensuring transaction monitoring systems are properly calibrated to identify higher risk transactions and reduce false positives. • Keeping good records and a clear audit trail of internal suspicion reports sent to the MLRO, whether or not they are finally disclosed to SOCA. • A good knowledge among key AML staff of a bank's highest risk/PEP customers. • More senior involvement in resolving alerts raised for transactions on higher risk or PEP customer accounts, including ensuring adequate explanation and, where necessary, corroboration of unusual transactions from RMs and/or customers. • Global consistency when deciding whether to keep or exit relationships with high-risk customers and PEPs. • Assessing RMs' performance on ongoing monitoring and feeding this into their annual performance assessment and pay review. • Lower transaction monitoring alert thresholds for higher risk customers.	• Unwarranted delay between identifying suspicious transactions and disclosure to SOCA. • Treating annual reviews as a tick-box exercise and copying information from the previous review. • Annual reviews which fail to assess AML risk and instead focus on business issues such as sales or debt repayment. • Failing to apply enhanced ongoing monitoring techniques to high-risk clients and PEPs. • Failing to update CDD based on actual transactional experience. • Allowing junior or inexperienced staff to play a key role in ongoing monitoring of high-risk and PEP customers. • Failing to apply sufficient challenge to explanations from RMs and customers about unusual transactions. • RMs failing to provide timely responses to alerts raised on transaction monitoring systems.

Box 12.5: - Correspondent banking - Risk assessment of respondent banks	
Examples of good practice:	**Examples of poor practice:**
• Regular~~ly~~ assessments of correspondent banking risks taking into account various money laundering risk factors such as the	• Failing to consider the money-laundering risks of correspondent relationships.

Box 12.5: - Correspondent banking - Risk assessment of respondent banks	
Examples of good practice:	**Examples of poor practice:**
country (and its AML regime); ownership/management structure (including the possible impact/influence that ultimate beneficial owners with political connections may have); products/operations; transaction volumes; market segments; the quality of the respondent's AML systems and controls and any adverse information known about the respondent. • More robust monitoring of respondents identified as presenting a higher risk. • Risk scores that drive the frequency of relationship reviews. • Taking into consideration publicly available information from national government bodies and non-governmental organisations and other credible sources.	• Inadequate or no documented policies and procedures setting out how to deal with respondents. • Applying a 'one size fits all' approach to due diligence with no assessment of the risks of doing business with respondents located in higher risk countries. • Failing to prioritise higher risk customers and transactions for review. • Failing to take into account high-risk business types such as money service businesses and offshore banks.

Box 12.6: Correspondent banking - Customer take-on	
Examples of good practice:	**Examples of poor practice:**
• Assigning clear responsibility for the CDD process and the gathering of relevant documentation. • EDD for respondents that present greater risks or where there is less publicly available information about the respondent. • Gathering enough information to understand client details; ownership and management; products and offerings; transaction volumes and values; client market segments; client reputation; as well as the AML control environment. • Screening the names of senior managers, owners and controllers of respondent banks to identify PEPs and assessing the risk that identified PEPs pose.	• Inadequate CDD on parent banks and/or group affiliates, particularly if the respondent is based in a high-risk jurisdiction. • Collecting CDD information but failing to assess the risks. • Over-relying on the Wolfsberg Group AML questionnaire. • Failing to follow up on outstanding information that has been requested during the CDD process. • Failing to follow up on issues identified during the CDD process. • Relying on parent banks to conduct CDD for a correspondent account and taking no

Box 12.6: Correspondent banking - Customer take-on	
Examples of good practice: • Independent quality assurance work to ensure that CDD standards are up to required standards consistently across the bank. • Discussing with overseas regulators and other relevant bodies about the AML regime in a respondent's home country. • Identifying risk in particular business areas (eg informal value transfer such as 'hawala', tax evasion, corruption) through discussions with overseas regulators. • Visiting, or otherwise liaising~~discuss~~ with, respondent banks to discuss AML issues and gather CDD information. • Gathering information about procedures at respondent firms for sanctions screening and identifying/managing PEPs. • Understanding respondents' processes for monitoring account activity and reporting suspicious activity. • Requesting details of how respondents manage their own correspondent banking relationships. • Senior management/senior committee sign-off for new correspondent banking relationships and reviews of existing ones.	**Examples of poor practice:** steps to ensure this has been done. • Collecting AML policies etc but making no effort to assess them. • Having no information on file for expected activity volumes and values. • Failing to consider adverse information about the respondent or individuals connected with it. • No senior management involvement in the approval process for new correspondent bank relationships or existing relationships being reviewed.

Box 12.7: Correspondent banking - Ongoing monitoring of respondent accounts	
Examples of good practice: • Review periods driven by the risk rating of a particular relationship; with high risk relationships reviewed more frequently. • Obtaining an updated picture of ~~for~~ the purpose of the account and expected	**Examples of poor practice:** • Copying periodic review forms year after year without challenge from senior management. • Failing to take account of any changes to key staff at respondent banks.

Box 12.7: Correspondent banking - Ongoing monitoring of respondent accounts	
Examples of good practice:	**Examples of poor practice:**
activity. • Updating screening of respondents and connected individuals to identify individuals/entities with PEP connections or on relevant sanctions lists. • Involving senior management and AML staff in reviews of respondent relationships and consideration of whether to maintain or exit high-risk relationships. • Where appropriate, using intelligence reports to help decide whether to maintain or exit a relationship. • Carrying out ad-hoc reviews in light of material changes to the risk profile of a customer.	• Carrying out annual reviews of respondent relationships but failing to consider money-laundering risk adequately. • Failing to assess new information gathered during ongoing monitoring of a relationship. • Failing to consider money laundering alerts generated since the last review. • Relying on parent banks to carry out monitoring of respondents without understanding what monitoring has been done or what the monitoring found. • Failing to take action when respondents do not provide satisfactory answers to reasonable questions regarding activity on their account. • Focusing too much on reputational or business issues when deciding whether to exit relationships with respondents which give rise to high money-laundering risk.

Box 12.8: Wire transfers - Paying banks	
Examples of good practice:	**Examples of poor practice:**
• Banks' core banking systems ensure that all static data (name, address, account number) held on the ordering customer are automatically inserted in the correct lines of the outgoing MT103 payment instruction and any matching MT202COV.	• Paying banks take insufficient steps to ensure that all outgoing MT103s contain sufficient beneficiary information to mitigate the risk of customer funds being incorrectly blocked, delayed or rejected.

Box 12.9: Wire transfers - Intermediary banks	
Examples of good practice:	**Examples of poor practice:**
• Where practical, intermediary and beneficiary banks delay processing payments until they receive complete and meaningful information on the ordering	• Banks have no procedures in place to detect incoming payments containing meaningless or inadequate payer information, which could allow payments in breach of sanctions to slip through

Box 12.9: Wire transfers - Intermediary banks	
Examples of good practice: customer. • Intermediary and beneficiary banks have systems that generate an automatic investigation every time a MT103 appears to contain inadequate payer information. • Following processing, risk-based sampling for inward payments identifies~~y~~ inadequate payer information. • Search for phrases in payment messages such as 'one of our clients' or 'our valued customer' in all the main languages which may indicate a bank or customer trying to conceal their identity.	**Examples of poor practice:** unnoticed.

Box 12.10: Wire transfers - Beneficiary banks	
Examples of good practice: • Establishing a specialist team to undertake risk-based sampling of incoming customer payments, with subsequent detailed analysis to identify banks initiating cross-border payments containing inadequate or meaningless payer information. • Actively engaging in dialogue with peers about the difficult issue of taking appropriate action against persistently offending banks.	**Examples of poor practice:** • Insufficient processes to identify payments with incomplete or meaningless payer information.

Box 12.11: Wire transfers - Implementation of SWIFT MT202COV	
Examples of good practice: • Reviewing all correspondent banks' use of the MT202 and MT202COV. • Introducing the MT202COV as an additional element of the CDD review process including whether the local regulator expects proper use of the new message type.	**Examples of poor practice:** • Continuing to use the MT202 for all bank-to-bank payments, even if the payment is cover for an underlying customer transaction.

Box 12.11: Wire transfers - Implementation of SWIFT MT202COV	
Examples of good practice: • Always sending an MT103 and matching MT202COV wherever the sending bank has a correspondent relationship and is not in a position to 'self clear' (eg for Euro payments within a scheme of which the bank is a member). • Searching relevant fields in MT202 messages for the word 'cover' to detect when the MT202COV is not being used as it should be.	**Examples of poor practice:**

Annex B

Amendments to the Glossary of definitions

Insert the following new definition in the appropriate alphabetical position.

FC	Financial crime: a guide for firms

Annex C

Amendments to the Senior Management Arrangements, Systems and Controls sourcebook (SYSC)

In this Annex, underlining indicates new text.

Financial crime guidance

3.2.6K G The *FSA* provides *guidance* on steps that a *firm* can take to reduce the risk that it might be used to further *financial crime* in *FC* (Financial crime: a guide for firms).

…

6.1.1A G The *FSA* provides *guidance* on steps that a *firm* can take to reduce the risk that it might be used to further *financial crime* in *FC* (Financial crime: a guide for firms).

…

Financial crime guidance

6.3.11 G The *FSA* provides *guidance* on steps that a *firm* can take to reduce the risk that it might be used to further *financial crime* in *FC* (Financial crime: a guide for firms).