Guidance consultation GC18/1

Proposed guidance on financial crime systems and controls: insider dealing and market manipulation

March 2018

1 Summary

Introduction

1.1 The financial crime guide for firms[1] (the Guide) consolidates our guidance on financial crime and aims to enhance firms' understanding of our expectations of systems and controls in this area. The Guide provides practical assistance and information for firms of all sizes on actions they can take to counter the risk that they might be used to further financial crime.

1.2 We keep the Guide under periodic review to make sure that it accurately reflects our findings and covers emerging risks and concerns. It is designed to help firms adopt a more effective, risk-based and outcomes-focussed approach to mitigating financial crime risk.

1.3 The material in the Guide does not form part of the Handbook, but it does contain guidance on Handbook rules and principles, in particular:

[1] www.handbook.fca.org.uk/handbook/FC/link/PDF.html. Part 1 and 2 of the Guide are referred to collectively in this paper.

- 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
- Principle 1 (integrity), Principle 2 (skill, care and diligence), Principle 3 (management and control) and Principle 11 (relations with regulators) of our Principles for Businesses, set out in PRIN 2.1.1R
- the Statements of Principle for Approved Persons set out in APER 2.1.2P
- the rules in SYSC 3.2.6AR to SYSC 3.2.6JG and SYSC 6.3 in relation to guidance on money laundering

1.4 We are proposing to update the Guide with an additional chapter on insider dealing and market manipulation. The new chapter will outline our observations of good and bad market practice around the requirement to detect, report and counter the risk of financial crime, as it relates to insider dealing and market manipulation.

1.5 We are also proposing minor amendments to other parts of the Guide to reflect recent regulatory changes and ensure the Guide remains up to date.

1.6 We are also proposing a complete renumbering of the Guide to facilitate its presentation in the online Handbook in a way which will make it more accessible and searchable than at present. References to specific provisions within the Guide below follow the numbering as it stands.

1.7 All the proposed changes can be found in the draft instrument in Appendix 1, including our proposed new chapter on insider dealing and market manipulation (Chapter 8).

Who does this guidance affect?

1.8 This guidance will be of interest to firms who are subject to the financial crime rules in SYSC 6.1.1R and who arrange or execute transactions in financial markets.

1.9 We have to consult on changes to guidance in the Guide because it forms 'guidance on rules' under section 139A of the Financial Services and Markets Act 2000 (FSMA). This guidance is not binding and we will not presume that a firm's departure from our guidance constitutes a breach of our rules. We do, however, expect firms to take note of what our guidance says and, where appropriate, use it to inform their own financial crime systems and controls.

Insider dealing and market manipulation

1.10 Insider dealing is a criminal offence under section 52 of the Criminal Justice Act 1993. Sections 89-91 of the Financial Services Act 2012 set out a range of behaviours which

amount to criminal offences, which are together referred to in the Guide as market manipulation.

1.11 Financial crime is defined as any offence involving fraud or dishonesty, misconduct in a financial market, or handling the proceeds of crime[2]. Insider dealing and market manipulation are both financial crimes.

1.12 Insider dealing or market manipulation can be committed by a firm as well as an individual. To commit insider dealing, as well as certain forms of market manipulation, the perpetrator must engage in the financial markets. It is critical that FCA authorised firms, which offer access to financial markets, or who engage in the financial markets themselves have adequate policies and procedures to counter the risk that the firm might be used to further financial crime, in accordance with SYSC 6.1.1R.

1.13 On 3 July 2016, the EU Market Abuse Regulation (No 596/2014) (MAR) came into force. MAR sets out the civil offences of market abuse. MAR also includes specific requirements on any person professionally arranging or executing transactions to establish and maintain effective arrangements, systems and procedures to detect and report suspicious orders and transactions under Article 16(2).

1.14 There is a key distinction between the obligations under Article 16(2) of MAR and the requirements in SYSC 6.1.1R. Article 16(2) of MAR requires firms to detect and report potential market abuse, whereas SYSC 6.1.1R extends firms' obligations to **counter** the risk of financial crime.

1.15 Firms subject to SYSC 6.1.1R should be aware that their obligation to counter financial crime risk extends to insider dealing and market manipulation, including considering what arrangements are in place to counter such activity.

1.16 Like any other financial crime, insider dealing and market manipulation are both predicate offences to money laundering. Therefore, firms will need to be aware of their obligations under the Proceeds of Crime Act 2002 (POCA), including the submission of Suspicious Activity Reports (SAR) to the National Crime Agency and the offence of 'tipping off' – see Annex 1 to Part 1 of the Guide for a description of tipping off.

1.17 While firms need to consider these obligations under POCA, we note that the submission of a SAR doesn't stop the firm from taking proactive steps to counter the risk of financial crime being committed through the firm, including communicating with customers about the business relationship.

Summary of proposals

1.18 We are proposing to add a chapter to Part 1 of the Guide to cover insider dealing and market manipulation. The new chapter will outline our observations of good and bad

[2] Financial Services and Markets Act 2000 (as amended)

market practice around the requirement to detect, report and counter the risk of financial crime, as it relates to insider dealing and market manipulation.

1.19 We are also proposing minor amendments to other chapters of the Guide to reflect recent regulatory changes and ensure the Guide remains up to date. These are mainly to reflect the introduction of the Money Laundering Regulations 2017 in June but also to remove outdated references in relation to the way we refer to Sanctions in Chapter 7.

1.20 The proposed changes are outlined in Appendix 1 of this guidance consultation.

1.21 It is proposed that this guidance will come into effect on 1 October 2018.

How to respond

1.22 Please comment on our draft guidance by close of business on 28 June 2018.

1.23 Respond by email to gc18-01@fca.org.uk or by post to:

Mark Edwards
Financial Conduct Authority
25 The North Colonnade
London E14 5HS

1.24 Responses to formal consultations are available for public inspection unless the respondent requests otherwise. We will not regard a standard confidentiality statement in an email message as a request for non-disclosure.

1.25 Despite this, we may be asked to disclose a confidential response under the Freedom of Information Act 2000. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by the Information Commissioner and the Information Rights Tribunal.

Equality and diversity considerations

1.26 We have considered the equality and diversity issues that may arise from this guidance. We do not consider that this guidance will adversely impact any of the groups with protected characteristics, ie age, disability, sex, marriage or civil partnership, pregnancy and maternity, race, religion and belief, sexual orientation and gender reassignment.

1.27 We will continue to consider the equality and diversity implications of this guidance during the consultation period, and will revisit them when publishing the final guidance. In the interim we welcome any feedback to this guidance consultation on such matters.

Cost benefit analysis

1.28 FSMA does not require the FCA to carry out a cost benefit analysis on guidance.

Compatibility statement

1.29 Section 1B of FSMA requires the FCA to carry out its general functions, as far as is reasonably possible, in a way that is compatible with its strategic objective and advances one or more of its operational objectives. The FCA also needs to, so as far as is compatible with acting in a way that advances the consumer protection objective or the integrity objective, carry out its general functions in a way that promotes effective competition in the interests of consumers.

1.30 We are satisfied that these proposals are compatible with our general duties under section 1B of FSMA, in particular having regard to the matters set out in 1C(2) FSMA and the regulatory principles in section 3B. We think that:

- it will help us to use our resources in an efficient and economical way
- the expectations contained within it are proportionate to the benefits
- it recognises differences in the nature of and the objectives of businesses carried on by different persons
- it supports the principle that the regulators should exercise their functions as transparently as possible

Appendix 1

FINANCIAL CRIME GUIDE (INSIDER DEALING AND REDESIGNATION) INSTRUMENT 2018

FINANCIAL CRIME GUIDE (INSIDER DEALING AND REDESIGNATION) INSTRUMENT 2018

Power exercised

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

(1) section 139A (Guidance) of the Financial Services and Markets Act 2000;
(2) regulation 120(1) (Guidance) of the Payment Services Regulations 2017; and
(3) regulation 60(1) (Guidance) of the Electronic Money Regulations 2011.

Commencement

B. This instrument comes into force on [*date*].

Renaming of the Financial Crime Guide (FC)

C. The Financial Crime Guide Part 1: A firm's guide to preventing financial crime is renamed as the Financial Crime Guide: A firm's guide to preventing crime (FCG).

D. The Financial Crime Guide Part 2: Financial crime thematic reviews is renamed as the Financial Crime Thematic Reviews (FCTR).

Amendments to the Handbook

E. The Glossary of definitions is amended in accordance with Annex A to this instrument.

Amendments to material outside the Handbook

F. The Financial Crime Guide: A firm's guide to preventing crime (FCG) is amended in accordance with Annex B to this instrument.

G. The Financial Crime Thematic Reviews (FCTR) is amended in accordance with Annex C to this instrument.

Citation

H. This instrument may be cited as the Financial Crime Guide (Insider Dealing and Redesignation) Instrument 2018.

By order of the Policy Development Committee of the Financial Conduct Authority
[*date*]

Annex A

Amendments to the Glossary of definitions

Insert the following new definitions in the appropriate alphabetical position. The text is not underlined.

FCG	the Financial Crime Guide: A firm's guide to preventing crime.
FCTR	the Financial Crime Thematic Reviews.

Annex B

Amendments to the Financial Crime Guide: A firm's guide to preventing crime (*FCG*)

In this Annex, the provisions and subheadings of *FCG* listed in column (1) are renumbered and revised as set out in Column (2) of the following tables. Cross-references throughout FCG are amended accordingly. For example, where a box now appears as a standard paragraph, all references to that 'box' now refer to a 'paragraph'. Similarly, where a box now appears as a list, all references to that 'box' now refer to a 'list'.

Old heading and numbering	New heading and numbering
1. Introduction	1. Introduction
	1.1 What is the *FCG*?
1.1	1.1.1
1.2	1.1.2
1.3	1.1.3
1.4	1.1.4
1.5	1.1.5
1.6	1.1.6
1.7	1.1.7
1.8	1.1.8
1.9	1.1.9
1.10	1.1.10
1.11	1.1.11
How to use this Guide	1.2 How to use *FCG*
1.12	1.2.1
1.13	1.2.2
1.14	1.2.3
	1.3 Format of *FCG*
Box 1.1	1.3.1
Box 1.2	1.3.2
	1.4 Further financial crime information
1.15	1.4.1
2. Financial crime systems and controls	2. Financial crime systems and controls
	2.1 Introduction
	2.1.1
	2.1.2
2.1	2.1.3
	2.2 Themes
Box 2.1	2.2.1
Box 2.1A	2.2.2
Box 2.2	2.2.3
Box 2.3	2.2.4
Box 2.4	2.2.5
Box 2.5	2.2.6
Box 2.6	2.2.7

Old heading and numbering	New heading and numbering
	2.3 Further guidance
2.2	2.3.1
2.3	2.3.2
2.4	2.3.3
2.5	2.3.4
2.6	2.3.5
2.7	2.3.6
3. Money laundering and terrorist financing	3. Money laundering and terrorist financing
	3.1 Introduction
	3.1.1
	3.1.2
	3.1.3
	3.1.4
	3.1.5
3.1	3.1.6
3.2	3.1.7
	3.1.7A
3.3	3.1.8
	3.2 Themes
Box 3.1	3.2.1
Box 3.2	3.2.2
Box 3.3	3.2.3
Box 3.4	3.2.4
Box 3.5	3.2.5
Box 3.5A	3.2.6
Box 3.6	3.2.7
Box 3.7	3.2.8
Box 3.8	3.2.9
Box 3.9	3.2.10
Box 3.10	3.2.11
Box 3.11	3.2.12
Box 3.12	3.2.13
Box 3.13	3.2.14
Box 3.14	3.2.15
Box 3.15	3.2.16
Box 3.16	3.2.17
	3.3 Further guidance
3.4	3.3.1
	3.3.2
	3.4 Sources of further information
3.5	3.4.1
3.6	3.4.2
3.7	3.4.3
	3.4.4

Old heading and numbering	New heading and numbering
4. Fraud	4. Fraud
	4.1 Introduction
	4.1.1
4.1	4.1.2
4.2	4.1.3
	4.2 Themes
Box 4.1	4.2.1
Box 4.2	4.2.2
Box 4.3	4.2.3
Box 4.4	4.2.4
Box 4.5	4.2.5
	4.3 Further guidance
4.3	4.3.1
	4.3.2
	4.4 Sources of further information
4.4	4.4.1
	4.4.2
5. Data security	5. Data security
	5.1 Introduction
	5.1.1
5.1	5.1.2
	5.2 Themes
Box 5.1	5.2.1
Box 5.2	5.2.2
Box 5.3	5.2.3
Box 5.4	5.2.4
Box 5.5	5.2.5
	5.3 Further guidance
5.2	5.3.1
	5.4 Sources of further information
5.3	5.4.1
6. Bribery and corruption	6. Bribery and corruption
	6.1 Introduction
	6.1.1
6.1	6.1.2
6.2	6.1.3
	6.1.4
6.3	6.1.5
	6.2 Themes
Box 6.1	6.2.1
Box 6.2	6.2.2
Box 6.3	6.2.3
Box 6.4	6.2.4
Box 6.5	6.2.5

Old heading and numbering	New heading and numbering
Box 6.6	6.2.6
	6.3 Further guidance
6.4	6.3.1
	6.4 Sources of further information
6.5	6.4.1
7. Sanctions and asset freezes	7. Sanctions and asset freezes
	7.1 Introduction
	7.1.1
	7.1.2
	7.1.3
7.1	7.1.4
7.2	7.1.5
	7.1.5A
7.3	7.1.6
	7.2 Themes
Box 7.1	7.2.1
Box 7.2	7.2.2
Box 7.3	7.2.3
Box 7.4	7.2.4
Box 7.5	7.2.5
Box 7.6	7.2.6
	7.3 Further guidance
7.4	7.3.1
	7.4 Sources of further information
7.5	7.4.1
7.6	7.4.2

Amend the following as shown. Underlining indicates new text and striking through indicates deleted text.

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

1 Introduction

1.1 What is the *FCG*?

1.1.1 ~~*This Guide*~~*FCG* provides practical assistance and information for firms of all sizes and across all ~~FCA~~ *FCA*-supervised sectors on actions they can take to counter the risk that they might be used to further financial crime. Its contents are drawn primarily from ~~FCA~~ *FCA* and ~~FSA~~ *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.~~

1.1.2 Effective systems and controls can help firms to detect, prevent and deter financial

crime. ~~Part 1~~ *FCG* provides guidance on financial crime systems and controls, both generally and in relation to specific risks such as money laundering, bribery and corruption and fraud. Annexed to ~~Part 1~~ *FCG* is a list of common and useful terms. *FCG* Annex 1 is provided for reference purposes only and is not a list of 'defined terms'. ~~The Guide~~ *FCG* does not use the ~~Handbook~~ *Handbook* Glossary of definitions unless otherwise indicated.

1.1.3 ~~Part 2~~ *FCTR* provides summaries of, and links to, ~~FCA~~ *FCA* and~~FSA~~ *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.

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

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

- ~~SYSC~~ *SYSC* 3.2.6R and ~~SYSC~~ *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~~ *PRIN* 2.1.1R;
- the Statements of Principle for Approved Persons set out in ~~APER~~ *APER* 2.1A.3R and the conduct rules set out in ~~COCON~~ *COCON* 2.1 and 2.2; and
- in relation to guidance on money laundering, the rules in ~~SYSC~~ *SYSC* 3.2.6~~A~~R to ~~SYSC~~ *SYSC* 3.2.6~~J~~G IR and ~~SYSC~~ *SYSC* 6.3 (Financial crime).

Where ~~the Guide~~ *FCG* refers to guidance in relation to ~~SYSC~~ *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~~ 2017 and the Electronic Money Regulations 2011.

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

1.1.7 ~~The Guide~~ *FCG* contains 'general guidance' as defined in section ~~158~~ 139B of the Financial Services and Markets Act 2000 (FSMA). The guidance is not binding and we will not presume that a firm's departure from our guidance indicates that it has breached our rules.

1.1.8 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~~ *FCG*. But we expect firms to be aware of what we say where it applies to them and to consider applicable guidance when establishing, implementing and maintaining

their anti-financial crime systems and controls. More information about ~~FCA~~ *FCA* guidance and its status can be found in our Reader's Guide: an introduction to the ~~Handbook~~ *Handbook*~~, p.24~~; paragraph 6.2.1G(4) of the Decision Procedures and Penalties (DEPP) manual of the ~~Handbook~~ *Handbook* and paragraphs 2.9.1G – 2.9.6G of our Enforcement Guide (EG).

1.1.9 ~~The Guide~~ *FCG* also contains guidance on how firms can meet the requirements of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations ~~2007~~ 2017 ('Money Laundering Regulations 2017') and the EU ~~Wire~~ Funds Transfer Regulation. This guidance is ~~not~~ 'relevant guidance' as described in Regulations ~~42(3)~~ 76(6) ~~or~~ and ~~45(2)~~ 86(2) of the Money Laundering Regulations 2017~~, or Regulation 14 of the Transfer of Funds (Information on the Payer) Regulations 2007 (which gives the FCA powers and responsibilities to supervise firms' compliance with the EU Wire Transfer Regulation)~~. This means that a decision maker ~~is not required to~~ under these regulations is required to consider whether a person followed the guidance the *FCG*, *FCTR* or other guidance issued by an appropriate body and approved by HM Treasury when it is deciding whether that person has ~~breached these regulations, although they may choose to do so~~ contravened a relevant requirement under these Regulations.

1.1.10 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~~ *EG* 12.1.2G and ~~EG 19.82~~ *EG* 19.15.5G, the ~~FCA~~ *FCA* will continue to have regard to whether firms have followed the relevant provisions of JMLSG's guidance when deciding whether conduct amounts to a breach of relevant requirements.

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

1.2 How to use *FCG*

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

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

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

- 'may' to describe examples of good practice that go beyond basic compliance.

1.2.3 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~~ *FCG* 2.2.1G (Governance) that senior management should actively engage in a firm's approach to addressing financial crime risk. The level of seniority and degree of engagement that is appropriate will differ based on a variety of factors, including the management structure of the firm and the seriousness of the risk.

- We ask in ~~Box~~ *FCG* 3.2.5G (Ongoing monitoring) how a firm monitors transactions to spot potential money laundering. While we expect that a global retail bank that carries out a large number of customer transactions would need to include automated systems in its processes if it is to monitor effectively, a small firm with low transaction volumes could do so manually.

- We say in ~~Box~~ *FCG* 4.2.1G (General – preventing losses from fraud) that it is good practice for firms to engage with relevant cross-industry efforts to combat fraud. A national retail bank is likely to have a greater exposure to fraud, and therefore to have more information to contribute to such efforts, than a small local building society, and we would expect this to be reflected in their levels of engagement.

1.3 Format of *FCG*

1.3.1 Financial crime: a guide for firms

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

Self-assessment questions:

- These questions will help you to consider whether your firm's approach is **appropriate**. (Text in brackets expands on this.)

- The ~~FCA~~ *FCA* may follow **similar lines of inquiry** when discussing financial crime issues with firms.

- The questions draw attention to some of the key points firms should consider when deciding how to address a financial crime issue or comply with a financial crime requirement.

Examples of good practice	Examples of poor practice
• This list provides **illustrative** examples of **good practices**.	• This list provides **illustrative** examples of **poor practices**.

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

1.3.2 Case studies and other information

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

1.4 Further financial crime information

1.4.1 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~~ *FCTR*.
- It also includes links to external websites and materials. Although the external links are included to assist readers of ~~the Guide~~ *FCG*, we are not responsible for the content of these, as we neither produce nor maintain them.

2 Financial crime systems and controls

2.1 Introduction

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

2.1.2 The Annex I **financial institutions** which we supervise for compliance with their obligations under the Money Laundering Regulations ~~2007~~ 2017 are not subject to the financial crime rules in ~~SYSC~~ *SYSC*. But the guidance in this chapter applies to

them as it can assist them to comply with their obligations under the Regulations.

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

2.2 Themes

2.2.1 Governance

We expect **senior management** to take **clear responsibility** for managing financial crime risks, which should be treated in the same manner as other risks faced by the business. There should be evidence that senior management are **actively engaged** in the firm's approach to addressing the risks.

Self-assessment questions:

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

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

issues.

2.2.2 Management information (MI)

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

Examples of financial crime MI include:

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

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

2.2.3 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

- Financial crime risks are addressed in a **coordinated** manner across the business and information is shared readily.
- Management responsible for financial crime are **sufficiently senior** as well as being credible, independent, and experienced.
- A firm has considered how counter-fraud and anti-money laundering efforts can **complement** each other.
- A firm has a strategy for self-improvement on financial crime.
- The firm bolsters insufficient in-house knowledge or resource with **external expertise**, for example in relation to assessing financial crime risk or monitoring compliance with standards.

Examples of poor practice

- The firm makes no effort to understand or address **gaps** in its financial crime defences.
- Financial crime officers are relatively **junior** and lack access to senior management. They are often **overruled** without documented justification.
- Financial crime departments are **under-resourced** and senior management are reluctant to address this.

2.2.4 Risk assessment

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

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

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

- be comprehensive and consider a wide range of factors – it is not normally enough to consider just one factor
- draw on a wide range of relevant information – it is not normally enough to consider just one source, and
- be proportionate to the nature, scale and complexity of the firm's activities.

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

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

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

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

Self-assessment questions:

- What are the main financial crime **risks** to the business?
- How does your firm seek to **understand** the financial crime risks it faces?
- When did the firm last **update** its **risk assessment**?
- How do you **identify new or emerging** financial crime risks?
- Is there evidence that risk is considered and recorded systematically, assessments are updated and **sign-off** is appropriate?
- Who **challenges** risk assessments and how? Is this process sufficiently

rigorous and well-documented?

- How do **procedures** on the ground adapt to emerging risks? (For example, how quickly are policy manuals updated and procedures amended?)

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

2.2.5 Policies and procedures

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

Self-assessment questions:

- How often are your firm's policies and procedures **reviewed**, and at what level of **seniority**?
- How does it **mitigate** the financial crime risks it identifies?
- What steps does the firm take to ensure that relevant policies and procedures **reflect new risks** or **external events**? How quickly are any necessary changes made?
- What steps does the firm take to ensure that staff **understand** its policies and procedures?
- For larger groups, how does your firm ensure that policies and procedures are **disseminated** and **applied** throughout the business?

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

See ~~SYSC~~ *SYSC* 3.2.6R and ~~SYSC~~ *SYSC* 6.1.1R.

2.2.6 Staff recruitment, vetting, training, awareness and remuneration

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

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

Self-assessment questions:

- What is your approach to **vetting** staff? Do vetting and management of different staff reflect the financial crime risks to which they are exposed?
- How does your firm ensure that its employees are aware of financial

crime risks and of their **obligations** in relation to those risks?

- Do staff have access to training on an **appropriate range** of financial crime risks?
- How does the firm ensure that training is of **consistent quality** and is **kept up to date**?
- Is training **tailored** to particular roles?
- How do you assess the **effectiveness** of your training on topics related to financial crime?
- Is training material relevant and up to date? When was it **last reviewed**?

Examples of good practice		Examples of poor practice	
•	Staff in higher risk roles are subject to **more thorough vetting**.	•	Staff are **not competent** to carry out preventative functions effectively, exposing the firm to financial crime risk.
•	**Temporary staff** in higher risk roles are subject to the same level of vetting as permanent members of staff in similar roles.	•	Staff vetting is a **one-off** exercise.
•	Where **employment agencies** are used, the firm periodically satisfies itself that the agency is adhering to the agreed vetting standard.	•	The firm fails to **identify changes** that could affect an individual's integrity and suitability.
•	**Tailored** training is in place to ensure staff knowledge is adequate and up to date.	•	The firm **limits enhanced vetting** to senior management roles and fails to vet staff whose roles expose them to higher financial crime risk.
•	New staff in **customer-facing** positions receive financial crime training tailored to their role before being able to interact with customers.	•	The firm fails to identify whether staff whose roles expose them to bribery and corruption risk have **links to relevant political or administrative decision-makers**.
•	Training has a strong **practical** dimension (e.g. case studies) and some form of testing.	•	Poor compliance records are not reflected in **staff appraisals and remuneration**.

•	The firm satisfies itself that staff **understand** their responsibilities (e.g. computerised training contains a test).	•	Training dwells unduly on **legislation and regulations** rather than practical examples.
•	**Whistleblowing** procedures are clear and accessible, and respect staff confidentiality.	•	Training material is **not kept up to date**.
		•	The firm **fails to identify** training needs.
		•	There are no **training logs** or tracking of employees' training history.
		•	Training **content** lacks management sign-off.
		•	Training does not cover **whistleblowing** and **escalation** procedures.

See ~~SYSC~~ *SYSC* 3.1.6R and ~~SYSC~~ *SYSC* 5.1.1R.

2.2.7 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.	•	Compliance unit and audit teams **lack experience** in financial crime matters.

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

2.3 Further guidance

2.3.1 ~~Part 2 of the Guide~~ *FCTR* contains the following additional guidance on **governance**:

- ~~Box 6.1~~*FCTR* 6.3.1G (Governance), from the ~~FSA~~ *FSA*'s thematic review Data security in Financial Services
- ~~Box 8.1~~*FCTR* 8.3.1G (Senior management responsibility) from the ~~FSA~~ *FSA*'s thematic review Financial services firms' approach to UK financial sanctions
- ~~Box 9.1~~*FCTR* 9.3.1G (Governance and management information) from the ~~FSA~~ *FSA*'s thematic review Anti-bribery and corruption in commercial insurance broking
- ~~Box 11.1~~*FCTR* 11.3.1G (Governance, culture and information sharing) from the ~~FSA~~ *FSA*'s thematic review Mortgage fraud against lenders

2.3.2 ~~Part 2 of the Guide~~ *FCTR* contains the following additional guidance on **risk assessment**:

- ~~Box 8.2~~ *FCTR* 8.3.2G (Risk assessment) from the ~~FSA~~ *FSA*'s thematic review Financial services firms' approach to UK financial sanctions
- ~~Box 9.2~~ *FCTR* 9.3.2G (Risk assessment and responses to significant bribery and corruption events) from the ~~FSA~~ *FSA*'s thematic review Anti-bribery and corruption in commercial insurance broking
- ~~Box 10.7~~*FCTR* 10.3.7G (Responsibilities and risk assessments) from the ~~FSA~~ *FSA*'s thematic review The Small Firms Financial Crime Review
- ~~Box 12.2~~*FCTR* 12.3.3G (High risk customers and PEPs – Risk assessment) and ~~Box 12.5~~ ~~*FCTR* 12.3.6G~~ (Correspondent banking – Risk assessment of respondent banks) from the ~~FSA~~ *FSA*'s thematic review Banks' management of high money laundering risk situations

2.3.3 ~~Part 2 of the Guide~~ *FCTR* contains the following additional guidance on **policies and procedures**:

- ~~Box 8.3~~ *FCTR* 8.3.3G (Policies and procedures) from the ~~FSA~~ *FSA's* thematic review Financial services firms' approach to UK financial sanctions
- ~~Box 10.1~~*FCTR* 10.3.1G (Regulatory/Legal obligations) from the ~~FSA~~ *FSA*'s thematic review The Small Firms Financial Crime Review
- Box 12.1*FCTR* 12.3.2G (High risk customers and PEPs – AML policies and procedures) from the ~~FSA~~ *FSA*'s thematic review Banks' management of high money laundering risk situations

2.3.4 ~~Part 2 of the Guide~~ *FCTR* contains the following additional guidance on **staff recruitment, vetting, training and awareness**:

- ~~Box 6.2~~*FCTR* 6.3.2G (Training and awareness) and *FCTR* 6.3.3G (Staff recruitment and vetting) from the ~~FSA~~ *FSA*'s thematic review Data security in Financial Services
- ~~Box 8.4~~*FCTR* 8.3.4G (Staff training and awareness) from the ~~FSA~~ *FSA*'s thematic review Financial services firms' approach to UK financial sanctions
- ~~Box 9.5~~ *FCTR* 9.3.5G (Staff recruitment and vetting) and *FCTR* 9.3.6G (Training and awareness) from the *FSA*'s thematic review Anti-bribery and corruption in commercial insurance broking
- ~~Box 10.6~~ *FCTR* 10.3.6G (Training) from the ~~FSA~~ *FSA*'s thematic review The Small Firms Financial Crime Review
- ~~Box 11.6~~ *FCTR* 11.3.6G (Staff recruitment and vetting) and ~~Box 11.8~~ *FCTR* 11.3.8G (Staff training and awareness) from the ~~FSA~~ *FSA*'s thematic review Mortgage fraud against lenders laundering risk situations

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

- ~~Box 6.15~~*FCTR* 6.3.15G (Internal audit and compliance monitoring) from the ~~FSA~~ *FSA*'s thematic review Data security in Financial Services
- ~~Box 9.9~~ *FCTR* 9.3.9G (The role of compliance and internal audit) from the ~~FSA~~ *FSA*'s thematic review Anti-bribery and corruption in commercial insurance broking
- ~~Box 11.6~~ *FCTR* 11.3.5G (Compliance and internal audit) from the ~~FSA~~ FSA's thematic review Mortgage fraud against lenders

2.3.6 For firms' obligations in relation to whistleblowers see the Public Interest

Disclosure Act 1998: www.legislation.gov.uk/ukpga/1998/23/contents

3 Money laundering and terrorist financing

3.1 Introduction

3.1.1 **Who should read this chapter?** This section applies to **all firms** who are subject to the money laundering provisions in ~~SYSC~~ *SYSC* 3.2.6A – J or ~~SYSC~~ *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~~ 2017** (referred to in this chapter as 'the ~~ML Regulations~~ Money Laundering Regulations 2017').

3.1.2 This guidance does not apply to **payment institutions**, which are supervised for compliance with the ~~ML Regulations~~ Money Laundering Regulations 2017 by HM Revenue and Customs. But it may be of interest to them, to the extent that we may refuse to authorise them, or remove their authorisation, if they do not satisfy us that they comply with the ~~ML Regulations~~ Money Laundering Regulations 2017.

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

3.1.4 ~~*Box 3.2*~~ *FCG* 3.2.2G (The Money Laundering Reporting Officer (MLRO)) applies only to firms who are subject to the money laundering provisions in ~~SYSC~~ *SYSC* 3.2.6A – J or ~~SYSC~~ *SYSC* 6.3, except it does not apply to **sole traders who have no employees**.

3.1.5 ~~Box 3.12~~*FCG* 3.2.13G (Customer payments) applies to banks subject to ~~SYSC~~ *SYSC* 6.3.

3.1.6 The guidance in this chapter relates both to our interpretation of requirements of the ~~ML Regulations~~ Money Laundering Regulations 2017 and to the financial crime and money laundering provisions of ~~SYSC~~ *SYSC* 3.2.6R – 3.2.6JG, ~~SYSC~~ *SYSC* 6.1.1R and ~~SYSC~~ *SYSC* 6.3.

3.1.7 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~~ *FCG* is not intended to replace, compete or conflict with the JMLSG's guidance, which should remain a key resource for firms.

3.1.7A The European Supervisory Authorities (ESAs) have produced guidelines that firms should consider when assessing the ML/TF risk associated with a business relationship or occasional transaction. The Money Laundering Regulations 2017 require firms to take account of these guidelines when meeting requirements in

Regulations 33 and 37.

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

3.2 Themes

3.2.1 Governance

The guidance in ~~Box 2.1~~ *FCG* 2.2.1G on governance in relation to financial crime also applies to money laundering. We expect senior management to take responsibility for the firm's anti-money laundering (AML) measures. This includes knowing about the money laundering risks to which the firm is exposed and ensuring that steps are taken to mitigate those risks effectively.

Self-assessment questions:

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

Examples of good practice		Examples of poor practice	
•	**Reward structures** take account of any failings related to AML compliance.	•	There is **little evidence** that AML is **taken seriously** by senior management. It is seen as a legal or **regulatory necessity** rather than a matter of true concern for the business.
•	Decisions on accepting or maintaining high money laundering risk relationships are reviewed and challenged **independently** of the business relationship and escalated to senior management or	•	Senior management attach greater importance to the risk that a customer might be involved in a **public scandal**, than to the risk that the customer might be corrupt or otherwise engaged in financial crime.

	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.	•	The board **never considers** MLRO reports.
•	A UK parent undertaking ensures that AML controls apply to all its branches and subsidiaries outside the UK.	•	A UK branch or subsidiary uses group policies which **do not comply** fully with UK AML legislation and regulatory requirements.

3.2.2 The Money Laundering Reporting Officer (MLRO)

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

Firms to which this section applies must appoint an individual as MLRO. The MLRO is responsible for oversight of the firm's compliance with its anti-money laundering obligations and should act as a focal point for the firm's AML activity.

Self-assessment questions:

- Does the MLRO have sufficient resources, experience, access and seniority to carry out their role effectively?
- Do the firm's staff, including its senior management, consult the MLRO on matters relating to money-laundering?
- Does the MLRO escalate relevant matters to senior management and, where appropriate, the board?
- What awareness and oversight does the MLRO have of the highest risk relationships?

Examples of good practice		Examples of poor practice	
•	The MLRO is independent, knowledgeable, robust and well-resourced, and poses effective challenge to the business where	•	The MLRO lacks credibility and authority, whether because of inexperience or lack of seniority.

	Warranted.		
•	The MLRO has a direct reporting line to executive management or the board.	•	The MLRO does not understand the policies they are supposed to oversee or the rationale behind them.
		•	The MLRO of a firm which is a member of a group has not considered whether group policy adequately addresses UK AML obligations.
		•	The MLRO is unable to retrieve information about the firm's high-risk customers on request and without delay and plays no role in monitoring such relationships.

See ~~SYSC~~ *SYSC* 3.2.6IR and ~~SYSC~~ *SYSC* 6.3.9R.

3.2.3 Risk assessment

The guidance in ~~Box 2.3~~ *FCG* 2.2.4G 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. A firm is required by Regulation 18 of the Money Laundering Regulations 2017 to undertake a risk assessment.

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.

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, transactions, 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.	•	An inappropriate risk classification system makes it almost impossible for a relationship to be classified as 'high risk'.
•	The firm has identified good sources of information on money laundering risks, such as National Risk Assessments, ESA Guidelines, FATF mutual evaluations and typology reports, NCA alerts, press reports, court judgements, reports by non-governmental organisations and commercial due diligence providers.	•	Higher risk countries are allocated low-risk scores to avoid enhanced due diligence measures.
•	Consideration of money laundering 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 assessments on money laundering are unduly influenced by the potential profitability of new or existing relationships.

	risk effectively.		
		•	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.

See ~~ML Regs 5,6 and 7 ML Reg 14 ML Reg 11~~ regulation 18 of the Money Laundering Regulations 2017, *SYSC* 3.2.6AR, *SYSC* 3.2.6CR, *SYSC* 6.3.1R and *SYSC* 6.3.3R.

3.2.4 Customer due diligence (CDD) checks

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.

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~~ *FCG* 3.2.8G below considers enhanced due diligence.

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

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.	•	Procedures are not **risk-based**: the firm applies the same CDD measures to products and customers of varying risk.
•	The firm can cater for **customers who lack common forms of ID** (such as the socially excluded, those in care, etc).	•	The firm has **no method for tracking** whether checks on customers are complete.
•	The firm understands and documents the **ownership and control structures** (including the reasons for any complex or opaque corporate structures) of customers and their beneficial owners.	•	The firm allows **language difficulties** or **customer objections** to get in the way of proper questioning to obtain necessary CDD information.
•	The firm obtains information about the purpose and nature of the business relationship sufficient to be satisfied that it **understands** the **associated money laundering risk**.	•	Staff do **less CDD** because a customer is referred by senior executives or influential people.
•	Staff who approve new or ongoing business relationships satisfy themselves that the firm has obtained **adequate CDD** information before doing so.	•	The firm has **no procedures** for dealing with situations requiring enhanced due diligence. **This breaches the ~~ML Regulations~~ Money Laundering Regulations 2017**.
		•	The firm fails to consider ~~both~~:
			◦ any individuals who ultimately control more ~~that~~ than 25% of shares or voting rights of a corporate customer; ~~**and**~~
			◦ any individuals who exercise control over the management ~~over~~ of a corporate customer; and
			◦ any individuals who control the body corporate

			~~a corporate customer~~ when identifying and verifying the customer's beneficial owners. **This breaches the ~~ML Regulations~~ Money Laundering Regulations 2017**.

See ~~ML Regs 8(1) MLR 8(2)(b) ML Reg 7(1)(d) ML Reg 14~~ regulations 5, 6, 27, 28, 31 33, 34 and 35 of the Money Laundering Regulations 2017.

3.2.5 Source of wealth and source of funds

A firm must conduct ongoing monitoring of its business relationships on a risk-sensitive basis. Ongoing monitoring means **scrutinising transactions** to ensure that they are consistent with what the firm knows about the customer, and taking steps to ensure that the firm's knowledge about the business relationship remains current. As part of this, firms must keep documents, data and information obtained in the CDD context (including information about the purpose and intended nature of the business relationship) up to date. It must apply CDD measures where it doubts the truth or adequacy of previously obtained documents, data or information (see ~~Box 3.4~~ *FCG* 3.2.4G).

Where the risk associated with the business relationship is increased, firms must carry out enhanced ongoing monitoring of the business relationship. ~~Box 3.8~~ *FCG* 3.2.9G provides guidance on enhanced ongoing monitoring.

Self-assessment questions:

- How are transactions **monitored** to spot potential money laundering? Are you satisfied that your monitoring (whether automatic, manual or both) is adequate and effective considering such factors as the size, nature and complexity of your business?
- Does the firm **challenge** unusual activity and explanations provided by the customer where appropriate?
- How are **unusual transactions** reviewed? (Many alerts will be false alarms, particularly when generated by automated systems. How does your firm decide whether behaviour really is suspicious?)
- How do you feed the **findings from monitoring** back into the customer's risk profile?

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	•	The firm fails to take adequate measures to understand the risk associated with the business relationship and is therefore **unable to conduct meaningful**

	transactions		**monitoring**.
•	Where a firm uses automated transaction monitoring systems, it understands their capabilities and limitations.	•	The MLRO can provide **little evidence** that **unusual transactions** are brought to their attention.
•	Small firms are able to apply credible **manual procedures** to scrutinise customers' behaviour.	•	Staff **always accept a customer's explanation** for unusual transactions at face value and do not probe further.
•	The '**rules**' underpinning monitoring systems are understood by the relevant staff and updated to reflect new trends.	•	The firm does not take risk-sensitive measures to ensure CDD information is **up to date**. **This is a breach of the ~~ML Regulations~~ Money Laundering Regulations 2017**.
•	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.		

See ~~MLR Reg 8(2)(b)~~ regulations 27, 28(11), 33, 34 of the Money Laundering Regulations 2017.

3.2.6 Source of wealth and source of funds

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

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

total wealth.

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

The JMLSG's guidance provides that, in situations where the risk of money laundering/terrorist financing is very low and subject to certain conditions, firms may assume that a payment drawn on an account in the customer's name with a UK, EU or equivalent regulated credit institution satisfied the standard CDD requirements. This is sometimes referred to as 'source of funds as evidence' and is distinct from 'source of funds' in the context of Regulation ~~8~~ 28(11) and ~~Regulation 14~~ Regulations 33 and 35 of the Money Laundering Regulations ~~2007~~ 2017 and of ~~this Guide~~ *FCG*. Nothing in ~~this Guide~~ *FCG* prevents the use of 'source of funds as evidence' in situations where this is appropriate.

Where the customer is a PEP a firm should have regard to guidance issued by the ~~FCA~~ *FCA* on the treatment of PEPs. See https://www.fca.org.uk/publications/finalised-guidance/fg17-6-treatment-politically-exposed-persons-peps-money-laundering.

3.2.7 Handling higher risk situations

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~~ Money Laundering Regulations 2017 also set out ~~three~~ some 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.~~

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

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

- **Business relationships or transactions with high risk third countries**: the Money Laundering Regulations 2017 define a high-risk third country as being one identified by the EU Commission by a delegated act. See EU Regulation 2016/1675.

- **Other transactions**: EDD must be performed where:

  (a) a transaction is complex and unusually large,

  (b) there is an unusual pattern of transactions, and

  (c) if the transaction(s) have no apparent economic or legal purpose.

- **Fake or Stolen identity documents**: if a firm discovers that a customer has provided such documents, and they propose to continue to deal with that customer, they must apply EDD.

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

See ~~ML Reg 7 7(3)(b) 14 14(2) 14(3) 14(4) 20~~ regulations 19, 20, 21, 28(16), 33 and 34 of the Money Laundering Regulations 2017.

3.2.8 Handling higher risk situations – enhanced due diligence (EDD)

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~~ *FCG* 3.2.3G considers risk assessment.

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

Examples of EDD include:

- obtaining more information about the customer's or beneficial owner's business
- obtaining more robust verification of the beneficial owner's identity based on information from a reliable and independent source
- gaining a better understanding of the customer's or beneficial owner's reputation and/or role in public life and assessing how this affects the level of risk associated with the business relationship
- carrying out searches on a corporate customer's directors or other individuals exercising control to understand whether their business or integrity affects the level of risk associated with the business relationship
- establishing how the customer or beneficial owner acquired their wealth to be satisfied that it is legitimate
- establishing the source of the customer's or beneficial owner's funds to be satisfied that they do not constitute the proceeds from crime.

Self-assessment questions:

- How does EDD differ from standard CDD? How are issues that are flagged during the due diligence process **followed up** and **resolved**? Is this adequately documented?
- How is EDD information **gathered**, **analysed**, **used** and **stored**?
- What involvement do senior management or committees have in **approving high risk customers**? What information do they receive to inform any decision-making in which they are involved?

Examples of good practice		Examples of poor practice	
•	The MLRO (and their team) have **adequate oversight** of all high risk relationships.	•	Senior management **do not give approval** for taking on high risk customers. **If the customer is a PEP or a non-EEA**

			correspondent ~~bank~~, this breaches the ~~ML Regulations~~ Money Laundering Regulations 2017.
•	The firm establishes the legitimacy of, and documents, the **source of wealth** and **source of funds** used in high risk business relationships.	•	~~The firm fails to consider whether a customer's **political connections** mean that they are high risk despite falling outside the ML Regulations Regulations' definition of a PEP.~~ [deleted]
•	Where money laundering risk is very high, the firm obtains **independent** internal or **external intelligence** reports.	•	The firm **does not distinguish** between the customer's source of funds and their source of wealth.
•	When assessing EDD, the firm **complements staff knowledge** of the customer or beneficial owner with more objective information.	•	The firm relies entirely on a **single source** of information for its enhanced due diligence.
•	The firm is able to provide evidence that relevant information staff have about customers or beneficial owners is **documented and challenged** during the CDD process.	•	A firm relies on intra-group introductions where **overseas standards are not UK-equivalent** or where due diligence data is **inaccessible** because of legal constraints.
•	A member of a group satisfies itself that it is appropriate to rely on due diligence performed by **other entities** in the same group.	•	The firm considers the **credit risk** posed by the customer, but not the **money laundering risk**.
•	The firm proactively **follows up gaps in, and updates,** CDD of higher risk customers.	•	The firm **disregards** allegations of the customer's or beneficial owner's **criminal activity** from reputable sources repeated over a sustained period of time.
•	A correspondent bank seeks to **identify PEPs** associated with their respondents.	•	The firm ignores adverse allegations simply because customers hold a UK **investment visa**.
•	A correspondent bank takes a view on the strength of the **AML regime** in a respondent bank's home country, drawing on discussions with the respondent,	•	A firm grants **waivers** from establishing source of funds, source of wealth or other due diligence without good reason.

	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.	•	A correspondent bank conducts inadequate due diligence on **parents** and **affiliates** of respondents.
		•	A correspondent bank **relies exclusively** on the Wolfsberg Group AML questionnaire.

See ~~ML Reg 14 14(4)(a) 14(3)(d)~~ regulations 33, 34, 34(1)(d), 35 and 35(5)(a) of the Money Laundering Regulations 2017.

3.2.9 Handling higher risk situations – enhanced ongoing monitoring

Firms must enhance their ongoing monitoring in higher risk situations.

Self-assessment questions:

- How does your firm **monitor** its high risk business relationships? How does enhanced ongoing monitoring differ from ongoing monitoring of other business relationships?
- Are reviews carried out **independently** of relationship managers?
- What **information** do you store in the files of high risk customers? Is it useful? (Does it include risk assessment, verification evidence, expected account activity, profile of customer or business relationship and, where applicable, information about the ultimate beneficial owner?)

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

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

See ~~ML Reg 14~~ regulation 33(1) of the Money Laundering Regulations 2017.

3.2.10 Liaison with law enforcement

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

Staff must report their concerns and may do so to the firm's nominated officer, who must then consider whether a report to NCA is necessary based on all the information at their disposal. Law enforcement agencies may seek information from the firm about a customer, often through the use of Production Orders (see *FCG* Annex 1~~: 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 nominated officer **passes all internal reports** to NCA without considering whether they truly are suspicious. These 'defensive' reports are likely to be of little value.
•	The firm's **SARs** set out a clear narrative of events and include detail that law enforcement authorities can use (e.g. names, addresses, passport numbers, phone numbers, email addresses).	•	The nominated officer **dismisses concerns** escalated by staff without reasons being documented.
•	SARs set out the reasons for suspicion in **plain English**. They include some context on any previous related SARs rather than just a cross-reference.	•	The firm **does not train** staff to make internal reports, thereby exposing them to personal legal liability and increasing the risk that suspicious activity goes unreported.
•	There is a clear process for **documenting** decisions.	•	The nominated officer **turns a blind eye** where a SAR might harm the business. **This could be a criminal offence.**
•	A firm's processes for dealing with suspicions reported to it by **third party administrators** are clear and effective.	•	A firm provides extraneous and irrelevant detail in response to a **Production Order**.

See ~~ML Reg 20(2)(d) 20(2)(d)(iii)~~ regulation 21 of the Money Laundering Regulations 2017 and s.330 POCA and s.331 POCA.

3.2.11 Record keeping and reliance on others

Firms must keep copies ~~or references to the evidence of the customer's identity~~ of any documents and information obtained to meet CDD requirements and sufficient supporting records for transactions for **five years** after the business relationship ends~~; and transactional documents for five years from the completion of the transaction~~ or five years after an occasional transaction. However, information need not be kept beyond 10 years for any transaction during a business relationship even if the business relationship has not ended. 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~~ the same time period. Firms must keep records sufficient to demonstrate to us that their CDD measures are appropriate in view of the risk of money laundering and terrorist financing.

Self-assessment questions:

- Can your firm retrieve records **promptly** in response to a Production Order?
- If the firm **relies on others** to carry out AML checks (see 'Reliance' in *FCG* Annex 1), is this within the limits permitted by the ~~ML Regulations~~ Money Laundering Regulations 2017? How does it satisfy itself that it can rely on these firms?

Examples of good practice		Examples of poor practice	
•	Records of customer ID and transaction data can be **retrieved quickly and without delay**.	•	The firm keeps customer records and related information in a way that **restricts** the **firm's access** to these records or their timely sharing with authorities.
•	Where the firm routinely relies on checks done by a third party (for example, a fund provider relies on an IFA's checks), it **requests sample documents** to test their reliability.	•	A firm cannot access CDD and related records for which it has relied on a third party. **This breaches the ~~ML Regulations~~ Money Laundering Regulations 2017**.
		•	Significant proportions of CDD records **cannot be retrieved** in good time.
		•	The firm has not considered whether a **third party** consents to being relied upon.
		•	There are **gaps** in customer records, which cannot be explained.

See ~~ML Reg 19 19(4) 7(3)(b) 19(6)~~ regulations 28(16), 40 and 40(7) of the Money Laundering Regulations 2017.

3.2.12 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~~ *FCG* 3.2.10G)

Examples of good practice		Examples of poor practice	
•	The firm has and uses an effective **process** for liaison with the authorities.	•	Financial crime **training** does not mention terrorist financing.
•	A firm identifies **sources of information** on terrorist financing risks: e.g. press reports, NCA alerts, Financial Action Task Force typologies, court judgements, etc.	•	A firm doing cross-border business has not assessed terrorism-related risks in **countries** in which it has a presence or does business.
•	This information informs the design of **transaction monitoring systems**.	•	A firm has not considered if its approach to **customer due diligence** is able to capture information relevant to the risks of terrorist finance.
•	Suspicions raised within the firm inform its own **typologies**.		

3.2.13 Customer payments

This section applies to banks subject to ~~SYSC~~ *SYSC* 6.3.

Interbank payments can be abused by criminals. International policymakers have taken steps intended to increase the transparency of interbank payments, allowing law enforcement agencies to more easily trace payments related to, for example, drug trafficking or terrorism. The ~~Wire~~ Funds Transfer Regulation requires banks to collect and attach information about ~~their customers~~ payers and payees of wire transfers (such as names and addresses, or, if a payment moves within the EU, a unique identifier like an account number) to payment messages. Banks are also required to check this information is present on inbound payments, and chase missing data. The ~~FCA~~ *FCA* has a legal responsibility to supervise banks' compliance with these requirements. Concerns have also been raised about interbank transfers known as "cover payments" (see *FCG* Annex 1~~: 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.

Self-assessment questions:

- How does your firm ensure that customer payment instructions contain **complete payer and payee information**? (For example, does it have appropriate procedures in place for checking payments it has received?)
- Does the firm review its **respondent banks'** track record on providing payer data and using appropriate SWIFT messages for cover payments?
- Does the firm use guidance issued by the ESAs? See http://www.eba.europa.eu/-/esas-provide-guidance-to-prevent-terrorist-financing-and-money-laundering-in-electronic-fund-transfers.

Examples of good practice		Examples of poor practice		
•	Although **not required by EU Regulation 1781/2006 on information on the payer accompanying transfers of funds (the Wire Transfer Regulation)**, the following are examples of good practice:	•	A *bank* fails to make use of the correct **SWIFT message type** for cover payments.	
•	Following processing, banks conduct **risk-based sampling** for inward payments to identify inadequate payer and payee information.	•	A bank fails to make use of the correct **SWIFT message type** for cover payments.	
•	An intermediary bank chases up **missing** information.	•	Compliance with regulations related to international customer payments has not been reviewed by the firm's **internal audit** or compliance departments. **The following practices breach the Funds Transfer Regulation:**	
•	A bank sends dummy messages to test the effectiveness of filters.		◦	International customer payment instructions sent by the payer's *bank* **lack meaningful payer and payee information**.
•	A bank is aware of guidance from the **Basel Committee** and the **Wolfsberg Group** on the use of cover payments, and has considered how this should apply to its own operations.		◦	An intermediary bank **strips** payee or payer information from payment instructions before passing the payment on.

•	The quality of payer and payee information in payment instructions from **respondent banks** is taken into account in the bank's ongoing review of correspondent banking relationships.		◦	The payee bank does not check any **incoming payments** to see if they include complete and meaningful data ~~about the ultimate transferor of the funds~~.
•	The firm actively engages in **peer discussions** about taking appropriate action against banks which persistently fail to provide complete payer information.			
	▫ ~~Following processing, *banks* conduct **risk-based sampling** for inward payments to identify inadequate payer information.~~			
	▫ ~~An intermediary *bank* chases up **missing** information.~~			
	▫ ~~A *bank* sends dummy messages to test the effectiveness of filters.~~			
	▫ ~~A bank is aware of guidance from the **Basel Committee** and the **Wolfsberg Group** on the use of cover payments, and has considered how this should apply to its own operations.~~			
~~•~~	~~The quality of payer information in payment instructions from **respondent banks** is taken into account in the bank's ongoing review of correspondent banking relationships.~~	~~•~~	~~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:**~~	
~~•~~	~~The firm actively engages in **peer discussions** about taking appropriate action against banks which persistently fail to provide~~		▫	~~International customer payment instructions sent by the payer's *bank* **lack meaningful payer*~~

	~~complete payer information.~~			**~~information~~**~~.~~
			~~b~~	~~An *intermediary* bank~~ **~~strips~~** ~~payer information from payment instructions before passing the payment on.~~
			~~b~~	~~The *payee bank* does not check any~~ **~~incoming payments~~** ~~to see if they include complete and meaningful data about the ultimate transferor of the funds.~~

3.2.14 Case study – poor AML controls

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

- Alpari failed to carry out satisfactory customer due diligence procedures at the account opening stage and failed to monitor accounts adequately.
- These failings were particularly serious given that the firm did business over the internet and had customers from higher risk jurisdictions.
- The firm failed to ensure that resources in its compliance and anti-money laundering areas kept pace with the firm's significant growth.

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

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

3.2.15 Case studies – wire transfer failures

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

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

In August 2010, Barclays Bank PLC agreed to pay US$298m to US authorities after it was found to have implemented practices designed to evade US sanctions

for the benefit of sanctioned countries and persons, including by stripping information from payment messages that would have alerted US financial institutions about the true origins of the funds. The bank self-reported the breaches, which took place over a decade-long period from as early as the mid-1990s to September 2006. See the US Department of Justice's press release: www.justice.gov/opa/pr/2010/August/10-crm-933.html.

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

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

- Coutts failed adequately to assess the level of money laundering risk posed by prospective and existing high risk customers.
- The firm failed to gather sufficient information to establish their high risk customers' source of funds and source of wealth, and to scrutinise appropriately the transactions of PEPs and other high risk accounts.
- The firm failed to ensure that resources in its compliance and anti-money laundering areas kept pace with the firm's significant growth.

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

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

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

3.2.17 Poor AML controls: risk assessment

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

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

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

of adequate and effective anti- money laundering risk management systems and controls.

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

3.3 Further guidance

3.3.1 ~~Part 2 of the Guide~~ *FCTR* contains the following additional AML guidance:

- ~~Chapter~~ *FCTR* 4 summarises the findings of, and consolidates good and poor practice from, the ~~FSA~~ *FSA*'s thematic review of Automated Anti-Money Laundering Transaction Monitoring Systems
- ~~Chapter~~ *FCTR* 5 summarises the findings of, and consolidates good and poor practice from, the ~~FSA~~ *FSA*'s Review of firms' implementation of a risk-based approach to anti-money laundering (AML*)*
- ~~Chapter~~ *FCTR* 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~~ *FCTR* 10.3.1G)
  - Account opening procedures (~~Box 10.2~~ *FCTR* 10.3.2G)
  - Monitoring activity (~~Box 10.3~~ *FCTR* 10.3.3G)
  - Suspicious activity reporting (~~Box 10.4~~ *FCTR* 10.3.4G)
  - Records (~~Box 10.5~~ *FCTR* 10.3.5G)
  - Responsibilities and risk assessments (~~Box 10.7~~*FCTR* 10.3.7G)
- ~~Chapter~~ *FCTR* 12 summarises the findings of the ~~FSA~~ *FSA*'s thematic review of Banks' management of high money laundering risk situations. It includes guidance on:
  - High risk customers and PEPs – AML policies and procedures (~~Box 12.1~~ *FCTR* 12.3.2G)
  - High risk customers and PEPs – Risk assessment (~~Box 12.2~~ *FCTR* 12.3.3G)
  - High risk customers and PEPs – Customer take-on (~~Box 12.3~~ *FCTR* 12.3.4G)
  - High risk customers and PEPs – Enhanced monitoring of high risk relationships (~~Box 12.4~~ *FCTR* 12.3.5G)
  - Correspondent banking – Risk assessment of respondent banks (~~Box 12.5~~ *FCTR* 12.3.6G)

- Correspondent banking – Customer take-on (~~Box 12.6~~ *FCTR* 12.3.7G)
- Correspondent banking – Ongoing monitoring of respondent accounts (~~Box 12.7~~ *FCTR* 12.3.8G)
- Wire transfers – Paying banks (~~Box 12.8~~*FCTR* 12.3.9G)
- Wire transfers – Intermediary banks (~~Box 12.9~~ *FCTR* 12.3.10G)
- Wire transfers – Beneficiary banks (~~Box 12.10~~ *FCTR* 12.3.11G)
- Wire transfers – Implementation of SWIFT MT202COV (~~Box 12.11~~ *FCTR* 12.3.12G)

3.3.2 ~~Part 2~~*FCTR* also summarises the findings of the following thematic reviews:

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

3.4 Sources of further information

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

- The Money Laundering Regulations ~~2007~~ 2017: ~~www.legislation.gov.uk/uksi/2007/2157/contents/made~~ http://www.legislation.gov.uk/uksi/2017/692/contents/made
- The NCA's website, which contains information on how to report suspicions of money laundering: www.nationalcrimeagency.gov.uk
- The JMLSG's guidance on measures firms can take to meet their anti-money laundering obligations, which is available from its website: www.jmlsg.org.uk
- ~~Our AML Regulations self-assessment fact sheet for financial advisers: www.fca.org.uk/static/documents/fsa-aml-tool-factsheet.pdf~~
- ~~The FCA's one-minute guide on AML Regulations for smaller firms: https://www.fca.org.uk/firms/financial-crime/money-laundering-terrorist-financing~~

3.4.2 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~~ work on terrorist financing: ~~www.fatf-gafi.org/dataoecd/28/43/40285899.pdf~~ http://www.fatf-gafi.org/publications/fatfgeneral/documents/terroristfinancing.html

3.4.3 To find out more on customer payments, see:

- Chapter 1 of Part III (Transparency in electronic payments (Wire transfers)) of the JMLSG's guidance, which will be banks' chief source of guidance on this topic: www.jmlsg.org.uk
- The Basel Committee's May 2009 paper on due diligence for cover payment messages: www.bis.org/publ/bcbs154.pdf
- The Wolfsberg Group's April 2007 statement on payment message standards: http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg_NYCH_Statement_on_Payment_Message_Standards_(2007).pdf
- Joint Guidelines to prevent terrorist financing and money laundering in electronic fund transfers- http://www.eba.europa.eu/-/esas-provide-guidance-to-prevent-terrorist-financing-and-money-laundering-in-electronic-fund-transfers
- The ~~Wire~~ Funds Transfer Regulation (EU Regulation ~~1781/2006~~ 847/2015 on information on the payer accompanying transfers of funds): ~~eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006R1781:en:NOT~~ http://data.europa.eu/eli/reg/2015/847/oj
- ~~Transfer of Funds (Information on the Payer) Regulations 2007: www.legislation.gov.uk/uksi/2007/3298/contents/made~~

3.4.4 To find out more on correspondent banking relationships see:

- FATF Guidance on correspondent banking services (October 2016)- http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Correspondent-Banking-Services.pdf
- Basel Committee on Banking Supervision guidance "Sound management of risks related to money laundering and financing of terrorism: revisions" (updated July 2017) https://www.bis.org/bcbs/publ/d405.htm

4 Fraud

4.1 Introduction

4.1.1 **Who should read this chapter?** This chapter applies to **all firms** subject to the financial crime rules in ~~SYSC~~ *SYSC* 3.2.6R or ~~SYSC~~ *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.

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

4.1.3 The contents of ~~the Guide's~~ *FCG*'s fraud chapter reflect the ~~FSA~~ *FSA*'s previous thematic work in this area. This means it does not specifically address such topics as plastic card, cheque or insurance fraud. This is not because the ~~FCA~~ *FCA* regards fraud prevention as unimportant. Rather it reflects our view that our limited resources are better directed elsewhere, given the strong incentive firms should have to protect themselves from fraud; and the number of other bodies active in fraud prevention. Links to some of these other bodies are provided in ~~paragraph 4.5~~ *FCG* 4.4.

4.2 Themes

4.2.1 ~~General – preventing~~ 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~~ *FCG* 2 also applies in relation to fraud.

Self-assessment questions:

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

Examples of good practice	Examples of poor practice

•	The firm takes a view on what areas of the firm are most **vulnerable** to fraudsters, and tailors defences accordingly.	•	Senior management appear **unaware** of fraud incidents and trends. No management information is produced.
•	Controls adapt to **new fraud threats**.	•	**Fraud losses are buried** in bad debts or other losses.
•	The firm engages with relevant **cross-industry efforts** to combat fraud (e.g. data-sharing initiatives like CIFAS and the Insurance Fraud Bureau, collaboration to strengthen payment systems, etc.) in relation to both internal and external fraud.	•	There is no clear and consistent **definition** of fraud across the business, so reporting is haphazard.
•	**Fraud response plans and investigation procedures** set out how the firm will respond to incidents of fraud.	•	Fraud risks are not explored when **new products** and **delivery channels** are developed.
•	**Lessons** are learnt from incidents of fraud.	•	Staff **lack awareness** of what constitutes fraudulent behaviour (e.g. for a salesman to misreport a customer's salary to secure a loan would be fraud).
•	**Anti-fraud good practice** is shared widely within the firm.	•	**Sales incentives** act to encourage staff or management to turn a blind eye to potential fraud.
•	To guard against **insider fraud**, staff in high risk positions (e.g. finance department, trading floor) are subject to enhanced vetting and closer scrutiny. 'Four eyes' procedures (see *FCG* Annex 1 for common terms) are in place.	•	Banks fail to implement the requirements of the **Payment Services Regulations** and **Banking Conduct of Business rules**, leaving customers out of pocket after fraudulent transactions are made.
•	**Enhanced due diligence** is performed on higher risk customers (e.g. commercial customers with limited financial history. See 'long firm fraud' in *FCG* Annex 1).	•	**Remuneration structures** may incentivise behaviour that increases the risk of mortgage fraud.

4.2.2 Mortgage fraud – lenders

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

Self-assessment questions:

- Are systems and controls to detect and prevent mortgage fraud **coordinated across the firm**, with resources allocated on the basis of an assessment of where they can be used to best effect?
- How does your firm contain the fraud risks posed by corrupt **conveyancers, brokers and valuers**?
- How and when does your firm engage with **cross-industry information-sharing exercises**?

Examples of good practice		Examples of poor practice	
•	A firm's underwriting process can **identify** applications that may present a **higher risk** of mortgage fraud.	•	A lender fails to report relevant information to the ~~FCA~~ *FCA*'s **Information from Lenders (IFL)** scheme as per ~~FCA~~ *FCA* guidance on IFL referrals.
•	Membership of a lender's **panels** of brokers, conveyancers and valuers is subject to ongoing review. Dormant third parties are identified.	•	A lender **lacks a clear definition** of mortgage fraud, undermining data collection and trend analysis.
•	A lender **reviews existing mortgage books** to identify and assess mortgage fraud indicators.	•	A lender's panels of conveyancers, brokers and valuers are **too large to be manageable**.
•	A lender verifies that funds are being dispersed **in line with instructions** before it releases them.	•	The lender does no work to identify **dormant parties**.
•	A lender **promptly discharges** mortgages that have been redeemed and checks whether conveyancers register charges with the **Land Registry** in good time.	•	A lender relies solely on the Financial Services Register when **vetting brokers**.
		•	Underwriters' demanding work targets **undermine** efforts to contain mortgage fraud.

4.2.3 Mortgage fraud – intermediaries

This section applies to mortgage intermediaries.

Self-assessment questions:

- does your firm satisfy itself that it is able to **recognise** mortgage fraud?
- When processing applications, does your firm consider whether the information the applicant provides is **consistent**? (For example, is declared income believable compared with stated employment? Is the value of the requested mortgage comparable with what your firm knows about the location of the property to be purchased?)
- What due diligence does your firm undertake on **introducers**?

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

4.2.4 Enforcement action against mortgage brokers

Since the ~~FSA~~ *FSA* began regulating mortgage brokers in October 2004, the ~~FSA~~ *FSA* have banned over 100 mortgage brokers. Breaches have included:

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

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

4.2.5 Investment fraud

UK consumers are targeted by share-sale frauds and other scams including land-banking frauds, unauthorised collective investment schemes and Ponzi schemes.

Customers of UK deposit-takers may fall victim to these frauds, or be complicit in them. We expect these risks to be considered as part of deposit-takers' risk assessments, and for this to inform management's decisions about the allocation of resources to a) the detection of fraudsters among the customer base and b) the protection of potential victims.

Self-assessment questions:

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

Examples of good practice		Examples of poor practice	
•	A bank regularly assesses the risk to itself and its customers of losses from fraud, including investment fraud, in accordance with their established risk management framework. The risk assessment does not only cover situations where the bank could cover losses, but also where customers could lose and not be reimbursed by the bank. Resource allocation and mitigation measures are informed by this assessment.	•	A bank has performed no risk assessment that considers the risk to customers from investment fraud.
•	A bank contacts customers if it suspects a payment is being made to an investment fraudster.	•	A bank fails to use actionable, credible information it has about known or suspected perpetrators of investment fraud in its financial crime prevention systems.
•	A bank has transaction monitoring rules designed to detect specific types of investment fraud. Investment fraud subject matter experts help set these rules.	•	Ongoing monitoring of commercial accounts is allocated to customer-facing staff incentivised to bring in or retain business.
		•	A bank allocates excessive numbers of commercial accounts to a staff member to monitor.

4.3 Further guidance

4.3.1 ~~Part 2 of the Guide~~ *FCTR* contains the following additional material on fraud:

- ~~Chapter~~ *FCTR* 10 summarises the findings of the Small Firms Financial Crime Review. It contains guidance directed at small firms on:
  - Monitoring activity (~~Box 10.3~~ *FCTR* 10.3.3G)
  - Responsibilities and risk assessments (~~Box 10.7~~ *FCTR* 10.3.7G)
  - General fraud (~~Box 10.13~~*FCTR* 10.3.13G)
  - Insurance fraud (~~Box 10.14~~*FCTR* 10.3.14G)
  - Investment fraud (~~Box 10.15~~*FCTR* 10.3.15G)
  - Mortgage fraud (~~Box 10.16~~ *FCTR* 10.3.16G)
  - Staff/Internal fraud (~~Box 10.17~~ *FCTR* 10.3.17G)
- *FCTR* 11 summarises the findings of the ~~FSA~~ *FSA*'s thematic review Mortgage fraud against lenders. It contains guidance on:
  - Governance, culture and information sharing (~~Box 11.1~~ *FCTR* 11.3.1G)
  - Applications processing and underwriting (~~Box 11.2~~ *FCTR* 11.3.2G)
  - Mortgage fraud prevention, investigations, and recoveries (~~Box 11.3~~ *FCTR* 11.3.3G)
  - Managing relationships with conveyancers, brokers and valuers (~~Box 11.4~~ *FCTR* 11.3.4G)
  - Compliance and internal audit (~~Box 11.5~~ *FCTR* 11.3.5G)
  - Staff recruitment and vetting (~~Box 11.6~~ *FCTR* 11.3.6G)
  - Remuneration structures (~~Box 11.7~~ *FCTR* 11.3.7G)
  - Staff training and awareness (~~Box 11.8~~ *FCTR* 11.3.8G)
- *FCTR* 14 summarises the findings of the ~~FSA~~ *FSA*'s thematic review Banks' defences against investment fraud. It contains guidance directed at deposit-takers with retail customers on:
  - Governance (~~Box 14.1~~ *FCTR* 14.3.2G)
  - Risk assessment (~~Box 14.2~~ *FCTR* 14.3.3G)

- Detecting perpetrators (~~Box 14.3~~ *FCTR* 14.3.4G)
- Automated monitoring (~~Box 14.4~~ *FCTR* 14.3.5G)
- Protecting victims (~~Box 14.5~~ *FCTR* 14.3.6G)
- Management reporting and escalation of suspicions (~~Box 14.6~~ *FCTR* 14.3.7G)
- Staff awareness (~~Box 14.7~~ *FCTR* 14.3.8G)
- Use of industry intelligence (~~Box 14.8~~ *FCTR* 14.3.9G)

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

4.4 Sources of further information

4..1 To find out more about what ~~FCA~~ *FCA* is doing about fraud, see:

- Details of the ~~FCA~~ *FCA*'s Information from Lenders scheme: https://www.fca.org.uk/firms/fraud/report-mortgage-fraud-lenders
- Details of the ~~FCA~~ *FCA*'s Information from Brokers scheme: www.fca.org.uk/firms/firm-types/mortgage-brokers-and-home-finance-lenders/report
- ~~Our fact sheet for mortgage brokers on mortgage fraud: www.fsa.gov.uk/smallfirms/resources/factsheets/pdfs/mortgage_fraud.pdf~~

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

- ~~The National Fraud Authority, which works with the counter-fraud community to make fraud more difficult to commit in and against the UK: www.homeoffice.gov.uk/agencies-public-bodies/nfa/~~
- ~~The National Fraud Authority's cross-sector strategy, Fighting Fraud Together. The strategy, which the FCA endorses, aims to reduce fraud: https://www.gov.uk/government/publications/nfa-fighting-fraud-together~~
- Action Fraud, which is the UK's national fraud reporting centre: ~~www.actionfraud.police.uk~~ www.actionfraud.org.uk
- Fighting Fraud Action (FFA-UK) is responsible for leading the collective fight against financial fraud on behalf of the UK payments industry, https://www.financialfraudaction.org.uk/.
- The City of London Police, which has 'lead authority' status in the UK for the investigation of economic crime, including fraud

https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/Pages/default.aspx

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

5 Data security

5.1 Introduction

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

5.1.2 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. See section 4 and schedule 1 Data Protection Act 1998.

5.2 Themes

5.2.1 Governance

The guidance in ~~Box 2.1~~ *FCG* 2.2.1G on governance in relation to financial crime also applies to data security.

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

Self-assessment questions:

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

Examples of good practice	Examples of poor practice

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

5.2.2 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.

5.2.3 Controls

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

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

Self-assessment questions:

- Is your firm's customer data taken **off-site**, whether by staff (sales people, those working from home) or third parties (suppliers, consultants, IT contractors etc)?
- If so, what **levels of security** exist? (For example, does the firm require automatic encryption of laptops that leave the premises, or measures to ensure no sensitive data is taken off-site? If customer data is transferred electronically, does the firm use secure internet links?)
- How does the firm **keep track** of its digital assets?
- How does it **dispose** of documents, computers, and imaging equipment such as photocopiers that retain records of copies? Are accredited suppliers used to, for example, destroy documents and hard disks? How does the firm satisfy itself that data is disposed of competently?
- How are **access** to the premises and sensitive areas of the business **controlled**?
- When are **staff access rights** reviewed? (It is good practice to review them at least on recruitment, when staff change roles, and when they leave the firm.)
- Is there enhanced **vetting** of staff with access to lots of data?
- How are staff made aware of **data security risks**?

Examples of good practice		Examples of poor practice	
•	**Access** to sensitive areas (call centres, server rooms, filing rooms) is restricted.	•	Staff and third party suppliers can access **data they do not need** for their role.

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

5.2.4 Case study – protecting customers' accounts from criminals

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

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

- Callers to Norwich Union Life call centres were able to satisfy the firm's caller identification procedures by providing public information to impersonate customers.
- Callers obtained access to customer information, including policy numbers and bank details and, using this information, were able to

request amendments to Norwich Union Life records, including changing the addresses and bank account details recorded for those customers.

- The frauds were committed through a series of calls, often carried out in quick succession.
- Callers subsequently requested the surrender of customers' policies.
- Over the course of 2006, 74 policies totalling £3.3m were fraudulently surrendered.
- The firm failed to address issues highlighted by the frauds in an appropriate and timely manner even after they were identified by its own compliance department.
- Norwich Union Life's procedures were insufficiently clear as to who was responsible for the management of its response to these actual and attempted frauds. As a result, the firm did not give appropriate priority to the financial crime risks when considering those risks against competing priorities such as customer service.

For more, see the ~~FSA~~ *FSA*'s press release:
www.fsa.gov.uk/pages/Library/Communication/PR/2007/130.shtml

5.2.5 Case study – data security failings

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

- The firm failed to take reasonable care to ensure that it had effective systems and controls to manage the risks relating to the security of confidential customer information arising out of its outsourcing arrangement with another Zurich company in South Africa.
- It failed to carry out adequate due diligence on the data security procedures used by the South African company and its subcontractors.
- It relied on group policies without considering whether this was sufficient and did not determine for itself whether appropriate data security policies had been adequately implemented by the South African company.
- The firm failed to put in place proper reporting lines. While various members of senior management had responsibility for data security issues, there was no single data security manager with overall responsibility.
- The firm did not discover that the South African entity had lost an unencrypted back-up tape until a year after it happened.

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

5.3 Further guidance

5.3.1 ~~Part 2 of the Guide~~ *FCTR* contains the following additional material on data security:

- ~~Chapter~~ *FCTR* 6 summarises the findings of the ~~FSA~~ *FSA*'s thematic review of Data security in Financial Services and includes guidance on:
  - Governance (~~Box 6.1~~ *FCTR* 6.3.1G)
  - Training and awareness (~~Box 6.2~~ *FCTR* 6.3.2G)
  - Staff recruitment and vetting (~~Box 6.3~~ *FCTR* 6.3.3G)
  - Controls – access rights (~~Box 6.4~~ *FCTR* 6.3.4G)
  - Controls – passwords and user accounts (~~Box 6.5~~ *FCTR* 6.3.5G)
  - Controls – monitoring access to customer data (~~Box 6.6~~ *FCTR* 6.3.6G)
  - Controls – data back-up (~~Box 6.7~~ *FCTR* 6.3.7G)
  - Controls – access to the internet and email (~~Box 6.8~~ *FCTR* 6.3.8G)
  - Controls – key-logging devices (~~Box 6.9~~ *FCTR* 6.3.9G)
  - Controls – laptop (~~Box 6.10~~*FCTR* 6.3.10G)
  - Controls – portable media including USB devices and CDs (~~Box 6.11~~ *FCTR* 6.3.11G)
  - Physical security (~~Box 6.12~~ *FCTR* 6.3.12G)
  - Disposal of customer data (~~Box 6.13~~ *FCTR* 6.3.13G)
  - Managing third party suppliers (~~Box 6.14~~ *FCTR* 6.3.14G)
  - Internal audit and compliance monitoring (~~Box 6.15~~ *FCTR* 6.3.15G)
- ~~*Chapter*~~ *FCTR* 10 summarises the findings of the Small Firms Financial Crime Review, and contains guidance directed at small firms on:
  - Records (~~Box 10.5~~ *FCTR* 10.3.5G)

- Responsibilities and risk assessments (~~Box 10.7~~ *FCTR* 10.3.7G)
- Access to systems (~~Box 10.8~~ *FCTR* 10.3.8G)
- Outsourcing (~~Box 10.9~~ *FCTR* 10.3.9G)
- Physical controls (~~Box 10.10~~ *FCTR* 10.3.10G)
- Data disposal (~~Box 10.11~~ *FCTR* 10.3.11G)
- Data compromise incidents (~~Box 10.12~~ *FCTR* 10.3.12G)

5.4 Sources of further information

5.4.1 To find out more, see~~:~~

- ~~The~~ the website of the Information Commissioner's Office: www.ico.org.uk.
- ~~A one-minute guide for small firms on data security: https://www.fca.org.uk/firms/financial-crime/data-security~~

6 Bribery and corruption

6.1 Introduction

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

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

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

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

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

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

6.2 Themes

6.2.1 Governance

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

Self-assessment questions:

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

Examples of good practice		Examples of poor practice	
•	The firm is committed to carrying out business fairly, honestly and openly.	•	There is a lack of awareness of, or engagement in, anti-bribery and corruption at senior management or board level.

•	Senior management lead by example in complying with the firm's anti-corruption policies and procedures.	•	An 'ask no questions' culture sees management turn a blind eye to how new business is generated.
•	Responsibility for anti-bribery and corruption systems and controls is clearly documented and apportioned to a single senior manager or a committee with appropriate terms of reference and senior management membership who reports ultimately to the board.	•	Little or no management information is sent to the board about existing and emerging bribery and corruption risks faced by the business, including: higher risk third-party relationships or payments; the systems and controls to mitigate those risks; the effectiveness of these systems and controls; and legal and regulatory developments.
•	Anti-bribery systems and controls are subject to audit.		
•	Management information submitted to the board ensures they are adequately informed of internal and external developments relevant to bribery and corruption and respond to these swiftly and effectively.		

6.2.2 Risk assessment

The guidance in ~~Box 2.3~~ *FCG* 2.2.4G on risk assessment in relation to financial crime also applies to bribery and corruption.

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

Self-assessment questions:

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

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

charitable and political donations and your use of third parties?)

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

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

Examples of good practice		Examples of poor practice	
•	Corruption risks are assessed in **all jurisdictions** where the firm operates and across all business channels.	•	Departments responsible for identifying and assessing bribery and corruption risk are ill equipped to do so.
•	The firm considers factors that might lead business units to **downplay** the level of bribery and corruption risk to which they are exposed, such as lack of expertise or awareness, or potential conflicts of interest.	•	For fear of harming the business, the firm classifies as low risk a jurisdiction generally associated with high risk.
		•	The risk assessment is only based on generic, external sources.

6.2.3 Policies and procedures

The guidance in ~~Box 2.4~~ *FCG* 2.2.5G on policies and procedures in relation to financial crime and in ~~Box 2.5~~ *FCG* 2.2.6G on staff recruitment, vetting, training, awareness and remuneration also applies to bribery and corruption.

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

Self-assessment questions:

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

- Have you considered the extent to which **corporate hospitality** might influence, or be perceived to influence, a business decision? Do you

impose and enforce limits that are appropriate to your business and proportionate to the bribery and corruption risk associated with your business relationships?

- How do you satisfy yourself that your anti-corruption policies and procedures are applied effectively?
- How do your firm's policies and procedures help it to identify whether someone acting on behalf of the firm is corrupt?
- How does your firm react to suspicions or allegations of bribery or corruption involving people with whom the firm is connected?

Examples of good practice		Examples of poor practice	
•	The firm **clearly sets out** behaviour expected of those acting on its behalf.	•	The firm **does not assess** the extent to which staff comply with its anti-corruption policies and procedures.
•	There are **unambiguous consequences** for breaches of the firm's anti-corruption policy.	•	The firm's anti-corruption policies and procedures are **out of date**.
•	Risk-based, appropriate additional monitoring and due diligence are undertaken for jurisdictions, sectors and business relationships identified as **higher risk**.	•	A firm relies on passages in the staff code of conduct that prohibit improper payments, but has no other **controls**.
•	Staff responsible for implementing and monitoring anti-bribery and corruption policies and procedures have adequate levels of **anti-corruption expertise**.	•	The firm does not **record** corporate hospitality given or received.
•	Where appropriate, the firm refers to existing sources of information, such as expense registers, policy queries and whistleblowing and complaints hotlines, to monitor the effectiveness of its anti- bribery and corruption policies and procedures.	•	The firm **does not respond** to external events that may highlight weaknesses in its anti-corruption systems and controls.
•	**Political and charitable donations** are subject to appropriate due diligence and	•	The firm fails to consider whether clients or charities who stand to benefit from corporate hospitality or

	are approved at an appropriate management level, with compliance input.		donations have **links to relevant political or administrative decision-makers**.
•	Firms who do not provide staff with access to whistleblowing hotlines have processes in place to allow staff to **raise concerns in confidence or, where possible, anonymously**, with adequate levels of protection.	•	The firm fails to maintain **records of incidents and complaints**.

See ~~SYSC~~ *SYSC* 3.2.6R and ~~SYSC~~ *SYSC* 6.1.1R.

6.2.4 Dealing with third parties

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

Self-assessment questions:

- Do your firm's policies and procedures **clearly define** 'third party'?
- Do you **know** your third party?
- What is your firm's policy on **selecting** third parties? How do you check whether it is being followed?
- To what extent are third-party relationships **monitored** and **reviewed**? Is the frequency and depth of the monitoring and review commensurate to the risk associated with the relationship?
- Is the **extent** of due diligence on third parties determined on a risk-sensitive basis? Do you seek to identify any bribery and corruption issues as part of your due diligence work, e.g. negative allegations against the third party or any political connections? Is due diligence applied consistently when establishing and reviewing third-party relationships?
- Is the risk assessment and due diligence information kept **up to date**? How?
- Do you have effective systems and controls in place to ensure **payments** to third parties are in line with what is both expected and approved?

Examples of good practice		Examples of poor practice	
•	Where a firm uses third parties to generate business, these	•	A firm using intermediaries fails to satisfy itself that those businesses

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

6.2.5 Case study – corruption risk

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

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

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

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

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

In July 2011, the ~~FSA~~ *FSA* fined Willis Limited, an insurance intermediary, £6.9m for failing to take appropriate steps to ensure that payments made to overseas third parties were not used for corrupt purposes. Between January 2005 and December 2009, Willis Limited made payments totalling £27m to overseas third parties who helped win and retain business from overseas clients, particularly in high risk jurisdictions.

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

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

- It did not ensure that adequate due diligence was carried out on overseas third parties to evaluate the risk involved in doing business with them.
- It failed to review in sufficient detail its relationships with overseas third parties on a regular basis to confirm whether it was necessary and appropriate to continue with the relationship.
- It did not adequately monitor its staff to ensure that each time it engaged an overseas third party an adequate commercial rationale had been recorded and that sufficient due diligence had been carried out.

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

6.3 Further guidance

6.3.1 ~~*Part 2 of the Guide*~~ *FCTR* contains the following additional material on bribery and corruption:

- ~~Chapter~~ FCTR 9 summarises the findings of the ~~FSA~~ *FSA*'s thematic review Anti-bribery and corruption in commercial insurance broking and includes guidance on:
  - Governance and management information (~~Box 9.1~~ *FCTR* 9.3.1G)
  - Risk assessment and responses to significant bribery and corruption events (~~Box 9.2~~*FCTR* 9.3.2G)
  - Due diligence on third-party relationships (~~Box 9.3~~ *FCTR* 9.3.3G)
  - Payment controls (~~Box 9.4~~ *FCTR* 9.3.4G)
  - Staff recruitment and vetting (~~Box 9.5~~ *FCTR* 9.3.5G)
  - Training and awareness (~~Box 9.6~~ *FCTR* 9.3.6G)
  - Risk arising from remuneration structures (~~Box 9.7~~ *FCTR* 9.3.7G)
  - Incident reporting (~~box 9.8~~ *FCTR* 9.3.8G)
  - The role of compliance and internal audit (~~Box 9.9~~ *FCTR* 9.3.9G)
- ~~*Chapter*~~ *FCTR* 13 summarises the findings of the ~~FSA~~ *FSA*'s thematic review on Anti-bribery and corruption systems and controls in investment banks and includes guidance on:
  - Governance and management information (~~Box 13.1~~*FCTR* 13.3.2G)
  - Assessing bribery and corruption risk (~~Box 13.2~~ *FCTR* 13.3.3G)
  - Policies and procedures (~~Box 13.3~~ *FCTR* 13.3.4G)

- Third party relationships and due diligence (~~Box 13.4~~ *FCTR* 13.3.5G)
- Payment controls (~~Box 13.5~~ *FCTR* 13.3.6G)
- Gifts and hospitality (~~Box 13.6~~ *FCTR* 13.3.7G)
- Staff recruitment and vetting (~~Box 13.7~~ *FCTR* 13.3.8G)
- Training and awareness (~~Box 13.8~~ *FCTR* 13.3.9G)
- Remuneration structures (~~Box 13.9~~ *FCTR* 13.3.10G)
- Incident reporting and management (~~Box 13.10~~ *FCTR* 13.3.11G)

6.4 Sources of further information

6.4.1 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:
  ~~http://webarchive.nationalarchives.gov.uk/20140102181807/https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/181762/bribery-act-2010-guidance.pdf (full version)~~
  https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf (full version)
  ~~http://webarchive.nationalarchives.gov.uk/20140102181807/https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/181764/bribery-act-2010-quick-start-guide.pdf (quick-start guide)~~
  https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-quick-start-guide.pdf (quick start guide)
- Our one-minute guide for smaller firms on anti-bribery and corruption: https://www.fca.org.uk/firms/financial-crime/bribery-corruption

7 Sanctions and asset freezes

7.1 Introduction

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

7.1.2 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~~ *FSA*-supervised firms. ~~Box 7.5~~ *FCG* 7.2.5G, 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.

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

7.1.4 ~~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 *FCG* Annex 1) and measures to prevent the proliferation of weapons of mass destruction.~~ Financial sanctions are restrictions put in place by the UK government or the multilateral organisations that limit the provision of certain financial services or restrict access to financial markets, funds and economic resources in order to achieve a specific foreign policy or national security objective.

7.1.5 ~~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 (United Nations Measures) Order 2009 (SI 2009/1747), financial services, to those on the list, unless a licence is obtained from the Treasury's dedicated Asset Freezing Unit. 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. The Treasury maintains a Consolidated List of financial sanctions targets designated by the United Nations, the European Union and the United Kingdom, which is available from its website. If firms become aware of a breach, they must notify the Asset Freezing Unit in accordance with the relevant provisions.~~ All individuals and legal entities who are within or undertake activities within the UK's territory must comply with the EU and UK financial sanctions that are in force. All UK nationals and UK legal entities established under UK law, including their branches, must also comply with UK financial sanctions that are in force, irrespective of where their activities take place.

7.1.5A The Office of Financial Sanctions (OFSI) within the Treasury maintains a Consolidated List of financial sanctions targets designated by the United Nations, the European Union and the United Kingdom, which is available from its website. If firms become aware of a breach, they must notify OFSI in accordance with the relevant provisions. OFSI have published guidance on complying with UK obligations and this is available on their website. See

https://www.gov.uk/government/publications/financial-sanctions-faqs.

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

7.2 Themes

7.2.1 Governance

The guidance in ~~Box 2.1~~ *FCG* 2.2.1G 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.	•	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**.
•	It is clear **at what stage customers are screened** in different situations (e.g. when customers are passed from agents or other companies in the group).	•	No **internal audit** resource is allocated to monitoring sanctions compliance.
•	There is **appropriate escalation** of actual target matches and breaches of UK sanctions. Notifications are timely.	•	Some business units in a large organisation think they are **exempt**.

The offence will depend on the sanctions provisions breached.

7.2.2 Risk assessment

The guidance in ~~Box 2.3~~ *FCG* 2.2.4G on risk assessment in relation to financial crime also applies to sanctions.

A firm should consider which areas of its business are most likely to provide services or resources to individuals or entities on the Consolidated List.

Self-assessment questions:

- Does your firm have a **clear view** on where within the firm breaches are most likely to occur? (This may cover different business lines, sales channels, customer types, geographical locations, etc.)
- How is the risk assessment **kept up to date**, particularly after the firm enters a new jurisdiction or introduces a new product?

Examples of good practice		Examples of poor practice	
•	A firm with international operations, or that deals in currencies other than sterling, understands the requirements of relevant **local financial sanctions regimes**.	•	There is **no process** for updating the risk assessment.
•	A small firm is **aware** of the sanctions regime and where it is most vulnerable, even if risk assessment is only informal.	•	The firm assumes financial sanctions **only apply to money transfers** and so has not assessed its risks.

7.2.3 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 knowingly continue to retain customers who are listed under UK sanctions: this is permitted if ~~the Asset Freezing Unit~~ OFSI 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 appropriate.	•	The firm assumes that an intermediary has screened a customer, but **does not check** this.
•	There are quality control checks over **manual screening**.	•	Where a firm uses automated systems, it does not understand how to **calibrate** them and does not check whether the number of hits is unexpectedly high or low.
•	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.).	•	An insurance company **only screens when claims** are made on a policy.
•	The firm screens customers' **directors** and known **beneficial owners** on a risk-sensitive basis.	•	Screening of customer databases is a **one-off** exercise.
•	Where the firm maintains an account for a listed individual, the status of this account is **clearly flagged** to staff.	•	Updating from the Consolidated List is **haphazard**. Some business units use out-of-date lists.
•	A firm only places faith in **other firms' screening** (such as outsourcers or intermediaries) after taking steps to satisfy themselves this is appropriate.	•	The firm has **no means** of monitoring payment instructions.

7.2.4 Matches and escalation

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

Self-assessment questions:

- What steps does your firm take to identify whether **a name match is**

real? (For example, does the firm look at a range of identifier information such as name, date of birth, address or other customer data?)

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

Examples of good practice		Examples of poor practice	
•	Sufficient resources are available to identify '**false positives**'.	•	The firm **does not report a breach** of the financial sanctions regime to OFSI ~~the Asset Freezing Unit~~: **this could be a criminal offence**.
•	After a breach, as well as meeting its formal obligation to notify **OFSI ~~the Asset Freezing Unit~~**, the firm considers whether it should report the breach to the ~~FCA~~ *FCA*. ~~Chapter 15.3 of the Supervision manual (SUP)~~ *SUP* 15.3 ~~of the *Handbook*~~ contains general notification requirements. Firms are required to tell us, for example, about significant rule breaches (see ~~SUP~~ *SUP* 15.3.11R(1)). Firms should therefore consider whether the breach is the result of any matter within the scope of ~~SUP~~ *SUP* 15.3, for example a significant failure in their financial crime systems and controls.	•	An account is **not frozen** when a match with the Consolidated List is identified. If, as a consequence, funds held, owned or controlled by a designated person are dealt with or made available to the designated person, **this could be a criminal offence**.
		•	A **lack of resources** prevents a firm from **adequately analysing** matches.
		•	**No audit trail** of decisions where potential target matches are judged to be false positives.

The offence will depend on the sanctions provisions breached.

7.2.5 Weapons proliferation

Alongside financial sanctions, the government imposes controls on certain types of trade in order to achieve foreign policy objectives. The export of goods and services for use in nuclear, radiological, chemical or biological weapons programmes is

subject to strict controls. Firms' systems and controls should address the proliferation risks they face.

Self-assessment questions:

- Does your firm finance trade with **high risk countries**? If so, is **enhanced due diligence** carried out on counterparties and goods? Where doubt remains, is evidence sought from exporters that the trade is legitimate?
- Does your firm have **customers from high risk countries**, or with a history of dealing with individuals and entities from such places? If so, has the firm reviewed how the sanctions situation could affect such counterparties, and discussed with them how they may be affected by relevant regulations?
- What **other business** takes place with high risk jurisdictions, and what measures are in place to contain the risks of transactions being related to proliferation?

Examples of good practice		Examples of poor practice	
•	A bank has identified if its customers export goods to high risk jurisdictions, and subjects transactions to **enhanced scrutiny** by identifying, for example, whether goods may be subject to export restrictions, or end-users may be of concern.	•	The firm **assumes** customers selling goods to countries of concern will have checked the exports are legitimate, and **does not ask for evidence** of this from customers.
•	Where **doubt exists**, the bank asks the customer to **demonstrate** that appropriate assurances have been gained from relevant government authorities.	•	~~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.
•	The firm has considered **how to respond** if the government takes action under the Counter-Terrorism Act 2008 against one of 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.~~ [deleted]

7.2.6 Case study – deficient sanctions systems and controls

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

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

The failings led the ~~FSA~~ *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~~ *FSA*.

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

7.3 Further guidance

7.3.1 ~~Part 2 of the Guide~~ *FCTR* contains the following additional material on sanctions and assets freezes:

- ~~Chapter~~ *FCTR* 8 summarises the findings of the ~~FSA~~ *FSA's* thematic review Financial services firms' approach to UK financial sanctions and includes guidance on:
  - Senior management responsibility (~~Box 8.1~~ *FCTR* 8.3.1G)
  - Risk assessment (~~Box 8.2~~ *FCTR* 8.3.2G)
  - Policies and procedures (~~Box 8.3~~*FCTR* 8.3.3G)
  - Staff training and awareness (~~Box 8.4~~ *FCTR* 8.3.4G)
  - Screening during client take-on (~~Box 8.5~~ *FCTR* 8.3.5G)
  - Ongoing screening (~~Box 8.6~~ *FCTR* 8.3.6G)
  - Treatment of potential target matches (~~Box 8.7~~ *FCTR* 8.3.7G)
- ~~Chapter~~ *FCTR* 15 summarises the findings of the ~~FCA~~ *FCA*'s thematic review Banks' management of financial crime risk in trade finance and includes guidance on:

- Sanctions Procedures (~~Box 15.7~~ *FCTR* 15.3.7G)
- Dual-Use Goods (~~Box 15.8~~ *FCTR* 15.3.8G)

7.4 Sources of further information

7.4.1 To find out more on financial sanctions, see:

- ~~The website of the Treasury's Asset Freezing Unit: https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation~~ OFSI's website: https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation
- OFSI provides FAQs on financial sanctions- https://www.gov.uk/government/publications/financial-sanctions-faqs
- Part III of the Joint Money Laundering Steering Group's guidance, which is a chief source of guidance for firms on this topic: www.jmlsg.org.uk
  - ~~The Treasury also provides information on general licences: www.hm-treasury.gov.uk/fin_sanctions_general_licences.htm~~
  - ~~Part III of the Joint Money Laundering Steering Group's guidance, which is a chief source of guidance for firms on this topic: www.jmlsg.org.uk~~
- ~~Our fact sheet on financial sanctions aimed at small firms: https://www.fca.org.uk/firms/financial-crime/financial-sanctions~~

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

- Part III of the Joint Money Laundering Steering Group's guidance on the prevention of money laundering and terrorist financing, which contains a chapter on proliferation financing that should be firms' chief source of guidance on this topic: www.jmlsg.org.uk
- The website of the UK's Export Control Organisation, which contains much useful information, including lists of equipment requiring a licence to be exported to any destination, because they are either military items or 'dual use' ~~(see *FCG* Annex 1). 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~~ https://www.gov.uk/government/organisations/export-control-organisation
- ~~The BIS Iran List, which shows, among other things, entities in Iran who have had export licenses declined:~~

~~www.bis.gov.uk/policies/export-control-organisation/eco-notices-exporters~~

- The NCA's website, which contains guidelines on how to report suspicions related to weapons proliferation: http://www.nationalcrimeagency.gov.uk/publications/514-guidelines-for-counter-proliferation-financing-reporting-1/file

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

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

8 Insider dealing and market manipulation

8.1 Introduction

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

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

8.1.3 Section 1H(3) of the Financial Services and Markets Act 2000 (FSMA) defines financial crime to include 'any offence involving:

(a) fraud or dishonesty,

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

(c) handling the proceeds of crime, or

(d) the financing of terrorism'.

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

8.1.4 To avoid doubt, all references to insider dealing and market manipulation in this document refer to the criminal offences set out above. The civil offences of insider dealing, unlawful disclosure of inside information and market manipulation set out in the EU Market Abuse Regulation (No 596/2014) (MAR) are referred to collectively herein as market abuse.

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

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

8.1.7 On 3 July 2016, MAR came into force. MAR sets out the civil offences of market abuse. Article 16 of MAR also imposes specific requirements on:

- Market operators and investment firms that operate a trading venue to establish and maintain effective arrangements, systems and procedures aimed at detecting and preventing insider dealing, market manipulation and attempted insider dealing and market manipulation. Such persons shall report orders and transactions that could constitute insider dealing or market manipulation (or attempts at such) to the competent authority of the trading venue. This is imposed under article 16(1).
- Any person professionally arranging or executing transactions to establish and maintain effective arrangements, systems and procedures to detect and report suspicious orders and transactions. This is imposed under article 16(2).

8.1.8 There is a key distinction between the obligations under article 16(2) of MAR and the requirements of *SYSC* 6.1.1R. Article 16(2) of MAR requires firms to detect and report potential market abuse, whereas *SYSC* 6.1.1R requires firms to counter the risk of financial crime. (As noted above, article 16(1) of MAR obliges market operators and investment firms that operate a trading venue to have systems aimed at preventing as well as detecting potential market abuse). This document does not provide any *FCA* guidance in relation to MAR article 16.

8.1.9 Appropriate measures for the prevention of financial crime are likely to fall into two distinct categories:

(1) the identification and prevention of attempted financial crime pre-trade, and

(2) the mitigation of future risks posed by clients who have been identified as having already traded suspiciously.

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

8.2 Themes

8.2.1 Governance

The guidance in *FCG* 2.2 above on governance in relation to financial crime also applies to countering the risk of insider dealing and market manipulation.

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

- Understanding the risks of insider dealing or market manipulation that their firm is exposed to (both through employee and client activity).
- Establishing adequate policies and procedures to counter these risks in accordance with *SYSC* 6.1.1R.

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

Self-assessment questions:

- Does the firm's senior management team understand the legal definitions of insider dealing and market manipulation, and the ways in which the firm may be exposed to the risk of these crimes?
- Does the firm's senior management team regularly receive management information in relation to suspected insider dealing or market manipulation?
- How does senior management make sure that the firm's systems and controls for detecting insider dealing and market manipulation are robust? How do they set the tone from the top?
- How does the firm's MLRO interact with the individual/departments responsible for order and trade surveillance/monitoring?
- How does senior management make decisions in relation to concerns about potential financial crime raised to them by Compliance? Do they act appropriately to mitigate these risks?
- How does senior management make sure that its employees have the appropriate training to identify potential insider dealing and market manipulation?

Examples of good practice		Examples of poor practice	
•	Senior management are able to recognise and articulate the warning signs that insider dealing and market manipulation	•	There is little evidence that possible insider dealing or market manipulation is taken seriously by senior management. Addressing

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

8.2.2 Risk assessment

The guidance in *FCG* 2.2.4G above on risk assessment in relation to financial crime also applies to countering the risk of insider dealing and market manipulation.

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

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

- undertaking enhanced order and transaction monitoring on clients,
- setting client specific pre-trade limits, and
- ultimately declining business or terminating client relationships if appropriate (see *FCG* 8.5 for more detail).

Self-assessment questions:

- Has the firm considered whether any of its products/services it offers, or the clients it has, pose a higher risk that the firm might be used to facilitate insider dealing or market manipulation? How has the firm determined this?
- Who is responsible for carrying out the risk assessment and keeping it up to date? Do they have sufficient levels of expertise (including

markets and financial crime knowledge) and seniority?

- How does the firm use its risk assessment when deciding which business to accept?
- How often is the risk framework reviewed and who approves it?
- How does the firm's risk framework for countering the risk of insider dealing and market manipulation interact with the firm's AML risk framework? Are the risk assessments aligned?

Examples of good practice		Examples of poor practice	
•	Insider dealing and market manipulation risks are assessed across every asset class and client type the firm operates with.	•	Risk assessments are generic, and not based upon the firm's own observations.
•	There is evidence that the firm's risk assessment informs the design of its surveillance controls.	•	An inappropriate risk classification system makes it almost impossible for a relationship to be considered 'high risk'.
•	The firm's risk framework is regularly tested and reviewed.	•	Risk assessments are inappropriately influenced by profitability of new or existing relationships.
•	Where a firm identifies a risk that it may be used to facilitate insider dealing or market manipulation, it takes appropriate steps to mitigate that risk.	•	The firm submits a significant number of SARs and STORs on a particular client, but continues to service that client without considering its obligation to counter the risk of financial crime.
•	The firm considers where relationship managers might become too close to customers to take an objective view of risk. It manages that risk effectively.		

8.2.3 Policies and procedures

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

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

market manipulation risk assessment.

Firms should ensure that their policies cover procedures for both:

(1) identifying and preventing attempted financial crime before any trade is executed, and

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

Firms should make sure that clear policies and procedures are in place so that front office employees are aware of the firm's obligation to counter the risk of financial crime. Among other things, these should reflect the *FCA's* expectation that market participants should refuse to execute any trade where there is a clear risk that the trade is in breach of relevant legal or regulatory requirements.

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

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

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

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

Self-assessment questions:

- Does the policy define how the firm will mitigate the risk of insider dealing and market manipulation? For example, does it outline what steps the firm will take to prevent suspicious trading from being accepted? In what circumstances would the firm stop providing trading access to a particular client?

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

- Do front office staff understand how insider dealing and market manipulation might be committed through the firm, to escalate potentially suspicious activity when appropriate, and challenge client orders if they believe the activity will amount to financial crime? Does the firm have effective whistleblowing arrangements in place to support appropriate financial crime detection and reporting?

Examples of good practice		Examples of poor practice	
•	The firm has clear and unambiguous expectations for its employees and anyone acting on its behalf, such as introducing brokers.	•	The firm's policies and procedures aren't updated for legal or regulatory changes.
•	Employees in dealing roles understand and are able to identify potentially illegal conduct, and their trading is regularly monitored by Compliance.	•	Policies and procedures are generic and don't consider the specific processes or risks of the firm.
•	The policies and procedures make adequate reference to the firm's risk assessment.	•	Policies and procedures cover only post-trade identification and reporting of suspicious activity and are silent on countering financial crime.
•	Policies and procedures make sure that the risk of financial crime is considered throughout the lifecycle of a security transaction, including before the order has been executed.	•	The firm sets apparently robust procedures for assessing and mitigating identified financial crime risk, but sets thresholds for engaging these measures which mean that they are almost impossible to trigger.
•	The firm takes swift, robust action for breaches of its policies and procedures.	•	The firm doesn't have policies detailing the circumstances when a prospective or existing client would be rejected or have their relationship with the firm terminated.
•	The firm has policies detailing when a prospective or existing client would be rejected or the relationship terminated.	•	The firm doesn't have appropriate policies or procedures in place regarding personal account dealing, so that staff are able to deal in a manner which creates conflict in escalating suspected market abuse.

8.2.4 Ongoing monitoring

We recognise that MAR already imposes monitoring requirements on persons professionally arranging or executing transactions, in order to detect and report suspicious orders and transactions in the form of STORs (as well as imposing similar monitoring obligations on market operators and investment firms that operate a trading venue). It may be appropriate to use the results of this monitoring

for the purpose of countering financial crime.

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

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

If a firm is, based on their understanding of a customer and monitoring of that customer's transactions, suspicious that a client might have committed or attempted to commit insider dealing or market manipulation, the firm should comply with its obligations to report those suspicions via a STOR and/or SAR, and review the options available to counter the risk of financial crime posed by its ongoing relationship with that client.

These could include:

- Carrying out enhanced due diligence and enhanced monitoring of the client's trading activity (including applying enhanced scrutiny to incoming orders, prior to execution).
- Restricting the client's access to particular markets or instruments.
- Restricting services provided to the client (eg direct market access).
- Restricting the amount of leverage the firm is willing to provide to the client.
- Ultimately terminating the client relationship. The appropriate response will depend on the outcome of the firm's monitoring procedures and the extent and nature of any suspicious activity identified.

Self-assessment questions:

- Does the firm consider its obligations to counter financial crime when a client's activity is determined as suspicious via surveillance systems and subsequent investigation?
- How do the firm's monitoring arrangements interact with the client-on-boarding process / AML framework?
- Does the firm undertake enhanced monitoring for high risk clients?
- Does the firm's monitoring cover the activity of any employee trading?

Examples of good practice	Examples of poor practice

•	The firm's monitoring seeks to identify trends in clients' behaviour, in addition to one off events.	•	Firm believes that its obligations cease when it reports the suspicious transactions and orders.
•	The firm undertakes enhanced monitoring of clients it has determined are high risk.	•	Suspicious transactions and orders are identified but not investigated further.
•	The firm conducts regular, targeted monitoring of voice and electronic communications.	•	Suspicious transactions and orders are identified but not investigated further.
•	Front office employees escalate suspicious activity promptly to Compliance.	•	Monitoring identifies individual suspicious events but does not attempt to identify patterns of suspicious behaviour by the same client or a group of clients, using, for example, historical assessments of potentially suspicious activity or STORs submitted.
•	The firm conducts regular monitoring of its staff trading activity, including proprietary and personal account dealing.	•	The firm does not use information obtained via monitoring and subsequent investigation to consider the suitability of retaining a client relationship.

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~~ *FCG*. This annex does not provide guidance on rules or amend corresponding references in the ~~Handbook Glossary~~ *Handbook's Glossary.*

Term	Meaning
Action Fraud	The UK's national fraud reporting centre. See: www.actionfraud.police.uk
advance fee fraud	A fraud where people are persuaded to hand over money, typically characterised as a 'fee', in the expectation that they will then be able to gain access to a much larger sum which does not actually exist.
~~AFU~~	~~See 'Asset Freezing Unit'.~~

AML	Anti-money laundering. See 'money laundering'.
Annex I financial institution	The Money Laundering Regulations ~~2007~~ 2017 give the ~~FCA~~ *FCA* responsibility for supervising the anti-money laundering controls of 'Annex I financial institutions' (a reference to Annex I to the ~~Banking Consolidation Directive~~ Capital Requirements Directive, where they are listed). In practice, this includes businesses that offer finance leases, commercial lenders and providers of safe deposit boxes. Where an authorised firm offers such services, we are responsible for overseeing whether these activities are performed in a manner that complies with the requirements of the Money Laundering Regulations ~~2007~~ 2017. Authorised firms are not formally required to inform us that they perform these activities, although some may choose to do so for the sake of transparency. Where these businesses are not authorised, we are responsible for supervising their activities. For more information on this, see the ~~FCA~~ *FCA*'s website: ~~www.fsa.gov.uk/pages/About/What/financial_crime/money_laundering/3mld/registered/index.shtml~~ https://www.fca.org.uk/firms/money-laundering-terrorist-financing/registration
~~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 first set out the list of 'Annex I Financial Institutions' that was subsequently used to define the scope of the Third Money Laundering Directive.~~
beneficial owner	The natural person who ultimately owns or controls the customer. An entity may have more than one beneficial owner. 'Beneficial owner' is defined in ~~Regulation~~ Regulations 5 and 6 of the Money Laundering Regulations ~~2007~~ 2017.
boiler room	See 'share sale fraud'.
bribery	Bribery is the offering or acceptance of an undue advantage in exchange for the improper performance of a function or activity. Statutory offences of bribery are set out more fully in the Bribery Act 2010.

Bribery Act 2010	The Bribery Act came into force in July 2011. It outlaws offering and receiving bribes, at home and abroad, as well as creating a corporate offence of failure to prevent bribery. The Ministry of Justice has issued guidance about procedures which firms can put in place to prevent bribery: ~~http://webarchive.nationalarchives.gov.uk/20140102181807/https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/181762/bribery-act-2010-guidance.pdf~~ https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf
business-wide risk assessment	A business-wide risk assessment means the identification and assessment of the financial crime risks to which a firm is exposed as a result of, for example, the products and services it offers, the jurisdictions it operates in, the types of customer it attracts, the complexity and volume of transactions, and the distribution channels it uses to service its customers.
carbon credit scams	Firms may sell carbon credit certificates or seek investment directly in a 'green' project that generates carbon credits as a return. Carbon credits can be sold and traded legitimately and there are many reputable firms operating in the sector. We are, however, concerned an increasing number of firms are using dubious, high-pressure sales tactics and targeting vulnerable consumers. See: ~~https://www.fca.org.uk/consumers/carbon-credit-trading~~ https://www.fca.org.uk/scamsmart/carbon-credit-scams
CDD	See 'customer due diligence'.
CIFAS	CIFAS is the UK's fraud prevention service with over 250 members across the financial industry and other sectors. See CIFAS's website for more information: www.cifas.org.uk
consent	If a firm is concerned that it may be assisting in the laundering of funds it can file a Suspicious Activity Report and apply to the NCA for consent to continue the transaction. ~~The Proceeds of Crime Act 2002 gives the NCA seven working days to respond. The NCA will either agree that the transaction can go ahead or it will refuse consent. In the latter case the NCA has 31 calendar days in which to take further action: for example, to seek a court order to restrain the assets in question.~~ The NCA has further details for this which they now refer to as "requesting a defence": http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/ukfiu/seeking-consent-for-financial-transactions

Consolidated List	~~The Treasury~~ OFSI maintains a Consolidated List of financial sanctions targets designated by the United Nations, the European Union and the United Kingdom. It is available from the Treasury's website: www.hm-treasury.gov.uk/fin_sanctions_index.htm
corruption	Corruption is the abuse of public or private office to obtain an undue advantage. Corruption includes not only bribery but also other forms of misconduct or improper behaviour. This behaviour may or may not be induced by the prospect of obtaining an undue advantage from another person.
Counter-Terrorism Act 2008	The Treasury has powers under Schedule 7 to the Counter-Terrorism Act 2008 to require financial firms to take specified actions in relation to a country of concern, or counterparties based in that country. Use of this power can be triggered if a) the risk of money laundering or terrorist financing activities is identified in a country, or b) the government believes a country has a nuclear, chemical, radiological or biological weapons programme that threatens the UK. The directions can require enhanced due diligence and ongoing monitoring, the systematic reporting of transactions, or the cessation of business. This offers the government flexibility that was not available in the traditional financial sanctions regime. We are responsible for monitoring authorised firms' and certain financial institutions' compliance with these directions.
cover payment	Where payments between customers of two banks in different countries and currencies require settlement by means of matching inter-bank payments, those matching payments are known as 'cover payments'. International policymakers have expressed concern that cover payments can be abused to hide the origins of flows of funds. In response to this, changes to the SWIFT payment messaging system now allow originator and beneficiary information to accompany cover payments.
CPS	See 'Crown Prosecution Service'
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~~ 2017. 'Customer due diligence' and 'Know Your Customer' (KYC) are sometimes used interchangeably.
dual use goods	Items that can have legitimate commercial uses, while also having applications in programmes to develop weapons of mass destruction. Examples may be alloys constructed to tolerances and thresholds sufficiently high for them to be suitable for use in nuclear reactors. Many such goods are listed in EU regulations which also restrict their unlicensed export.
Data Protection Act 1998 (DPA)	The DPA imposes legal obligations on those who handle individuals' personal information. Authorised firms are required to take appropriate security measures against the loss, destruction or damage of personal data. Firms also retain responsibility when data is passed to a third party for processing.
economic sanctions	Restrictions on trade or financial flows imposed by the government in order to achieve foreign policy goals. See: 'financial sanctions regime', 'trade sanctions', and 'proliferation finance'.
EEA firms	Firms from the European Economic Area (EEA) which passport into the UK are authorised persons. This means, generally speaking, EEA firms who carry on relevant business from a UK branch will be subject to the requirements of the ~~Handbook~~ *Handbook* and of the Money Laundering Regulations ~~2007~~ 2017. 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~~ 2017, unless it carries on its business through representatives who are temporarily located in the UK.
Egmont Group	A forum for financial intelligence units from across the world. See the Egmont Group's website for more information: www.egmontgroup.org
embargos	See 'trade sanctions'.
e-money	The *Electronic Money Regulations 2011* (SI 2011/99) define electronic money as electronically (including magnetically)

	stored monetary value, represented by a claim on the issuer, which is issued on receipt of funds for the purpose of making payment transactions, and which is accepted by a person other than the electronic money issuer. The E-money Regulations specify who can issue e-money; this includes credit institutions and e-money institutions.
e-money institutions (EMIs)	E-money institutions are a specific category of financial institutions authorised or registered to issue e-money under the *Electronic Money Regulations 2011*, rather than FSMA. The ~~FCA~~ *FCA*'s financial crime ~~Handbook~~ *Handbook* provisions do not apply to e-money institutions, but the ~~FCA~~ *FCA* supervises e-money institutions for compliance with their obligations under the Money Laundering Regulations ~~2007~~ 2017. 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 payment services and e-money approach document: ~~www.fsa.gov.uk/pubs/international/approach_emoney.pdf~~ https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf
enhanced due diligence (EDD)	~~The~~ Regulations 33-35 of the Money Laundering Regulations ~~2007~~ 2017 require firms to apply additional, 'enhanced' customer due diligence measures in higher risk situations (see ~~Boxes 3.6~~ *FCG* 3.2.7G to ~~3,8~~ *FCG* 3.2.9G).
equivalent jurisdiction	A jurisdiction (other than an EEA state) whose law contains equivalent provisions to those contained in the ~~Third~~ Fourth Money Laundering Directive. The JMLSG has prepared guidance for firms on how to identify which jurisdictions are equivalent. Equivalent jurisdictions are significant because it is a factor that a firm ~~is able~~ may consider when deciding whether to apply 'simplified due diligence' to financial institutions from these places. Firms can also rely on the customer due diligence checks undertaken by certain introducers from these jurisdictions (see 'reliance').
export controls	UK exporters must obtain a licence from the government before exporting certain types of goods, primarily those with military applications. Exporting these goods without a licence is prohibited by the Export Control Order 2008 (SI 2008/3231). If an authorised financial firm were to finance or insure these illegal exports, it would arguably have been used to further financial crime.
family member of a PEP	Regulation 35(12)(b) of the Money Laundering Regulations 2017 defines a family member of a PEP as including a spouse

	or civil partner of a PEP; children of the PEP and the spouses or civil partners of the PEP's children; and the parents of a PEP. The *FCA's* Finalised Guidance 'FG17/16: The treatment of politically exposed persons for anti-money laundering purposes' provides further guidance on this definition.
FATF	See 'Financial Action Task Force'.
FATF Recommendations	Forty Recommendations issued by the FATF on the structural, supervisory and operational procedures that countries should have in place to combat money laundering. These were revised in February 2012, and now incorporate the nine Special Recommendations on the prevention of terrorist financing that were previously listed separately. The Forty Recommendations can be downloaded from the FATF's website: www.fatf-gafi.org/dataoecd/7/40/34849567.PDF
FATF Special Recommendations	Nine Recommendations on the prevention of terrorist financing were introduced by the FATF in October 2001. These were incorporated into the revised 40 Recommendations in February 2012 and are no longer separately listed.
FATF-style regional bodies	Regional international bodies such as Moneyval and the Asia-Pacific Group which have a similar form and functions to those of the FATF. The FATF seeks to work closely with such bodies.
FI	See 'Financial Investigator'.
Financial Action Task Force (FATF)	An intergovernmental body that develops and promotes anti-money laundering and counter terrorist financing standards worldwide. Further information is available on its website: www.fatf-gafi.org
Financial Conduct Authority (~~FCA~~ *FCA*)	The *Financial Conduct Authority* has statutory objectives under FSMA that include protecting and enhancing the integrity of the UK financial system. The integrity of the UK financial system includes its not being used for a purpose connected with financial crime. We have supervisory responsibilities under the Money Laundering Regulations ~~2007~~ 2017 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~~ as Schedule 7 to the Counter-Terrorism Act 2008.

financial crime	Financial crime is any crime involving money. More formally, the Financial Services and Markets Act 2000 defines financial crime 'to include any offence involving (a) fraud or dishonesty; (b) misconduct in, or misuse of information relating to, a financial market; or (c) handling the proceeds of crime'. The use of the term 'to include' means financial crime can be interpreted widely to include, for example, corruption or funding terrorism.
financial intelligence unit (FIU)	The IMF uses the following definition: 'a central national agency responsible for receiving, analyzing, and transmitting disclosures on suspicious transactions to the competent authorities.' The NCA has this role in the UK.
Financial Investigator (FI)	Financial Investigators are accredited people able under the relevant legislation to investigate financial offences and recover the proceeds of crime.
financial sanctions regime	This prohibits firms from providing funds and other economic resources (and, in the case of designated terrorists, financial services) to individuals and entities on a Consolidated List maintained ~~by the Asset Freezing Unit of the Treasury~~ OFSI. ~~The Asset Freezing Unit~~ OFSI is responsible for ensuring compliance with the UK's financial sanctions regime; our role is to ensure firms have appropriate systems and controls to enable compliance.
Financial Services and Markets Act 2000 (FSMA)	The Financial Services and Markets Act 2000 sets out the objectives, duties and powers of the Financial Conduct Authority and the Prudential Regulation Authority.
Financial Services Authority (~~FSA~~ *FSA*)	The Financial Services Authority was the previous financial services regulator. It had statutory objectives under FSMA that included the reduction of financial crime. The ~~FSA~~ *FSA* had supervisory responsibilities under the Money Laundering Regulations 2007 for authorised firms and businesses such as leasing companies and providers of safe deposit boxes. It also had functions under other legislation such as the Transfer of Funds (Information on the Payer) Regulations 2007, in relation to the EU Wire Transfer Regulation, and schedule 7 to the Counter-Terrorism Act 2008.
FIU	See 'financial intelligence unit'.
four-eyes procedures	Procedures that require the oversight of two people, to lessen the risk of fraudulent behaviour, financial mismanagement or incompetence going unchecked.

Fourth Money Laundering Directive (4MLD)	The Fourth Money Laundering Directive (2015/849/EC). The UK has implemented this Directive mainly through the Money Laundering Regulations 2017.	
fraud (types of)	Fraud can affect firms and their customers in many ways. The following are examples of fraud:	
	•	a firm is defrauded by customers (e.g. mortgage fraud);
	•	a firm is defrauded by employees or contractors ('insiders') (e.g. a staff member steals from his employer and amends records to cover-up the theft);
	•	a firm's customers are defrauded by an insider (e.g. a staff member steals customers' money);
	•	a firm's customers are defrauded after a third party misleads the firm (e.g. criminals evade security measures to gain access to a customer's account);
	•	a firm's customers are defrauded by a third party because of the firm's actions (e.g. the firm loses sensitive personal data allowing the customer's identity to be stolen);
	•	a customer is defrauded, with a firm executing payments connected to this fraud on the customer's instruction (e.g. a customer asks his bank to transfer funds to what turns out to be a share sale scam).
	See also: 'advance fee fraud', 'boiler room', 'carbon credit scams', 'investment fraud', 'land banking scams', 'long firm fraud', 'mass-marketing fraud', 'Missing Trader Inter-Community fraud', 'Ponzi and pyramid schemes', 'share sale fraud'.	
Fraud Act 2006	The Fraud Act 2006 sets out a series of fraud offences such as fraud by false representation, fraud by failing to disclose information and fraud by abuse of position.	
FSA	See 'Financial Services Authority'.	
FSMA	See 'Financial Services and Markets Act 2000'.	
FSRB	See 'FATF-style regional bodies'.	

fuzzy matching	The JMLSG suggests the term 'fuzzy matching' 'describes any process that identifies non-exact matches. Fuzzy matching software solutions identify possible matches where data – whether in official lists or in firms' internal records – is misspelled, incomplete, or missing. They are often tolerant of multinational and linguistic differences in spelling, formats for dates of birth, and similar data. A sophisticated system will have a variety of settings, enabling greater or less fuzziness in the matching process'. See Part III of the JMLSG's guidance: ~~www.jmlsg.org/download/7323~~ http://www.jmlsg.org.uk/download/10007
Funds Transfer Regulation	This EU Regulation is formally titled 'Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds'. It implements FATF's Recommendation 16 in the EU and requires firms to accompany the transfer of funds with specified information identifying the payer and the payee. We are given supervisory and enforcement powers for compliance with this regulation by the Money Laundering Regulations 2017.
high-value dealer	A firm trading in goods (e.g. cars, jewellery and antiques) that accepts cash of ~~€15,000~~ €10,000 or more in payment (whether in one go or in several payments that appear to be linked). HMRC is the supervisory authority for high value dealers. A full definition is set out in Regulation ~~3(12)~~ 14(1)(a) of the Money Laundering Regulations ~~2007~~ 2017.
HM Revenue and Customs (HMRC)	HM Revenue and Customs has supervisory responsibilities under the Money Laundering Regulations ~~2007~~ 2017. It oversees money service businesses, dealers in high value goods, estate agents and trust or company service providers, amongst others. See HMRC's website for more information: ~~www.hmrc.gov.uk/index.htm~~ https://www.gov.uk/topic/business-tax/money-laundering-regulations
HMRC	See 'HM Revenue and Customs'.
HMT	See 'Treasury'.
ICO	See 'Information Commissioner's Office'.
ID	Identification (or Identity Documents).
identification	The JMLSG's definition is: 'ascertaining the name of, and other relevant information about, a customer or beneficial owner'.

IFB	Insurance Fraud Bureau.
Information Commissioner's Office (ICO)	The Information Commissioner's Office is tasked with protecting the public's personal information. See the ICO's website for further information: www.ico.org.uk
Information From Lenders (IFL)	The Information From Lenders scheme enables mortgage lenders to inform the ~~FCA~~ *FCA* of suspected fraud by mortgage brokers. Details are here: ~~www.fsa.gov.uk/pages/doing/regulated/supervise/mortgage_fraud.shtml~~ https://www.fca.org.uk/firms/fraud/report-mortgage-fraud-advisers
insider fraud	Fraud against a firm committed by an employee or group of employees. This can range from junior staff to senior management, directors, etc. Insiders seeking to defraud their employer may work alone, or with others outside the firm, including organised criminals.
Institute of Chartered Accountants in England and Wales (ICAEW)	The Institute of Chartered Accountants in England and Wales has supervisory responsibility for its members under the Money Laundering Regulations ~~2007~~ 2017, as do other professional bodies for accountants and book-keepers. See the ICAEW's website for further information: www.icaew.com
integration	See 'placement, layering, integration'.
investment fraud	UK-based investors lose money every year to share sale frauds and other scams including, but not limited to, land-banking frauds, Ponzi schemes, and rogue carbon credit schemes. See~~:~~ ~~www.fsa.gov.uk/consumerinformation/scamsandswindles/investment_scams~~ ~~FCA~~ *FCA's* scamsmart, http://scamsmart.fca.org.uk/
JMLSG	See 'Joint Money Laundering Steering Group'.
Joint Money Laundering Steering Group (JMLSG)	This industry body is made up of financial sector trade bodies. It produces guidance on compliance with legal and regulatory requirements related to money laundering. See the JMLSG's website for more information: www.jmlsg.org.uk
Know Your Customer (KYC)	This term is often used as a synonym for 'customer due diligence' checks. The term can also refer to suitability checks related to the regulated sales of financial products. The Money Laundering Regulations ~~2007~~ 2017 refer to 'customer due diligence' and not to KYC.
known close	Regulation 35(12)(c) of the Money Laundering Regulations

associate of a PEP	2017 defines a known close associate of a PEP as being either an individual known to have joint beneficial ownership of a legal entity or a legal arrangement or any other close business relations with a PEP or an individual who has sole beneficial ownership of a legal entity or a legal arrangement which is known to have been set up for the benefit of a PEP.
KYC	See 'Know Your Customer'.
land banking scams	Land banking companies divide land into smaller plots to sell it to investors on the basis that once it is available for development it will soar in value. However, the land is often in rural areas, with little chance of planning permission being granted. See: ~~https://www.fca.org.uk/consumers/land-banking-investment-schemes~~ https://www.fca.org.uk/consumers/land-banking-investment-schemes
layering	See 'placement, layering, integration'.
long firm fraud	A fraud where an apparently legitimate company is established and, over a period of time, builds up a good credit record with wholesalers, paying promptly for modest transactions. Correspondence from bankers may be used by them as evidence of good standing. The company then places a large order, takes delivery, but disappears without paying. This type of fraud is not limited to wholesalers of physical goods: financial firms have been victim to variants of this scam.
Market Abuse Regulation (MAR)	MAR, short for Market Abuse Regulation (EU No.596/2014), entered into force on 3 July 2016. It contains the civil offences of insider dealing, unlawful disclosure of inside information and market manipulation, in addition to provisions to prevent and detect these offences.
MLRO	See 'Money Laundering Reporting Officer'.
mass-marketing fraud	Action Fraud (the UK's national fraud reporting centre) says "Mass marketing fraud is when you receive an uninvited contact by email, letter, phone or adverts, making false promises to con you out of money." Share sale fraud is a type of mass marketing fraud. See: www.actionfraud.police.uk/types-of-fraud/mass-marketing-fraud
Missing Trader Inter-Community (MTIC) fraud	This fraud exploits the EU system for rebating Value Added Tax payments in situations where goods have moved across borders within the EU. National authorities are misled into giving rebates to import-export companies that are not

	entitled to them.
money laundering	The process by which the proceeds of crime are converted into assets which appear to have a legitimate origin, so that they can be retained permanently, or recycled to fund further crime.
Money Laundering Directive	See '~~Third~~ Fourth Money Laundering Directive'.
Money Laundering Regulations 2007	The Money Laundering Regulations 2007 (SI 2007/2157) transposed the Third Money Laundering Directive into UK law. The Regulations require firms to take specified steps to detect and prevent both money laundering and terrorist financing. The Money Laundering Regulations 2007 were revoked and replaced by the Money Laundering Regulations 2017.
Money Laundering Regulations ~~2007~~ 2017	The Money Laundering Regulations ~~2007~~ 2017 (SI ~~2007/2157~~ 2017/692) transpose the requirements of the ~~Third~~ Fourth Money Laundering Directive into UK law. The Regulations require firms to take specified steps to detect and prevent both money laundering and terrorist financing. The Regulations identify the firms we supervise and impose on us a duty to take measures to secure those firms' compliance with the Regulations' requirements.
Money Laundering Reporting Officer (MLRO)	The MLRO is responsible for ensuring that measures to combat money laundering within the firm are effective. The MLRO is also usually the 'nominated officer' under the Proceeds of Crime Act (POCA). The MLRO is a 'controlled function' under the Approved Persons Regime and a 'senior management function' under the Senior Managers and Certification Regime.
money service business (MSB)	An undertaking that by way of business operates a currency exchange office, transmits money (or any representations of monetary value) by any means or which cashes cheques which are made payable to customers. (See Regulation ~~2(1)~~ 3(1) of the Money Laundering Regulations ~~2007~~ 2017.) Firms authorised under FSMA 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~~ https://www.fca.org.uk/firms/money-laundering-terrorist-financing/reporting HM Revenue and Customs supervises the AML controls of

	money service businesses that are not authorised under FSMA. More information about registration with HMRC can be found on its website: ~~www.hmrc.gov.uk/mlr~~ https://www.gov.uk/topic/business-tax/money-laundering-regulations
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~~ *SYSC* 3.2.6R. However, they are not subject to the Money Laundering Regulations ~~2007~~ 2017 or the provisions of the ~~Handbook~~ *Handbook* that specifically relate to money laundering (~~SYSC~~ *SYSC* 3.2.6AR – ~~SYSC~~ SYSC 3.2.6JG). Firms offering these services alongside other products that are subject to the Money Laundering Regulations 2017 (such as banking and stock broking services) can therefore apply different customer due diligence checks in both situations. But in practice, many will choose to apply a consistent approach for the sake of operational convenience.
MSB	See 'money service business'.
MTIC	See 'Missing Trader Inter-Community Fraud'.
National Crime Agency (NCA)	The NCA leads the UK's fight against serious and organised crime. It became operational, replacing the Serious Organised Crime Agency, in October 2013. For more information see the NCA's website: http://www.nationalcrimeagency.gov.uk/.
~~National Fraud Authority (NFA)~~	~~The National Fraud Authority is responsible for devising and implementing a national fraud strategy. See the NFA's website for more information: www.homeoffice.gov.uk/agencies-public-bodies/nfa~~
NCA	See 'National Crime Agency'.
NCCT	See 'non-cooperative countries or territories'.
~~NFA~~	~~See 'National Fraud Authority'.~~
nominated officer	~~A person in a firm nominated to receive disclosures from others within the firm who know or suspect that a person is engaged in money laundering or terrorist financing.~~ Regulation 3(1) of the Money Laundering Regulations 2017 defines this as "a person who is nominated to receive disclosures under Part 3 (terrorist property) of the Terrorism Act 2000 or Part 7 (money laundering) of the Proceeds of Crime Act 2002". See section 330 of POCA, Part 3 of the

	Terrorism Act 2000, and Regulation ~~20(2)(d)~~ 21(3) of the Money Laundering Regulations ~~2007~~ 2017 which requires all firms to appoint a nominated officer.
non-cooperative countries and territories	FATF can designate certain countries and territories as being non-cooperative. This indicates severe weaknesses in anti-money laundering arrangements in those jurisdictions. An up-to-date statement can be found on the FATF website. The JMLSG has prepared guidance for firms on how to judge the risks of conducting business in different countries.
occasional transaction	Any transaction (carried out other than as part of a business relationship) amounting to €15,000 or more, whether the transaction is carried out in a single operation or several operations which appear to be linked. (See Regulation ~~2(1)~~ 27(2) of the Money Laundering Regulations ~~2007~~ 2017.) Any transaction that amounts to a transfer of funds within the meaning of article 3(9) of the Funds Transfer Regulation exceeding €1,000.
ongoing monitoring	The Money Laundering Regulations ~~2007~~ 2017 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.
Office of Financial Sanctions Implementation (OFSI)	The Office of Financial Sanctions Implementation within HM Treasury is responsible for the implementation and administration of the UK sanctions regime. See: https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation for more.
payment institutions	A 'payment institution' is a UK firm which is required under the Payment Services Regulations ~~2009 (SI 2009/209)~~ 2017 (SI 2017/752) to be authorised or registered in order to provide payment services in the UK. This term is not used to describe payment service providers that are already authorised by us because they carry out regulated activities (such as banks and e-money institutions) or that are exempt under the Payment Services Regulations (such as credit unions). For more information, see our publication ~~The FSA's~~

	~~role under the Payment Services Regulations.~~ For the *FCA*'s approach to Payment institutions and e-money institutions under the *Payment Services Regulations 2017* and the *Electronic Money Regulations 2011*, see https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf.
PEP	See 'politically exposed person'.
placement, layering, integration	The three stages in a common model of money laundering. In the placement stage, money generated from criminal activity (e.g. funds from the illegal import of narcotics) is first introduced to the financial system. The layering phase sees the launderer entering into a series of transactions (e.g. buying, and then cancelling, an insurance policy) designed to conceal the illicit origins of the funds. Once the funds are so far removed from their criminal source that it is not feasible for the authorities to trace their origins, the integration stage allows the funds to be treated as ostensibly 'clean' money.
POCA	See 'Proceeds of Crime Act 2002'.
politically exposed person (PEP)	~~A person entrusted with a prominent public function in a foreign state, an EU institution or an international body; their immediate family members; and known close associates. PEPs are associated with an increased money laundering risk as their position makes them vulnerable to corruption. A formal definition is set out in Regulation 14(5) and Schedule 2 of the Money Laundering Regulations 2007.~~ ~~Business relationships with PEPs must be subject to greater scrutiny. (See also Regulation 14(4) of the Money Laundering Regulations 2007.)~~ A person entrusted with a prominent public function. See Regulation 35 of the Money Laundering Regulations 2017 and Finalised Guidance 'FG17/16: The treatment of politically exposed persons for anti-money laundering purposes' https://www.fca.org.uk/publications/finalised-guidance/fg17-6-treatment-politically-exposed-persons-peps-money-laundering.
Ponzi and pyramid schemes	Ponzi and pyramid schemes promise investors high returns or dividends not usually available through traditional investments. While they may meet this promise to early investors, people who invest in the scheme later usually lose their money; these schemes collapse when the unsustainable supply of new investors dries up. Investors usually find most or all of their money is gone, and the fraudsters who set up the scheme ~~claimed~~ have disappeared.

Proceeds of Crime Act 2002 (POCA)	POCA criminalises all forms of money laundering and creates other offences such as failing to report a suspicion of money laundering and 'tipping off'.	
Production Order	The Proceeds of Crime Act 2002 allows Financial Investigators to use production orders to obtain information from financial firms about an individual's financial affairs.	
Proliferation finance	Funding the proliferation of weapons of mass destruction in contravention of international law.	
pyramid schemes	See 'Ponzi and pyramid schemes'.	
Recognised investment exchanges, and recognised clearing houses	To be recognised under FSMA, exchanges and clearing houses must, among other things, adopt appropriate measures to:	
	•	reduce the extent to which their facilities can be used for a purpose connected with market abuse or financial crime; and
	•	monitor the incidence of market abuse or financial crime, and facilitate its detection.
	Measures should include the monitoring of transactions. This is set out in ~~the Recognised Investment Exchanges and Recognised Clearing Houses (*REC*) module of the *Handbook*~~, which contains our guidance on our interpretation of the recognition requirements. It also explains the factors we may consider when assessing a recognised body's compliance with the requirements. ~~The guidance in REC 2.10.4G provides that the Money Laundering Regulations 2007, among other laws, apply to recognised bodies~~ Regulation 7(1)(a)(vii) of the Money Laundering Regulations 2017 confers supervisory functions on the *FCA* to oversee recognised investment exchanges' compliance with requirements imposed on them by those regulations.	
reliance	The Money Laundering Regulations ~~2007~~ 2017 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~~ 39 of the Money Laundering Regulations ~~2007~~ 2017 and the	

	JMLSG guidance for more detail.
safe deposit boxes	The ~~FCA~~ *FCA* is responsible for supervising anti-money laundering controls of safe custody services; this includes the provision of safe deposit boxes.
sanctions	See 'financial sanctions regime'.
SAR	See 'Suspicious Activity Report'.
Senior Management Arrangements, Systems and Controls sourcebook	See ~~'SYSC'~~ '*SYSC*'.
share sale fraud	Share scams are often run from 'boiler rooms' where fraudsters cold-call investors offering them often worthless, overpriced or even non-existent shares. While they promise high returns, those who invest usually end up losing their money. We have found victims of boiler rooms lose an average of £20,000 to these scams, with as much as £200m lost in the UK each year. Even seasoned investors have been caught out, with the biggest individual loss recorded by the police being £6m. We receive almost 5,000 calls each year from people who think they are victims of boiler room fraud. See: ~~www.fsa.gov.uk/consumerinformation/scamsandswindles/investment_scams/boiler_room~~ http://scamsmart.fca.org.uk
simplified due diligence (SDD)	~~The Money Laundering Regulations 2007 allow firms, in certain specific situations which present a low money laundering risk, not to apply customer due diligence measures to their customers and, where applicable, their beneficial owners. See Regulation 13 of the Money Laundering Regulations 2007 for more detail.~~ ~~Applying simplified due diligence does not exempt the firm from the need for ongoing monitoring of the customer relationship, and a firm will have to obtain sufficient information to have a meaningful basis for monitoring. Firms also need to report any suspicious transactions. Also, in practice, firms may have other reasons to satisfy themselves that a customer is who they purport to be: for example, in order to control fraud or credit losses.~~ Regulation 37 of the Money Laundering Regulations 2017 allows firms, where they assess that a business relationship or transaction presents a low degree of risk of money laundering

	or terrorist financing. This regulation sets out a series of factors firms should consider when determining this risk. SDD does not exempt firms from applying CDD measures but permits them to adjust the extent, timing or type of the measures it undertakes to reflect the lower risk it has assessed. A firm is required to carry out sufficient monitoring of any business relationships or transactions which are subject to those measures to enable it to detect any unusual or suspicious transactions.
Solicitors Regulation Authority (SRA)	The Solicitors Regulation Authority has supervisory responsibility for solicitors under the Money Laundering Regulations ~~2007~~ 2017. The Bar Council and other professional bodies for the legal sector perform a similar role for their members. See www.sra.org.uk for more information.
Special Recommendations	See 'FATF Special Recommendations'.
source of funds and source of wealth	'Source of wealth' describes how a customer or beneficial owner acquired their total wealth. 'Source of funds' refers to the origin of the funds involved in the business relationship or occasional transaction. It refers to the activity that generated the funds, for example salary payments or sale proceeds, as well as the means through which the customer's or beneficial owner's funds were transferred.
SRA	See 'Solicitors Regulation Authority'.
STOR	See 'Suspicious Transaction and Order Report'.
Suspicious Activity Report (SAR)	A report made to the NCA about suspicions of money laundering or terrorist financing. This is commonly known as a 'SAR'. See also 'Suspicious Transaction Report'.
Suspicious Transaction and Order Report (STOR)	~~When applied to money laundering reporting, the term 'Suspicious Transaction Report' is used commonly outside of the UK in place of 'Suspicious Activity Report'. Both terms have substantially the same meaning.~~ A report made to the *FCA* in accordance with articles 16(1) and 16(2) of the Markets Abuse Regulation (MAR) about any suspicious order or transaction. For more see: https://www.fca.org.uk/markets/market-abuse/suspicious-transaction-order-reports/stor-supervisory-priorities
~~Suspicious Transaction and~~	~~Following implementation of the Market Abuse Regulation, in the EU the term 'Suspicious Transaction and Order Report'~~

~~Order Report (STOR)~~	~~(STOR) is 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* ~~SYSC~~ is the Senior Management Arrangements, Systems and Controls sourcebook of the ~~Handbook~~ *Handbook*. It sets out the responsibilities of directors and senior management. ~~SYSC~~ *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~~ *SYSC* 6.1.1R, or for insurers, managing agents and Lloyd's, ~~SYSC~~ *SYSC* 3.2.6R). ~~SYSC~~ *SYSC* 6.3 contains anti-money laundering specific rules and guidance. These provisions are also set out in ~~SYSC~~ *SYSC* 3.2.6AR to ~~SYSC~~ *SYSC* 3.2.6JG as they apply to certain insurers, managing agents and Lloyd's. These money laundering specific provisions of ~~SYSC~~ *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 Regulations)~~	~~The Third Money Laundering Directive (2005/60/EC), adopted in 2005, translated the FATF's Recommendations into EC legislation. The UK has implemented this Directive chiefly through the Money Laundering Regulations 2007.~~
third party	'Third party' is a term often used to refer to entities that are involved in a business or other transaction but are neither the firm nor its customer. Where a third party acts on a firm's behalf, it might expose the firm to financial crime risk.
tipping off	The offence of tipping off is committed where a person discloses that:

	•	any person has made a report under the Proceeds of Crime Act 2002 to the Police, HM Revenue and Customs or the NCA concerning money laundering, where that disclosure is likely to prejudice any investigation into the report; or
	•	an investigation into allegations that an offence of money laundering has been committed, is being contemplated or is being carried out.
	See section 333A of the Proceeds of Crime Act 2002. A similar offence exists in relation to terrorism (including terrorism financing) by virtue of section 21D of the Terrorism Act 2000.	
trade sanctions	Government restrictions on the import or export of certain goods and services, often to or from specific countries, to advance foreign policy objectives. See 'economic sanctions'.	
~~Transfer of Funds (Information on the Payer) Regulation 2007~~	~~The Transfer of Funds (Information on the Payer) Regulations 2007 [SI 2007/3298] allow the *FSA* to place penalties on banks that fail to include data about the payer in payment instructions, as is required by the EU Wire Transfer Regulation. See also 'Wire Transfer Regulation'.~~	
Treasury	The Treasury is the UK government's AML policy lead. It also implements the UK's financial sanctions regime through ~~its Asset Freezing Unit~~ OFSI.	
trust or company service provision	A formal legal definition of 'trust or company service provider' is given in ~~Regulation 3(10)~~ Regulation 12(2) of the Money Laundering Regulations ~~2007~~ 2017. 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: ~~http://www.fsa.gov.uk/pages/About/What/financial_crime/money_laundering/3mld/authorised/index.shtml~~ https://www.fca.org.uk/firms/money-laundering-terrorist-financing/reporting Trust or company service providers that are not authorised by us have their anti-money laundering controls supervised by	

	HM Revenue and Customs. More information can be found at its website: ~~www.hmrc.gov.uk/mlr~~ https://www.gov.uk/topic/business-tax/money-laundering-regulations
verification	Making sure the customer or beneficial owner is who they claim to be. ~~The~~ Regulation 28 of the Money Laundering Regulations ~~2007 require~~ 2017 requires the customer's identity ~~to be identified on the basis or reliable and independent information, and the beneficial owner's in a way~~ to be verified on the basis of documents or information in either case obtained from a reliable source which is independent of the person whose identity is being verified. This includes documents issued or made available by an official body even if they are provided or made available to the firm by or on behalf of the customer. It also refers to checking any beneficial owner in a way that the firm is satisfied that it knows who the beneficial owner is; see Regulation 5 of the Money Laundering Regulations ~~2007~~ 2017.
~~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

Annex C

Amendments to the Financial Crime Thematic Reviews (FCTR)

In this Annex, the provisions and subheadings of FCTR listed in column (1) are renumbered and revised as set out in Column (2) of the following tables. Cross-references throughout FCTR are amended accordingly.

Old heading and numbering	New heading and numbering
1. Introduction	1. Introduction
	1.1 What is the *FCTR*?
1.1	1.1.1
1.2	1.1.2
1.3	1.1.3
1.4	1.1.4
2. Firms' high-level management of fraud risk (2006)	2. Firms' high-level management of fraud risk (2006)
	2.1 Introduction
	2.1.1
2.1.	2.1.2
2.2.	2.1.3
2.3	2.1.4
2.4	2.1.5
	2.2 The ~~FSA~~ *FSA's* findings
2.5	2.2.1
	2.3 Consolidated examples of good and poor practice
2.6	2.3.1
3. Review of private banks' anti-money laundering systems and controls (2007)	3. Review of private banks' anti-money laundering systems and controls (2007)
	3.1 Introduction
	3.1.1
3.1	3.1.2
3.2	3.1.3
3.3	3.1.4
3.4	3.1.5
3.5	3.1.6
	3.2 The ~~FSA~~ *FSA's* findings
3.6	3.2.1
	3.3 Consolidated examples of good and poor practice
3.7	3.3.1
4. Automated Anti-Money Laundering Transaction Monitoring Systems (2007)	4. Automated Anti-Money Laundering Transaction Monitoring Systems (2007)

Old heading and numbering	New heading and numbering
	4.1 Introduction
	4.1.1
	4.1.2
4.1	4.1.3
4.2	4.1.4
4.3	4.1.5
4.4	4.1.6
	4.2 The ~~FSA~~ *FSA's* findings
4.5	4.2.1
	4.3 Consolidated examples of good and poor practice
	4.3.1
Box 4.1	4.3.2
5. Review of firms' implementation of a risk-based approach to anti-money laundering (AML) (2008)	5. Review of firms' implementation of a risk-based approach to anti-money laundering (AML) (2008)
	5.1 Introduction
	5.1.1
5.1	5.1.2
5.2	5.1.3
5.3	5.1.4
5.4	5.1.5
	5.2 The ~~FSA~~ *FSA's* findings
4.5 (sic)	5.2.1
	5.3 Consolidated examples of good and poor practice
Box 5.1	5.3.1
6. Data security in Financial Services (2008)	6. Data security in Financial Services (2008)
	6.1 Introduction
	6.1.1
6.1	6.1.2
6.2	6.1.3
6.3	6.1.4
6.4	6.1.5
	6.2 The ~~FSA~~ *FSA's* findings
6.5	6.2.1
	6.3 Consolidated examples of good and poor practice
Box 6.1	6.3.1
Box 6.2	6.3.2
Box 6.3	6.3.3
Box 6.4	6.3.4
Box 6.5	6.3.5
Box 6.6	6.3.6
Box 6.7	6.3.7
Box 6.8	6.3.8
Box 6.9	6.3.9

Old heading and numbering	New heading and numbering
Box 6.10	6.3.10
Box 6.11	6.3.11
Box 6.12	6.3.12
Box 6.13	6.3.13
Box 6.14	6.3.14
Box 6.15	6.3.15
7. Review of financial crime controls in offshore centres (2008)	7. Review of financial crime controls in offshore centres (2008)
	7.1 Introduction
	7.1.1
7.1	7.1.2
7.2	7.1.3
7.3	7.1.4
7.4	7.1.5
	7.2 The ~~FSA~~ *FSA's* findings
7.5	7.2.1
	7.3 Consolidated examples of good and poor practice
7.6	7.3.1
8. Financial services firms' approach to UK financial sanctions	8. Financial services firms' approach to UK financial sanctions
	8.1 Introduction
	8.1.1
8.1	8.1.2
8.2	8.1.3
8.3	8.1.4
8.4	8.1.5
	8.2 The ~~FSA~~ *FSA's* findings
	8.2.1
	8.3 Consolidated examples of good and poor practice
Box 8.1	8.3.1
Box 8.2	8.3.2
Box 8.3	8.3.3
Box 8.4	8.3.4
Box 8.5	8.3.5
Box 8.6	8.3.6
Box 8.7	8.3.7
9. Anti-bribery and corruption in commercial insurance broking (2010)	9. Anti-bribery and corruption in commercial insurance broking (2010)
	9.1 Introduction
	9.1.1
9.1	9.1.2

Old heading and numbering	New heading and numbering
9.2	9.1.3
9.3	9.1.4
9.4	9.1.5
9.5	9.1.6
	9.2 The ~~FSA~~ *FSA's* findings
9.6	9.2.1
	9.3 Consolidated examples of good and poor practice
Box 9.1	9.3.1
Box 9.2	9.3.2
Box 9.3	9.3.3
Box 9.4	9.3.4
Box 9.5	9.3.5
Box 9.6	9.3.6
Box 9.7	9.3.7
Box 9.8	9.3.8
Box 9.9	9.3.9
10. The Small Firms Financial Crime Review (2010)	10. The Small Firms Financial Crime Review (2010)
	10.1 Introduction
	10.1.1
10.1	10.1.2
10.2	10.1.3
10.3	10.1.4
10.4	10.1.5
10.5	10.1.6
10.6	10.1.7
	10.2 The ~~FSA~~ *FSA's* findings
10.7	10.2.1
	10.3 Consolidated examples of good and poor practice
Box 10.1	10.3.1
Box 10.2	10.3.2
Box 10.3	10.3.3
Box 10.4	10.3.4
Box 10.5	10.3.5
Box 10.6	10.3.6
Box 10.7	10.3.7
Box 10.8	10.3.8
Box 10.9	10.3.9
Box 10.10	10.3.10
Box 10.11	10.3.11
Box 10.12	10.3.12
Box 10.13	10.3.13

Old heading and numbering	New heading and numbering
Box 10.14	10.3.14
Box 10.15	10.3.15
Box 10.16	10.3.16
Box 10.17	10.3.17
11. Mortgage fraud against lenders (2011)	11. Mortgage fraud against lenders (2011)
	11.1 Introduction
	11.1.1
11.1	11.1.2
11.2	11.1.3
11.3	11.1.4
	11.2 The ~~FSA~~ *FSA's* findings
11.4	11.2.1
	11.3 Consolidated examples of good and poor practice
Box 11.1	11.3.1
Box 11.2	11.3.2
Box 11.3	11.3.3
Box 11.4	11.3.4
Box 11.5	11.3.5
Box 11.6	11.3.6
Box 11.7	11.3.7
Box 11.8	11.3.8
12. Banks' management of high money-laundering risk situations (2011)	12. Banks' management of high money-laundering risk situations (2011)
	12.1 Introduction
	12.1.1
12.1	12.1.2
12.2	12.1.3
12.3	12.1.4
12.4	12.1.5
	12.2 The ~~FSA~~ *FSA's* findings
12.5.	12.2.1
	12.3 Consolidated examples of good and poor practice
12.6	12.3.1
Box 12.1	12.3.2
Box 12.2	12.3.3
Box 12.3	12.3.4
Box 12.4	12.3.5
Box 12.5	12.3.6
Box 12.6	12.3.7
Box 12.7	12.3.8

Old heading and numbering	New heading and numbering
Box 12.8	12.3.9
Box 12.9	12.3.10
Box 12.10	12.3.11
Box 12.11	12.3.12
13. Anti-bribery and corruption systems and controls in investment banks (2012)	13. Anti-bribery and corruption systems and controls in investment banks (2012)
	13.1 Introduction
	13.1.1
13.1	13.1.2
13.2	13.1.3
13.3	13.1.4
	13.2 The ~~FSA~~ *FSA's* findings
13.4	13.2.1
	13.3 Consolidated examples of good and poor practice
13.5	13.3.1
Box 13.1	13.3.2
Box 13.2	13.3.3
Box 13.3	13.3.4
Box 13.4	13.3.5
Box 13.5	13.3.6
Box 13.6	13.3.7
Box 13.7	13.3.8
Box 13.8	13.3.9
Box 13.9	13.3.10
Box 13.10	13.3.11
14. Banks' defences against investment fraud (2012)	14. Banks' defences against investment fraud (2012)
	14.1 Introduction
	14.1.1
14.1	14.1.2
14.2	14.1.3
14.3	14.1.4
	14.2 The ~~FSA~~ *FSA's* findings
14.4	14.2.1
	14.3 Consolidated examples of good and poor practice
14.5	14.3.1
Box 14.1	14.3.2
Box 14.2	14.3.3
Box 14.3	14.3.4
Box 14.4	14.3.5

Old heading and numbering	New heading and numbering
Box 14.5	14.3.6
Box 14.6	14.3.7
Box 14.7	14.3.8
Box 14.8	14.3.9
15. Banks' control of financial crime risks in trade finance (2013)	15. Banks' control of financial crime risks in trade finance (2013)
	15.1 Introduction
	15.1.1
15.1	15.1.2
15.2	15.1.3
15.3	15.1.4
	15.2 The ~~FSA~~ *FSA's* findings
15.4	15.2.1
	15.3 Consolidated examples of good and poor practice
Box 15.1	15.3.1
Box 15.2	15.3.2
Box 15.3	15.3.3
Box 15.4	15.3.4
Box 15.5	15.3.5
Box 15.6	15.3.6
Box 15.7	15.3.7
Box 15.8	15.3.8
16. How small banks manage money laundering and sanctions risk – update (2014)	16. How small banks manage money laundering and sanctions risk – update (2014)
	16.1 Introduction
	16.1.1
16.1.	16.1.2
16.2	16.1.3
16.3.	16.1.4
	16.2 The ~~FCA~~ *FCA's* findings
16.4	16.2.1
	16.3 Themes
Box 16.1	16.3.1
Box 16.2	16.3.2
Box 16.3	16.3.3
Box 16.4	16.3.4
Box 16.5	16.3.5
Box 16.6	16.3.6
Box 16.7	16.3.7
17. Managing bribery and corruption risk in commercial insurance broking – update (2014)	17. Managing bribery and corruption risk in commercial insurance broking – update (2014)

Old heading and numbering	New heading and numbering
	17.1 Introduction
	17.1.1
17.1	17.1.2
17.2	17.1.3
17.3	17.1.4
	17.2 The ~~FCA~~ *FCA's* findings
17.4	17.2.1
	17.3 Themes
Box 17.1	17.3.1
Box 17.2	17.3.2
Box 17.3	17.3.3
Box 17.4	17.3.4
Box 17.5	17.3.5
Box 17.6	17.3.6
Box 17.7	17.3.7

Amend the following as shown. Underlining indicates new text and striking through indicates deleted text.

Financial Crime Thematic Reviews (FCTR)

1 Introduction

1.1 What is the *FCTR*?

1.1.1 ~~Part 2 of *Financial Crime: a guide for firms*~~*FCTR* contains summaries of, and links to, 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~~ *FCG*.

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

1.1.3 As with ~~Part 1~~ *FCG*, ~~Part 2~~ *FCTR* contains guidance on ~~Handbook~~ *Handbook* rules and principles, particularly:

- ~~SYSC~~ *SYSC* 3.2.6R and ~~SYSC~~ *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* 2.1A.3R and the conduct rules set out in *COCON* 2.1 and 2.2; and
- in relation to guidance on money laundering, the rules in ~~SYSC~~ *SYSC* 3.2.6AR to ~~SYSC~~ *SYSC* 3.2.6JG and ~~SYSC~~ *SYSC* 6.3 (Financial crime)

~~*FCTR* 4, 5, and 12 also contain guidance on how firms can meet the requirements of the Money Laundering Regulations 2007; *FCTR* 12 also contains guidance on the EU Wire Transfer Regulation. See EU Regulation 1781/2006 on information on the payer. See *FCG* Annex 1 for more information.~~

1.1.4 Not all thematic reviews contain consolidated examples of good and poor practice. All reports do, however, discuss what the ~~FSA~~ *FSA* found about the practices in place at the firms it 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. Firms should consider whether information in historic thematic reviews in *FCTR* relating to the Money Laundering Regulations 2007 remain relevant for the Money Laundering Regulations 2017.

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

2.1 Introduction

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

2.1.2 In February 2006 the ~~FSA~~ *FSA* reviewed a sample of 16 firms (predominantly larger financial services groups) to assess how firms' senior management were managing fraud risk.

2.1.3 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.

2.1.4 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.

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

2.2 The ~~FSA~~ *FSA's* findings

2.2.1 You can read the findings of the ~~FSA~~ *FSA*'s thematic review here: http://www.fsa.gov.uk/pubs/other/fraud_risk.pdf

2.3 Consolidated examples of good and poor practice

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

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

3.1 Introduction

3.1.1 **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~~ 2017.

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

3.1.3 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).

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

3.1.5 Overall the ~~FSA~~ *FSA* 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.

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

3.2 The ~~FSA~~ *FSA's* findings

3.2.1 You can read the findings of the ~~FSA~~ *FSA*'s thematic review here: http://www.fsa.gov.uk/pubs/other/fraud_risk.pdf

3.3 Consolidated examples of good and poor practice

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

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

4.1 Introduction

4.1.1 **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~~ 2017.

4.1.2 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.

4.1.3 The ~~FSA~~ *FSA* 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.

4.1.4 The report explains that the ~~FSA~~ *FSA* 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.

4.1.5 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.

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

4.2 The *FSA's* findings

4.2.1 You can read the findings of the ~~FSA~~ *FSA*'s thematic review here: http://www.fsa.gov.uk/pubs/other/money_laundering/aml_system.pdf

4.3 Consolidated examples of good and poor practice

4.3.1 This report contained the following Examples of good practice:

4.3.2 Statement of good practice

- Depending on the nature and scale of a firm's business activities, automated AML TM 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 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 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)

5.1 Introduction

5.1.1 **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~~ 2017.

5.1.2 In March 2008 the ~~FSA~~ *FSA* 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)~~ (*SYSC*) of the ~~Handbook~~ *Handbook*.

5.1.3 The ~~FSA~~ *FSA* 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.

5.1.4 Due to the wide range of firms the ~~FSA~~ *FSA* 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. The ~~FSA~~ *FSA* also recognised that smaller firms, which generally represent lower risk, had fewer resources to devote to money laundering risk assessment and mitigation.

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

5.2 The ~~FSA~~ *FSA's* findings

5.2.1 You can read the findings of the ~~FSA~~ *FSA*'s thematic review here: http://www.fsa.gov.uk/pubs/other/jmlsg_guidance.pdf

5.3 Consolidated examples of good and poor practice

5.3.1 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;	•	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

	Cs every two years; and Ds and Es are reviewed annually. For lower risk (A-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.		procedures provided that the Compliance Officer or MLRO (Money Laundering Reporting Officer. See ~~Part 1~~ *FCG* Annex 1 for common terms) 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.
•	One building society undertook a comprehensive policy review following the publication of the 2006 JMLSG (Joint Money Laundering Steering Group. See ~~Part 1~~ *FCG* Annex 1 for common terms) 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	•	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 (Suspicious Activity Report. See ~~Part 1~~*FCG* Annex 1 for common terms) process for possible deficiencies.

	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 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~~ *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~~ *SYSC*/JMLSG changes proved to be a catalyst for the bank establishing more organised MI and a Group-level Financial Risk Committee to consider	•	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.

	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 what impact this constant 'drip feed' of training had on suspicious activity reporting. At the time of the ~~FSA~~ *FSA*'s 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.	•	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 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.

6 Data security in Financial Services (2008)

6.1 Introduction

6.1.1 **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~~ *SYSC* 3.2.6R or ~~SYSC~~ *SYSC* 6.1.1R and to **e-money institutions** and **payment institutions** within our supervisory scope.

6.1.2 In April 2008 the ~~FSA~~ *FSA* 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. The ~~FSA~~ *FSA* visited 39 firms, including retail and wholesale banks, investment firms, insurance companies, financial advisers and credit unions. The ~~FSA~~ *FSA* 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.

6.1.3 The ~~FSA~~ *FSA* 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, the ~~FSA~~ *FSA* found that data security in financial services firms needed to be improved significantly.

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

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

6.2 The ~~FSA~~ *FSA's* findings

6.2.1 You can read the findings of the ~~FSA~~ *FSA*'s thematic review here: http://www.fsa.gov.uk/pubs/other/data_security.pdf

6.3 Consolidated examples of good and poor practice

6.3.1 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.	•	Treating data security as an IT issue and failing to involve other key staff from across the business in the risk assessment process.
•	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.	•	No written policies and procedures on data security.
•	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	•	Firms do not understand the need for knowledge-sharing on data security.

	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.	•	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.
•	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 security concerns and data loss without fear of blame or recrimination.	•	A 'blame culture' that discourages staff from reporting data security concerns and data losses.
•	Firms seeking external assistance if they feel they do not have the necessary expertise to complete a data security risk assessment themselves.	•	Failure to notify customers affected by data loss in case the details are picked up by the media
•	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.		

6.3.2 Training and awareness

Examples of good practice		Examples of poor 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.	•	No training to communicate policies and procedures.
•	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.	•	Managers assuming that employees understand data security risk without any training.
•	Simple, memorable and easily digestible guidance for staff on good data security practice.	•	Data security policies which are very lengthy, complicated and difficult to read.
•	Testing of staff understanding of data security policies on induction and once a year after that.	•	Reliance on staff signing an annual declaration stating that they have read policy documents without any further testing.
•	Competitions, posters, screensavers and group discussion to raise interest in the subject.	•	Staff being given no incentive to learn about data security.

6.3.3 Staff recruitment and vetting

Examples of good practice		Examples of poor practice	
•	Vetting staff on a risk-based approach, taking into account data security and other fraud risk.	•	Allowing new recruits to access customer data before vetting has been completed.
•	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	•	Temporary staff receiving less rigorous vetting than permanently employed colleagues carrying out similar roles.

	amounts of customer data.		
•	Liaison between HR and Financial Crime to ensure that financial crime risk indicators are considered during the vetting process.	•	Failing to consider continually whether staff in higher-risk positions are becoming vulnerable to committing fraud or being coerced by criminals.
•	A good understanding of vetting conducted by employment agencies for 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.		

6.3.4 Controls – Access rights

Examples of good practice		Examples of poor 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.	•	Staff having access to customer data that they do not require 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.	•	User access rights set up on a case-by-case basis with no independent check that they are appropriate.
•	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.	•	Failing to consider continually whether staff in higher-risk positions are becoming vulnerable to committing fraud or being coerced by criminals.

•	Regular reviews of staff IT access rights to ensure that there are no anomalies.	•	User accounts being left 'live' or only suspended (i.e. not permanently disabled) when a staff member leaves.
•	Least privilege' access to call recordings and copies of scanned documents obtained for 'know your customer' purposes.	•	A lack of independent check of changes effected at any stage in the joiners, movers and leavers process.
•	Authentication of customers' identities using, for example, touch-tone telephone before a conversation with a call centre adviser takes place. This limits the amount 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.		

6.3.5 Controls – passwords and user accounts

Examples of good practice		Examples of poor practice	
•	Individual user accounts – requiring passwords – in place for all systems containing customer data.	•	The same user account and password used by multiple users to access particular systems.
•	Password standards at least equivalent to those recommended by Get Safe Online – a government-backed campaign group. In July 2011, their recommended standard for passwords was a combination of letters, numbers and keyboard symbols at least eight characters in length and	•	Names and dictionary words used as passwords.

	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.	•	Systems that allow passwords to be set which do not comply with password policy.
•	'Straight-through processing', but only if complemented by accurate role-based access profiles and strong passwords.	•	Individuals share passwords.

6.3.6 Controls – monitoring access to customer data

Examples of good practice		Examples of poor practice	
•	Risk-based, proactive monitoring of staff's access to customer data to ensure it is being accessed and/or updated for a genuine business reason.	•	Assuming that vetted staff with appropriate access rights will always act appropriately. Staff can breach procedures, for example by looking at account information relating to celebrities, be tempted to commit fraud themselves or be bribed or threatened to give customer data to criminals.
•	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.	•	Names and dictionary words used as passwords.
•	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.	•	Failing to monitor superusers or other employees with access to large amounts of customer data.

6.3.7 Controls – data back-up

Examples of good practice		Examples of poor 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 failing to consider data security risk arising from the backing up of customer data.
•	Firms encrypting backed-up data that is held off-site, including while in transit.	•	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.
•	Regular reviews of the level of encryption to ensure it remains appropriate to the current risk environment.	•	Unrestricted access to back-up tapes for large numbers of staff at third party firms.
•	Back-up data being transferred by secure Internet links.	•	Back-up tapes being held insecurely by firm's employees; for example, being left in their cars or at home on the kitchen table.
•	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, 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 in accordance with accepted policies and procedures.		

6.3.8 Controls – access to the internet and email

Examples of good practice		Examples of poor practice	
•	Giving internet and email access only to staff with a genuine business need.	•	Allowing staff who handle customer data to have access to the internet and email if there is no business reason for this.
•	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.	•	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.
•	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.		

6.3.9 Controls – key-logging devices

Examples of good practice		Examples of poor practice	
•	Regular sweeping for key-		

	logging devices in parts of the firm where employees have access to large amounts of, or sensitive, 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.		

6.3.10 Controls – laptop

Examples of good practice		Examples of poor practice	
•	The encryption of laptops and other portable devices containing customer data.	•	Unencrypted customer data on laptops.
•	Controls that mitigate the risk of employees failing to follow policies and procedures. The ~~FSA~~ *FSA* has dealt with several cases of lost or stolen laptops that arose from firms' staff not doing what they should.	•	A poor understanding of which employees have been issued or are using laptops to hold customer data.
•	Maintaining an accurate register of laptops issued to staff.	•	Shared laptops used by staff without being signed out or wiped between uses.
•	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.		

6.3.11 Controls – portable media including USB devices and CDs

Examples of good practice		Examples of poor practice	
•	Ensuring that only staff with a genuine business need can download customer data to portable media such as USB devices and CDs.	•	Allowing staff with access to bulk customer data – for example, superusers – to download to unencrypted portable media.
•	Ensuring that staff authorised to hold customer data on portable media can only do so if it is encrypted.	•	Failing to review regularly threats posed by increasingly sophisticated and quickly evolving personal technology such as mobile phones.
•	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.		

6.3.12 Controls – Physical security

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

6.3.13 Controls – 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.	•	Poor awareness among staff about how to dispose of customer data securely.
•	Treating all paper as 'confidential waste' to eliminate confusion among employees about which type of bin to use.	•	Slack procedures that present opportunities for fraudsters, for instance when confidential waste is left unguarded on the premises before it is destroyed.
•	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.	•	Staff working remotely failing to dispose of customer data securely.
•	Checking general waste bins for the accidental disposal of customer data.	•	Firms failing to provide guidance or assistance to remote workers who need to dispose of an obsolete home computer.
•	Using a third party supplier, preferably one with BSIA (British Security Industry Association) 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.	•	Firms stockpiling obsolete computers and other portable media for too long and in insecure environments.
•	Providing guidance for travelling or home-based staff on the secure disposal of customer data.	•	Firms relying on others to erase or destroy their hard drives and other portable media securely without evidence that this has been done competently.
•	Computer hard drives and portable media being properly wiped (using specialist software) or destroyed as soon		

	as they become obsolete.		

6.3.14 Managing third-party suppliers

Examples of good practice		Examples of poor practice	
•	Conducting due diligence of data security standards at third-party suppliers before contracts are agreed.	•	Allowing third-party suppliers to access customer data when no due diligence of data security arrangements has been performed.
•	Regular reviews of third-party suppliers' data security systems and controls, with the frequency of review dependent on data security risks identified.	•	Firms not knowing exactly which third-party staff have access to their customer data.
•	Ensuring third-party suppliers' vetting standards are adequate by testing the checks performed on a sample of staff with access to customer data.	•	Firms not knowing how third-party suppliers' staff have been vetted.
•	Only allowing third-party IT suppliers access to customer databases for specific tasks on a case- by-case basis.	•	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.
•	Third-party suppliers being subject to procedures for reporting data security breaches within an agreed timeframe.	•	Allowing IT suppliers unrestricted or unmonitored access to customer data.
•	The use of secure internet links to transfer data to third parties.	•	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.

6.3.15 Internal audit and compliance monitoring

Examples of good practice	Examples of poor practice

•	Firms seeking external assistance where they do not have the necessary in-house expertise or resources.	•	Compliance focusing only on compliance with data protection legislation and failing to consider adherence to data security policies and procedures.
•	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.	•	Compliance consultants adopting a 'one size fits all' approach to different clients' businesses.
•	Firms using expertise from across the business to help with the more technical aspects of data security audits and compliance monitoring.		

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

7.1 Introduction

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

- **all firms** subject to the financial crime rules in ~~SYSC~~ *SYSC* 3.2.6R or ~~SYSC~~ *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.

7.1.2 In the second half of 2008 the ~~FSA~~ *FSA* 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 the ~~FSA~~ *FSA's* report into data security in financial services (April 2008 – http://www.fsa.gov.uk/pubs/other/data_security.pdf).

7.1.3 The main financial crime risks the ~~FSA~~ *FSA* 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'.

7.1.4 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.

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

7.2 The *FSA's* findings

7.2.1 You can read the findings of the ~~FSA~~ *FSA*'s thematic review here: http://www.fsa.gov.uk/pages/About/What/financial_crime/library/reports/review_offshore.shtml

7.3 Consolidated examples of good and poor practice

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

8 Financial services firms' approach to UK financial sanctions

8.1 Introduction

8.1.1 **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~~ *SYSC* 3.2.6R or ~~SYSC~~ *SYSC* 6.1.1R and to e-money institutions and payment institutions within our supervisory scope.

8.1.2 In April 2009 the ~~FSA~~ *FSA* published the findings of our thematic review of firms' approach to UK financial sanctions. The ~~FSA~~ *FSA* 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. The ~~FSA~~ *FSA* then selected a sub-sample of 25 firms to visit to substantiate the findings from the surveys.

8.1.3 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. The ~~FSA~~ *FSA* 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, the ~~FSA~~ *FSA* found a widespread lack of awareness of the UK financial sanctions regime.

8.1.4 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. The ~~FSA~~ *FSA* 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. The ~~FSA~~ *FSA* also had concerns about firms' screening of clients, both initially and as an ongoing process.

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

8.2 The ~~FSA~~ *FSA's* findings

8.2.1 You can read the findings of the ~~FSA~~ *FSA*'s thematic review here: http://www.fsa.gov.uk/pubs/other/Sanctions_final_report.pdf

8.3 Consolidated examples of good and poor practice

8.3.1 Senior management responsibility

Examples of good practice		Examples of poor practice	
•	Senior management involvement in approving and taking responsibility for policies and procedures.	•	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.
•	A level of senior management awareness of the firm's obligations regarding financial sanctions sufficient to enable them to discharge their functions effectively.	•	No, or insufficient, management oversight of the day-to-day operation of systems and controls.
•	Appropriate escalation in cases where a potential target match cannot easily be verified.	•	Failure to included assessments of the financial sanctions systems and controls as a normal part of internal audit programmes.
•	Adequate and appropriate resources allocated by senior management.	•	No senior management involvement in any cases where a potential target match cannot easily be verified.
•	Appropriate escalation of actual target matches and breaches of UK financial sanctions.	•	Senior management never being made aware of a target match or breach of sanctions for an existing customer.
		•	Failure to notify customers affected by data loss in case the

			details are picked up by the media.

8.3.2 Risk assessment

Examples of good practice		Examples of poor 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.	•	Not assessing the risks that the firm may face of breaching financial sanctions.
•	Taking into account associated parties, such as directors and beneficial owners.	•	Risk assessments that are based on misconceptions.
•	A formal documented risk assessment with a clearly documented rationale for the approach.		

8.3.3 Policies and procedures

Examples of good practice		Examples of poor 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.	•	No policies or procedures in place for complying with the legal and regulatory requirements of the UK financial sanctions regime.
•	Group-wide policies for UK financial sanctions screening, to ensure that business unit-specific policies and procedures reflect the standard set out in group policy.	•	Internal audits of procedures carried out by persons with responsibility for oversight of financial sanctions procedures, rather than an independent party.
•	Effective procedures to screen against the Consolidated List (See ~~Part 1~~		

	FCG Annex 1 for descriptions of common terms) 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.		

8.3.4 Staff training and awareness

Examples of good practice		Examples of poor practice	
•	Regularly updated training and awareness programmes that are relevant and appropriate for employees' particular roles.	•	No training on financial sanctions.
•	Testing to ensure that employees have a good understanding of financial sanctions risks and procedures.	•	Relevant staff unaware of the firm's policies and procedures to comply with the UK financial sanctions regime.
•	Ongoing monitoring of employees' work to ensure they understand the financial sanctions procedures and are adhering to them.	•	Changes to the financial sanctions policies, procedures, systems and controls are not communicated to relevant staff.

•	Training provided to each business unit covering both the group-wide and business unit-specific policies on financial sanctions.		

8.3.5 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 only on notification of a claim on an insurance policy, rather than during client take-on.
•	Screening against the Consolidated List at the time of client take-on before providing any services or undertaking any transactions for a customer.	•	Relying on other ~~FSA~~ *FSA*-authorised firms and compliance consultants to screen clients against the Consolidated List without taking reasonable steps to ensure that they are doing so effectively.
•	Screening directors and beneficial owners of corporate customers.	•	Assuming that AML customer due diligence checks include screening against the Consolidated List.
•	Screening third party payees where adequate information is available.	•	Failing to screen UK-based clients on the assumption that there are no UK-based persons or entities on the Consolidated List or failure to screen due to any other misconception.
•	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.	•	Large global institutions with millions of clients using manual screening, increasing the likelihood of human error and leading to matches being missed.
•	The use of 'fuzzy matching' where automated screening systems are used.	•	IT systems that cannot flag potential matches clearly and prominently.
•	Where a commercially available automated screening system is	•	Firms calibrating their screening rules too narrowly or too widely so that they, for example, match

	implemented, making sure that there is a full understanding of the capabilities and limits of the system.		only exact names with the Consolidated 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.

8.3.6 Ongoing screening

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

•	Screening systems calibrated in accordance with the firm's risk appetite, rather than the settings suggested by 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.		

8.3.7 Treatment of potential target matches

Examples of good practice		Examples of poor practice	
•	Procedures for investigating whether a potential match is an actual target match or a false positive.	•	No procedures in place for investigating potential matches with the Consolidated List.
•	Procedures for freezing accounts where an actual target match is identified.	•	Discounting actual target matches incorrectly as false positives due to insufficient investigation.
•	Procedures for notifying the Treasury's AFU promptly of any confirmed matches.	•	No audit trail of decisions where potential target matches are judged to be false positives.
•	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.		
•	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.		

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

9.1 Introduction

9.1.1 **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~~ *SYSC* 3.2.6R or ~~SYSC~~ *SYSC* 6.1.1R; and
- **e-money institutions** and **payment institutions** within our supervisory scope.

Except that ~~Box 9.3~~*FCTR* 9.3.3G and ~~Box 9.4~~ *FCTR* 9.3.4G 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~~ *SYSC* 3.2.6R and ~~SYSC~~ *SYSC* 6.1.1R.

9.1.2 In May 2010 the ~~FSA~~ *FSA* 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. The ~~FSA~~ *FSA* visited 17 broker firms. Although this report focused on commercial insurance brokers, the findings are relevant in other sectors.

9.1.3 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.

9.1.4 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.

9.1.5 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. The ~~FSA~~ *FSA* 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.

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

9.2 The ~~FSA~~ *FSA's* findings

9.2.1 You can read the findings of the ~~FSA~~ *FSA*'s thematic review here: http://www.fsa.gov.uk/pubs/anti_bribery.pdf

9.3 Consolidated examples of good and poor practice

9.3.1 Governance and management information

Examples of good practice		Examples of poor 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.	•	Failing to allocate official responsibility for anti-bribery and corruption to a single senior manager or appropriately formed committee.
•	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.	•	A lack of awareness and/or engagement in anti-bribery and corruption at senior management or Board level.
•	Swift and effective senior management-led response to significant bribery and corruption events, which highlight potential areas for improvement in systems and controls.	•	Little or no MI sent to the Board about higher risk third party relationships or payments.
•	Regular MI to the Board and other relevant senior management forums.	•	Failing to include details of wider issues, such as new legislation or regulatory developments in MI.
•	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	•	IT systems unable to produce the necessary MI.

	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 acted on appropriately.		

9.3.2 Risk assessment and responses to significant bribery and corruption events

Examples of good practice		Examples of poor 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.	•	Failing to consider the bribery and corruption risks posed by third parties used to win business.
•	More robust due diligence on and monitoring of higher risk third-party relationships.	•	Failing to allocate formal responsibility for anti-bribery and corruption risk assessments.
•	Thorough reviews and gap analyses of systems and controls against relevant external events, with strong senior management involvement or sponsorship.	•	Little or no MI sent to the Board about higher risk third party relationships or payments.
•	Ensuring review teams have sufficient knowledge of relevant issues and supplementing this with external expertise where necessary.	•	Failing to respond to external events which may draw attention to weaknesses in systems and controls.
•	Establishing clear plans to implement improvements arising from reviews, including updating policies,	•	Taking too long to implement changes to systems and controls after analysing external events.

	procedures and staff training.		
•	Adequate and prompt reporting to SOCA (Serious Organised Crime Agency. See ~~Part 1~~ *FCG* Annex 1 for common terms) and use of any inappropriate payments identified during business practice review.	•	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.

9.3.3 Due diligence on third-party relationships

Examples of good practice		Examples of poor practice	
•	Establishing and documenting policies with a clear definition of a 'third party' and the due diligence required when establishing and reviewing third-party relationships.	•	Failing to carry out or document due diligence on 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.	•	Relying heavily on the informal 'market view' of the integrity of third parties as due diligence.
•	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.	•	Relying on the fact that third-party relationships are longstanding when no due diligence has ever been carried out.
•	Taking reasonable steps to verify the information provided by third parties during the due diligence process.	•	Failing to respond to external events which may draw attention to weaknesses in systems and controls.

•	Using third party forms which ask relevant questions and clearly state which fields are mandatory.	•	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).
•	Having third party account opening forms reviewed and approved by compliance, risk or committees involving these areas.	•	Accepting vague explanations of the business case for using third parties.
•	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.	•	Approvers of third-party relationships working within the broking department or being too close to it to provide adequate challenge.
•	Routinely informing all parties involved in the insurance transaction about the involvement of third parties being paid commission.	•	Accepting instructions from third parties to pay commission to other individuals or entities which have not been subject to due diligence.
•	Ensuring current third-party due diligence standards are appropriate when business is acquired that is higher risk than existing business.	•	Assuming that third-party relationships acquired from other firms have been subject to adequate due diligence.
•	Considering the level of bribery and corruption risk posed by a third party when agreeing the level of commission.	•	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.
•	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.	•	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.
•	Paying commission to third	•	Leaving redundant third-party

	parties on a one-off fee basis where their role is pure introduction.		accounts 'live' on the accounting systems because third-party relationships have not been regularly reviewed.
•	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.	•	Being unable to produce a list of approved third parties, associated due diligence and details of payments made to them.
•	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.		

9.3.4 Payment controls

Examples of good practice		Examples of poor practice	
•	Ensuring adequate due diligence and approval of third-party relationships before payments are made to the third party.	•	Failing to check whether third parties to whom payments are due have been subject to appropriate due diligence and approval.
•	Risk-based approval procedures for payments and a clear understanding of why payments are made.	•	The inability to produce regular third-party payment schedules for review.

•	Checking third-party payments individually prior to approval, to ensure consistency with the business case for that account.	•	Failing to check thoroughly the nature, reasonableness and appropriateness of gifts and hospitality.
•	Regular and thorough monitoring of third-party payments to check, for example, whether a payment is unusual in the context of previous similar payments.	•	No absolute limits on different types of expenditure, combined with inadequate scrutiny during the approvals process.
•	A healthily sceptical approach to approving third-party payments.	•	The giving or receipt of cash gifts.
•	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.		

9.3.5 Staff recruitment and vetting

Examples of good practice		Examples of poor practice	
•	Vetting staff on a risk-based	•	Relying entirely on an

	approach, taking into account financial crime risk.		individual's market reputation or market gossip as the basis for recruiting staff.
•	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.	•	Failing to check thoroughly the nature, reasonableness and appropriateness of gifts and hospitality.
•	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 individual's role or proposed role.	•	Failing to consider on a continuing basis whether staff in higher risk positions are becoming vulnerable to committing fraud or being coerced by criminals.
•	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.	•	Relying on contracts with employment agencies covering staff vetting standards without checking periodically that the agency is adhering to them.
•	Conducting periodic checks to ensure that agencies are complying with agreed vetting standards.	•	Temporary or contract staff receiving less rigorous vetting than permanently employed colleagues carrying out similar roles.
•	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.		

9.3.6 Training and awareness

Examples of good practice		Examples of poor practice	
•	Providing good quality, standard training on anti-	•	Failing to provide training on anti-bribery and corruption,

	bribery and corruption for all staff.		especially to staff in higher risk positions.
•	Additional anti-bribery and corruption training for staff in higher risk positions.	•	Training staff on legislative and regulatory requirements but failing to provide practical examples of how to comply with them.
•	Ensuring staff responsible for training others have adequate training themselves.	•	Failing to ensure anti-bribery and corruption policies and procedures are easily accessible to staff.
•	Ensuring training covers practical examples of risk and how to comply with policies.		Neglecting the need for appropriate staff training in the belief that robust payment controls are sufficient to combat anti-bribery and corruption.
•	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.		

9.3.7 Risk arising from remuneration structures

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

9.3.8 Incident reporting

Examples of good practice		Examples of poor practice	
•	Clear procedures for whistleblowing and reporting suspicions, and communicating these to staff.	•	Failing to report suspicious activity relating to bribery and corruption.
•	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.	•	No clear internal procedure for whistleblowing or reporting suspicions.
•	Respect for the confidentiality of workers who raise concerns.	•	No alternative reporting routes for staff wishing to make a whistleblowing disclosure about their line management or senior managers.
•	Internal and external suspicious activity reporting procedures in line with the Joint Money Laundering Steering Group guidance.	•	A lack of training and awareness in relation to whistleblowing the reporting of suspicious activity.
•	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.		

9.3.9 The role of compliance and internal audit

Examples of good practice		Examples of poor practice	
•	Compliance and internal audit staff receiving specialist training to achieve a very good knowledge of bribery and corruption risks.	•	Failing to carry out compliance or internal audit work on anti-bribery and corruption.
•	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.	•	Compliance, in effect, signing off their own work, by approving new third party accounts and carrying out compliance monitoring on the same accounts.
•	Independent checking of compliance's operational role in approving third party relationships and accounts, where relevant.	•	Compliance and internal audit not recognising or acting on the need for a risk-based approach.
•	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.		

10 The Small Firms Financial Crime Review (2010)

10.1 Introduction

10.1.1 **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~~ *SYSC* 3.2.6R or ~~SYSC~~ *SYSC* 6.1.1R and small **e-money institutions** and **payment institutions** within our supervisory scope.

10.1.2 In May 2010 the ~~FSA~~ *FSA* published the findings of its 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~~ *FSA*.

10.1.3 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.

10.1.4 The ~~FSA~~ *FSA* found that firms generally demonstrated a reasonable awareness of their obligations, particularly regarding AML systems and controls. But it found weaknesses across the sector regarding the implementation of systems and controls put in place to reduce firms' broader financial crime risk.

10.1.5 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.

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

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

10.2 The *FSA's* findings

10.2.1 You can read the findings of the ~~FSA~~ *FSA*'s thematic review here: http://www.fsa.gov.uk/smallfirms/pdf/financial_crime_report.pdf

10.3 Consolidated examples of good and poor practice

10.3.1 Regulatory/Legal obligations

Examples of good practice		Examples of poor 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.	•	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.
•	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.		

10.3.2 Account opening procedures

Examples of good practice		Examples of poor 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.	•	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.

10.3.3 Monitoring activity

Examples of good practice		Examples of poor 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 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.		

10.3.4 Suspicious activity reporting

Examples of good practice		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 he should carry on as normal and just report it as a SAR to SOCA.

10.3.5 Records

Examples of good practice		Examples of poor 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 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 (We expect that KYC information should be kept together in the file so that it is easily identifiable and auditable.)
•	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.		

10.3.6 Training

Examples of good practice		Examples of poor 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.	•	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.
•	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.	•	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.

10.3.7 Responsibilities and risk assessments

Examples of good practice		Examples of poor practice	
•	At an IFA there was a clearly documented policy on data security which staff were tested on annually. The policy contained, but was not limited to, details around clear desks, non-sharing of passwords, the	•	At an IFA, a risk assessment had been undertaken by the firm's compliance consultant but the firm demonstrated no real appreciation of the financial crime risks in its business. The risk assessment was not tailored to 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.		risks inherent in that business.
•	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~~ *FSA* in April 2008.	•	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.
•	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.		

10.3.8 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.	•	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.
•	A discretionary investment manager conducted five year	•	In an advising-only intermediary, staff set their own systems

	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. There were role profiles for each job within the firm and these were reviewed monthly for accuracy.		passwords which had no defined length or complexity and were only changed every six months.
•	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.		

10.3.9 Outsourcing

Examples of good practice		Examples of poor 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 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 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.	•	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.

•	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, 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, unauthorised data access attempts by staff were monitored by the IT manager and email alerts sent to staff and management when identified.	•	In an authorised professional firm there had been two incidents where people had walked into the office and stolen staff wallets and laptops.
•	In a general insurance intermediary the two directors had recently visited the offsite data storage facility to satisfy themselves about the security arrangements at the premises.		

10.3.10 Physical controls

Examples of good practice		Examples of poor 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.	•	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.
•	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.		

10.3.11 Data disposal

Examples of good practice		Examples of poor 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.	•	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.
•	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 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.		

10.3.12 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.

10.3.13 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.	•	One GI broker 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.
•	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 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 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.		

10.3.14 Insurance fraud

Examples of good practice		Examples of poor practice	
•	A small general insurer had compiled a handbook which detailed indicators of potential insurance fraud.	•	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.
•	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.		

10.3.15 Investment fraud

Examples of good practice		Examples of poor practice	
•	An IFA had undertaken a risk assessment for all high net worth customers.	•	An IFA had a 'one size fits all' approach to identifying the risks associated with customers and investments.
•	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.		

10.3.16 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 (Customer Due Diligence. See ~~Part 1~~ *FCG* Annex 1 for common terms), including source of funds information, was also obtained early in the application process before the application was completed and submitted to the lender.	•	An IFA did not undertake any KYC checks, considering this to be the responsibility of the lender.
•	A home finance broker would	•	An IFA did not investigate source

	not conduct any remote business – meeting all customers face-to-face.		of funds. The firm stated this was because ‘a bank would pick it up and report it.’
•	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 extra verification of its non face-to-face customers.

10.3.17 Staff/Internal fraud

Examples of good practice		Examples of poor 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.	•	One general insurance intermediary did not undertake any background checks before appointing a member of staff or authenticate qualifications or references.
•	An IFA ensured that staff vetting is repeated by completing a credit reference check on each member of staff.	•	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.
•	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.		

11 Mortgage fraud against lenders (2011)

11.1 Introduction

11.1.1 **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~~ *SYSC* 3.2.6R or ~~SYSC~~ *SYSC* 6.1.1R.

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

11.1.3 The ~~FSA~~ *FSA*'s 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, the ~~FSA~~ *FSA* found that many in the industry could do better; the ~~FSA~~ *FSA* were disappointed, for example, that more firms were not actively participating in the ~~FSA~~ *FSA*'s Information From Lenders scheme and other industry-wide initiatives to tackle mortgage fraud. Other areas of concern the ~~FSA~~ *FSA* 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 the ~~FSA~~ *FSA* identified scope for significant improvement in the way lenders dealt with third parties such as brokers, valuers and conveyancers.

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

11.2 The ~~FSA~~ *FSA's* findings

11.2.1 You can read the findings of the ~~FSA~~ *FSA*'s thematic review here: http://www.fsa.gov.uk/pubs/other/mortgage_fraud.pdf

11.3 Consolidated examples of good and poor practice

11.3.1 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.	•	A firm fails to report relevant information to the Information From Lenders scheme as per the guidance on IFL referrals.

•	Senior management engage with mortgage fraud risks and receive sufficient management information about incidents and trends.	•	A firm fails to define mortgage fraud clearly, undermining efforts to compile statistics related to mortgage fraud trends.
•	A firm engages in cross-industry efforts to exchange information about fraud risks.	•	A firm does not allocate responsibility for countering mortgage fraud clearly within the management hierarchy.
•	A firm engages front-line business areas in anti-mortgage fraud initiatives.		

11.3.2 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.	•	A firm's underwriters have a poor understanding of potential fraud indicators, whether through inexperience or poor training.
•	Underwriters can contact all parties to the application process (customers, brokers, valuers etc.) to clarify aspects of the application.	•	Underwriters' demanding work targets undermine efforts to contain mortgage fraud.
•	The firm verifies that deposit monies for a mortgage transaction are from a legitimate source.	•	A firm does not allocate responsibility for countering mortgage fraud clearly within the management hierarchy.
•	New or inexperienced underwriters receive training about mortgage fraud risks, potential risk indicators, and the firm's approach to tackling the issue.	•	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.

11.3.3 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 new areas of the mortgage market (such as sub-prime or buy-to-let).	•	A firm's anti-fraud efforts are uncoordinated and under-resourced.
•	A firm reviews existing mortgage books to identify fraud indicators.	•	Fraud investigators lack relevant experience or knowledge of mortgage fraud issues, and have received insufficient training.
•	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's internal escalation procedures are unclear and leave staff confused about when and how to report their concerns about mortgage fraud.
•	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.		

11.3.4 Managing relationships with 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 firm's scrutiny of third parties is a one-off exercise; membership of a panel is not subject to ongoing review.
•	A third party reinstated to a panel after termination is subject to fresh due diligence checks.	•	A firm's panels are too large to be manageable. No work is undertaken to identify dormant third parties.
•	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 solely relies on the Financial Services Register to check mortgage brokers, while scrutiny of conveyancers only involves a check of public material from the Law Society or Solicitors Regulation Authority.
•	Where a conveyancer is changed during the processing of an application, lenders contact both the original and new conveyancer to ensure the change is for a legitimate reason.	•	A firm's internal escalation procedures are unclear and leave staff confused about when and how to report their concerns about mortgage fraud.
•	A firm checks whether third parties maintain 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.		

11.3.5 Compliance and internal audit

Examples of good practice		Examples of poor 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.	•	A firm's management of third party relationships is subject to only cursory oversight by compliance and internal audit.
•	There is a degree of specialist anti-fraud expertise within the compliance and internal audit functions.	•	Compliance and internal audit staff demonstrate a weak understanding of mortgage fraud risks, because of inexperience or deficient training.

11.3.6 Staff recruitment and vetting

Examples of good practice		Examples of poor practice	
•	A firm requires staff to disclose conflicts of interest stemming from their relationships with third parties such as brokers or conveyancers.	•	A firm uses recruitment agencies without understanding the checks they perform on candidates, and without checking whether they continue to meet agreed recruitment standards.
•	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).	•	Staff vetting is a one-off exercise.
•	A firm adopts a risk-sensitive approach to managing adverse information about an employee or new candidate.	•	Enhanced vetting techniques are applied only to staff in Approved Persons positions.
•	A firm seeks to identify when a deterioration in employees' financial circumstances may	•	A firm's vetting of temporary or contract staff is less thorough than checks on permanent staff in

	indicate increased vulnerability to becoming involved in fraud.		similar roles.

11.3.7 Remuneration structures

Examples of good practice		Examples of poor practice	
•	A firm has considered whether remuneration structures could incentivise behaviour that may increase the risk of mortgage fraud.	•	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.
•	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.	•	The variable element of salespeople's remuneration is excessive.
		•	Staff members' objectives fail to reflect any consideration of mortgage fraud prevention.

11.3.8 Staff training and awareness

Examples of good practice		Examples of poor 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 fails to provide adequate training on mortgage fraud, particularly to staff in higher-risk business areas.
•	A firm verifies that staff understand training materials, perhaps with a test.	•	A firm relies on staff reading up on the topic of mortgage fraud on their own initiative, without providing formal training support.
•	Training is updated to reflect new mortgage fraud trends and types.	•	A firm fails to ensure mortgage lending policies and procedures are readily accessible to staff.
•	Mortgage fraud 'champions' offer guidance or mentoring to	•	A firm fails to define mortgage fraud in training documents or

	staff.		policies and procedures.
		•	Training fails to ensure all staff are aware of their responsibilities to report suspicions, and the channels they should use.

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

12.1 Introduction

12.1.1 **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~~ 2017. ~~Boxes 12.1- 12.4~~ *FCTR* 12.3.2G – *FCTR* 12.3.5G also apply to other **firms** we supervise under the Money Laundering Regulations 2017 **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~~ 2017.

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

12.1.3 The ~~FSA~~ *FSA*'s 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 the ~~FSA~~ *FSA*'s sample, carried out either inadequate due diligence or none at all.

12.1.4 However, the ~~FSA~~ *FSA*'s main conclusion was that around three-quarters of banks in its 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. The ~~FSA~~ *FSA* 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 the ~~FSA~~ *FSA* found it likely that some banks were handling the proceeds of corruption or other financial crime.

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

12.2 The ~~FSA~~ *FSA's* findings

12.2.1 You can read the findings of the ~~FSA~~ *FSA*'s thematic review here: http://www.fsa.gov.uk/pubs/other/aml_final_report.pdf

12.3 Consolidated examples of good and poor practice

12.3.1 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 the ~~FSA~~ *FSA* particular concern. The case studies can be accessed via the link in the paragraph above.

12.3.2 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 2007 are trying to achieve.	•	A lack of commitment to AML risk management among senior management and key AML staff.
•	Keeping AML policies and procedures up to date to ensure compliance with evolving legal and regulatory obligations.	•	Failing to conduct quality assurance work to ensure AML policies and procedures are fit for purpose and working in practice.
•	A clearly articulated definition of a PEP (and any relevant sub-categories) which is well understood by relevant staff.	•	Informal, undocumented processes for identifying, classifying and declassifying customers as PEPs.
•	Considering the risk posed by former PEPs and 'domestic PEPs' on a case-by-case basis.	•	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.
•	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.	•	Giving waivers from AML policies without good reason.
•	Providing good quality training to relevant staff on the risks posed by higher risk customers including PEPs and correspondent banks.	•	Considering the reputational risk rather than the AML risk presented by customers.
•	A clearly articulated definition	•	Using group policies which do not

	of a PEP (and any relevant sub-categories) which is well understood by relevant staff.		comply fully with UK AML legislation and regulatory requirements.
•	Ensuring RMs (Relationship Managers) 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.	•	Using consultants to draw up policies which are then not implemented.
•	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.	•	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.

12.3.3 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.	•	Allocating higher risk countries with low risk scores to avoid having to conduct EDD.
•	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;	•	MLROs who are too stretched or under resourced to carry out their function appropriately.

	and involvement in public contracts.		
•	Risk assessment policies which reflect the bank's risk assessment procedures and risk appetite.	•	Failing to risk assess customers until shortly before an ~~FCA~~ *FCA* visit.
•	Clear understanding and awareness of risk assessment policies, procedures, systems and controls among relevant staff.	•	Allowing RMs to override customer risk scores without sufficient evidence to support their decision.
•	Quality assurance work to ensure risk assessment policies, procedures, systems and controls are working effectively in practice.	•	Inappropriate customer classification systems which make it almost impossible for a customer to be classified as high risk.
•	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.		

12.3.4 High risk customers and PEPs – Customer take-on

Examples of good practice		Examples of poor 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.	•	Failing to give due consideration to certain political connections which fall outside the Money Laundering Regulations 2007 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.
•	The MLRO (and their team) have adequate oversight of all high-risk relationships.	•	Poor quality, incomplete or inconsistent CDD.
•	Clear processes for escalating the approval of high risk and	•	Relying on Group introductions where overseas standards are not

	all PEP customer relationships to senior management or committees which consider AML risk and give appropriate challenge to RMs and the business.		UK-equivalent or where CDD is inaccessible due to legal constraints.
•	Using, where available, local knowledge and open source internet checks to supplement commercially available databases when researching potential high risk customers including PEPs.	•	Inadequate analysis and challenge of information found in documents gathered for CDD purposes.
•	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.	•	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.
•	Effective challenge of RMs and business units by banks' AML and compliance teams, and senior management.	•	Failing to record adequately face-to-face meetings that form part of CDD.
•	Reward structures for RMs which take into account good AML/compliance practice rather than simply the amount of profit generated.	•	Failing to carry out EDD for high risk/PEP customers.
•	Clearly establishing and documenting PEP and other high-risk customers' source of wealth.	•	Failing to conduct adequate CDD before customer relationships are approved.
•	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.	•	Over-reliance on undocumented 'staff knowledge' during the CDD process.
•	Understanding and documenting complex or opaque ownership and corporate structures and the	•	Granting waivers from establishing a customer's source of funds, source of wealth and other CDD without good reason.

	reasons for them.		
•	Face-to-face meetings and discussions with high-risk and PEP prospects before accepting them as a customer.	•	Discouraging business units from carrying out adequate CDD, for example by charging them for intelligence reports.
•	Making clear judgements on money-laundering risk which are not compromised by the potential profitability of new or existing relationships.	•	Failing to carry out CDD on customers because they were referred by senior managers.
•	Recognising and mitigating the risk arising from RMs becoming too close to customers and conflicts of interest arising from RMs' remuneration structures.	•	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 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.

12.3.5 High risk customers and PEPs – Enhanced monitoring of high risk relationships

Examples of good practice		Examples of poor practice	
•	Transaction monitoring which takes account of up-to-date CDD information including expected activity, source of wealth and source of funds.	•	Failing to carry out regular reviews of high-risk and PEP customers in order to update CDD.
•	Regularly reviewing PEP relationships at a senior level based on a full and balanced assessment of the source of wealth of the PEP.	•	Reviews carried out by RMs with no independent assessment by money laundering or compliance professionals of the quality or validity of the review.
•	Monitoring new clients more closely to confirm or amend	•	Failing to disclose suspicious

	the expected account activity.		transactions to SOCA.
•	A risk-based framework for assessing the necessary frequency of relationship reviews and the degree of scrutiny required for transaction monitoring.	•	No formal procedure for escalating prospective customers to committees and senior management on a risk based approach.
•	Proactively following up gaps in, and updating, CDD during the course of a relationship.	•	Failing to seek consent from SOCA on suspicious transactions before processing them.
•	Ensuring transaction monitoring systems are properly calibrated to identify higher risk transactions and reduce false positives.	•	Unwarranted delay between identifying suspicious transactions and disclosure to SOCA.
•	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.	•	Treating annual reviews as a tick-box exercise and copying information from the previous review.
•	A good knowledge among key AML staff of a bank's highest risk/PEP customers.	•	Annual reviews which fail to assess AML risk and instead focus on business issues such as sales or debt repayment.
•	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.	•	Failing to apply enhanced ongoing monitoring techniques to high-risk clients and PEPs.
•	Global consistency when deciding whether to keep or exit relationships with high-risk customers and PEPs.	•	Failing to update CDD based on actual transactional experience.
•	Assessing RMs' performance on ongoing monitoring and feeding this into their annual performance assessment and pay review.	•	Allowing junior or inexperienced staff to play a key role in ongoing monitoring of high-risk and PEP customers.

•	Lower transaction monitoring alert thresholds for higher risk 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.

12.3.6 Correspondent banking – Risk assessment of respondent banks

Examples of good practice		Examples of poor practice	
•	Regular assessments of correspondent banking risks taking into account various money laundering risk factors such as the 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.	•	Failing to consider the money-laundering risks of correspondent relationships.
•	More robust monitoring of respondents identified as presenting a higher risk.	•	Inadequate or no documented policies and procedures setting out how to deal with respondents.
•	Risk scores that drive the frequency of relationship reviews.	•	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.
•	Taking into consideration publicly available information from national government bodies and non-governmental organisations and other credible sources.	•	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.

12.3.7 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.	•	Inadequate CDD on parent banks and/or group affiliates, particularly if the respondent is based in a high-risk jurisdiction.
•	EDD for respondents that present greater risks or where there is less publicly available information about the respondent.	•	Collecting CDD information but failing to assess the risks.
•	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.	•	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.
•	Screening the names of senior managers, owners and controllers of respondent banks to identify PEPs and assessing the risk that identified PEPs pose.	•	Failing to follow up on outstanding information that has been requested during the CDD process.
•	Independent quality assurance work to ensure that CDD standards are up to required standards consistently across the bank.	•	Failing to follow up on issues identified during the CDD process.
•	Discussing with overseas regulators and other relevant bodies about the AML regime in a respondent's home country.	•	Relying on parent banks to conduct CDD for a correspondent account and taking no steps to ensure this has been done.

•	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.	•	Collecting AML policies etc but making no effort to assess them.
•	Visiting, or otherwise liaising with, respondent banks to discuss AML issues and gather CDD information.	•	Having no information on file for expected activity volumes and values.
•	Gathering information about procedures at respondent firms for sanctions screening and identifying/managing PEPs.	•	Failing to consider adverse information about the respondent or individuals connected with it.
•	Understanding respondents' processes for monitoring account activity and reporting suspicious activity.	•	No senior management involvement in the approval process for new correspondent bank relationships or existing relationships being reviewed.
•	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.		

12.3.8 Correspondent banking –Ongoing monitoring of respondent accounts

Examples of good practice		Examples of poor practice	
•	Review periods driven by the risk rating of a particular relationship; with high risk relationships reviewed more frequently.	•	Copying periodic review forms year after year without challenge from senior management.
•	Obtaining an updated picture of the purpose of the account	•	Failing to take account of any changes to key staff at respondent

	and expected activity.		banks.
•	Updating screening of respondents and connected individuals to identify individuals/entities with PEP connections or on relevant sanctions lists.	•	Carrying out annual reviews of respondent relationships but failing to consider money-laundering risk adequately.
•	Involving senior management and AML staff in reviews of respondent relationships and consideration of whether to maintain or exit high-risk relationships.	•	Failing to assess new information gathered during ongoing monitoring of a relationship.
•	Where appropriate, using intelligence reports to help decide whether to maintain or exit a relationship.	•	Failing to consider money laundering alerts generated since the last review.
•	Carrying out ad-hoc reviews in light of material changes to the risk profile of a customer.	•	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.

12.3.9 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	•	Paying banks take insufficient steps to ensure that all outgoing MT103s contain sufficient beneficiary information to mitigate the risk of customer

	inserted in the correct lines of the outgoing MT103 payment instruction and any matching MT202COV.		funds being incorrectly blocked, delayed or rejected.

12.3.10 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 customer.	•	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 unnoticed.
•	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 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.		

12.3.11 Wire transfers – Beneficiary banks

Examples of good practice		Examples of poor 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	•	Insufficient processes to identify payments with incomplete or meaningless payer information.

	inadequate or meaningless payer information.		
•	Actively engaging in dialogue with peers about the difficult issue of taking appropriate action against persistently offending banks.		

12.3.12 Wire transfers – Implementation of SWIFT MT202COV

Examples of good practice		Examples of poor practice	
•	Reviewing all correspondent banks' use of the MT202 and MT202COV.	•	Continuing to use the MT202 for all bank-to-bank payments, even if the payment is cover for an underlying customer transaction.
•	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.		
•	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.		

13 Anti-bribery and corruption systems and controls in investment banks (2012)

13.1 Introduction

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

- investment banks and firms carrying on investment banking or

similar activities in the UK;

- all other firms who are subject to our financial crime rules in ~~SYSC~~ *SYSC* 3.2.6R or 6.1.1R; and
- electronic money institutions and payment institutions within our supervisory scope.

~~Box 13.4~~ *FCTR* 13.3.5G and ~~Box 13.5~~ *FCTR* 13.3.6G only apply to firms or institutions who use third parties to win business.

13.1.2 In March 2012, the ~~FSA~~ *FSA* published the findings of its review of investment banks' anti-bribery and corruption systems and controls. The ~~FSA~~ *FSA* visited 15 investment banks and firms carrying on investment banking or similar activities in the UK to assess how they were managing bribery and corruption risk. Although this report focused on investment banking, its findings are relevant to other sectors.

13.1.3 The ~~FSA~~ *FSA* found that although some investment banks had completed a great deal of work to implement effective anti-bribery and corruption controls in the months preceding its visit, the majority of them had more work to do and some firms' systems and controls fell short of its regulatory requirements. Weaknesses related in particular to: many firms' limited understanding of the applicable legal and regulatory regimes, incomplete or inadequate bribery and corruption risk assessments; lack of senior management oversight; and failure to monitor the effective implementation of, and compliance with, anti-bribery and corruption policies and procedures.

13.1.4 The contents of this report are reflected in ~~Chapter 6~~ *FCG* 6 (Bribery and corruption).

13.2 The ~~FSA~~ *FSA's* findings

13.2.1 You can read the findings of the ~~FSA~~ *FSA*'s thematic review here: http://www.fsa.gov.uk/pubs/other/anti-bribery-investment-banks.pdf

13.3 Consolidated examples of good and poor practice

13.3.1 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 the ~~FSA~~ *FSA* particular concern. The case studies can be accessed via the link in the paragraph above.

13.3.2 Governance and management information (MI)

Examples of good practice		Examples of poor practice	
•	Clear, documented responsibility for anti-bribery and corruption apportioned to either a single senior manager or a committee with	•	Failing to establish an effective governance framework to address bribery and corruption risk.

	appropriate terms of reference and senior management membership, reporting ultimately to the Board.		
•	Regular and substantive MI to the Board and other relevant senior management forums, including: an overview of the bribery and corruption risks faced by the business; systems and controls to mitigate those risks; information about the effectiveness of those systems and controls; and legal and regulatory developments.	•	Failing to allocate responsibility for anti-bribery and corruption to a single senior manager or an appropriately formed committee.
•	Where relevant, 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.	•	Little or no MI sent to the Board about bribery and corruption issues, including legislative or regulatory developments, emerging risks and higher risk third-party relationships or payments.
•	Considering the risk posed by former PEPs and 'domestic PEPs' on a case-by-case basis.		
•	Actions taken or proposed in response to issues highlighted by MI are minuted and acted on appropriately.		

13.3.3 Assessing bribery and corruption risk

Examples of good practice		Examples of poor practice	
•	Responsibility for carrying out a risk assessment and keeping it up-to-date is clearly apportioned to an individual or a group of individuals with sufficient levels of expertise and seniority.	•	The risk assessment is a one-off exercise.

•	The firm takes adequate steps to identify the bribery and corruption risk. Where internal knowledge and understanding of corruption risk is limited, the firm supplements this with external expertise.	•	Efforts to understand the risk assessment are piecemeal and lack coordination.
•	Risk assessment is a continuous process based on qualitative and relevant information available from internal and external sources.	•	Risk assessments are incomplete and too generic.
•	Firms consider the potential conflicts of interest which might lead business units to downplay the level of bribery and corruption risk to which they are exposed.	•	Firms do not satisfy themselves that staff involved in risk assessment are sufficiently aware of, or sensitised to, bribery and corruption issues.
•	The bribery and corruption risk assessment informs the development of monitoring programmes; policies and procedures; training; and operational processes.		
•	The risk assessment demonstrates an awareness and understanding of firms' legal and regulatory obligations.		
•	The firm assesses where risks are greater and concentrates its resources accordingly.		
•	The firm considers financial crime risk when designing new products and services.		

13.3.4 Policies and procedures

Examples of good practice		Examples of poor practice	
•	The firm clearly sets out the behaviour expected of those acting on its behalf.	•	The firm has no method in place to monitor and assess staff compliance with anti-bribery and corruption policies and

			procedures.
•	Firms have conducted a gap analysis of existing bribery and corruption procedures against applicable legislation, regulations and guidance and made necessary enhancements.	•	Staff responsible for the implementation and monitoring of anti-bribery and corruption policies and procedures have inadequate expertise on bribery and corruption.
•	The firm has a defined process in place for dealing with breaches of policy.		
•	The team responsible for ensuring the firm's compliance with its anti-bribery and corruption obligations engages with the business units about the development and implementation of anti-bribery and corruption systems and controls.		
•	anti-bribery and corruption policies and procedures will vary depending on a firm's exposure to bribery and corruption risk. But in most cases, firms should have policies and procedures which cover expected standards of behaviour; escalation processes; conflicts of interest; expenses, gifts and hospitality; the use of third parties to win business; whistleblowing; monitoring and review mechanisms; and disciplinary sanctions for breaches. These policies need not be in a single 'ABC policy' document and may be contained in separate policies.		
•	There should be an effective mechanism for reporting issues to the team or committee responsible for ensuring compliance with the firm's anti-bribery and corruption		

	obligations.		

13.3.5 Third-party relationships and due diligence

Examples of good practice		Examples of poor practice	
•	Where third parties are used to generate business, these relationships are subject to thorough due diligence and management oversight.	•	A firm using intermediaries fails to satisfy itself that those businesses have adequate controls to detect and prevent staff using bribery or corruption to generate business.
•	Third-party relationships are reviewed regularly and in sufficient detail to confirm that they are still necessary and appropriate to continue.	•	The firm fails to establish and record an adequate commercial rationale for using the services of third parties.
•	There are higher, or extra, levels of due diligence and approval for high risk third-party relationships.	•	The firm is unable to produce a list of approved third parties, associated due diligence and details of payments made to them.
•	There is appropriate scrutiny of, and approval for, relationships with third parties that introduce business to the firm.	•	There is no checking of compliance's operational role in approving new third-party relationships and accounts.
•	The firm's compliance function has oversight of all third-party relationships and monitors this list to identify risk indicators, eg a third party's political or public service connections.	•	A firm assumes that long-standing third-party relationships present no bribery or corruption risk.
•	Evidence that a risk-based approach has been adopted to identify higher risk relationships in order to apply enhanced due diligence.	•	A firm relies exclusively on informal means, such as staff's personal knowledge, to assess the bribery and corruption risk associated with third parties.
•	Enhanced due diligence procedures include a review of the third party's own anti-bribery and corruption controls.	•	No prescribed take-on process for new third-party relationships.

•	Consideration, where appropriate, of compliance involvement in interviewing consultants and the provision of anti-bribery and corruption training to consultants.	•	A firm does not keep full records of due diligence on third parties and cannot evidence that it has considered the bribery and corruption risk associated with a third-party relationship.
•	Inclusion of anti-bribery and corruption-specific clauses and appropriate protections in contracts with third parties.	•	The firm cannot provide evidence of appropriate checks to identify whether introducers and consultants are PEPs.
		•	Failure to demonstrate that due diligence information in another language has been understood by the firm.

13.3.6 Payment controls

Examples of good practice		Examples of poor practice	
•	Ensuring adequate due diligence on and approval of third-party relationships before payments are made to the third party.	•	Failing to check whether third parties to whom payments are due have been subject to appropriate due diligence and approval.
•	Risk-based approval procedures for payments and a clear understanding of the reason for all payments.	•	Failing to produce regular third-party payment schedules for review.
•	Checking third-party payments individually prior to approval, to ensure consistency with the business case for that account.	•	Failing to check thoroughly the nature, reasonableness and appropriateness of gifts and hospitality.
•	Regular and thorough monitoring of third-party payments to check, for example, whether a payment is unusual in the context of previous similar payments.	•	No absolute limits on different types of expenditure, combined with inadequate scrutiny during the approvals process.
•	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 hospitality.		
•	Ensuring the reasons for third-party payments via Accounts Payable are clearly documented and appropriately approved.		
•	The facility to produce accurate MI to assist effective payment monitoring.		

13.3.7 Gifts and hospitality (G&H)

Examples of good practice		Examples of poor practice	
•	Policies and procedures clearly define the approval process and the limits applicable to G&H.	•	Senior management do not set a good example to staff on G&H policies.
•	Processes for filtering G&H by employee, client and type of hospitality for analysis.	•	Acceptable limits and the approval process are not defined.
•	Processes to identify unusual or unauthorised G&H and deviations from approval limits for G&H.	•	The G&H policy is not kept up-to-date.
•	Staff are trained on G&H policies to an extent appropriate to their role, in terms of both content and frequency, and regularly reminded to disclose G&H in line with policy.	•	G&H and levels of staff compliance with related policies are not monitored.

•	Cash or cash-equivalent gifts are prohibited.	•	No steps are taken to minimise the risk of gifts going unrecorded.
•	Political and charitable donations are approved at an appropriate level, with input from the appropriate control function, and subject to appropriate due diligence.	•	Failure to record a clear rationale for approving gifts that fall outside set thresholds.
		•	Failure to check whether charities being donated to are linked to relevant political or administrative decision-makers.

13.3.8 Staff recruitment and vetting

Examples of good practice		Examples of poor practice	
•	Vetting staff on a risk-based approach, taking into account financial crime risk.	•	Failing to carry out ongoing checks to identify changes that could affect an individual's integrity and suitability.
•	Enhanced vetting – including checks of credit records, criminal records, financial sanctions lists, commercially-available intelligence databases – for staff in roles with higher bribery and corruption risk.	•	No risk-based processes for identifying staff who are PEPs or otherwise connected to relevant political or administrative decision-makers.
•	Conducting periodic checks to ensure that agencies are complying with agreed vetting standards.	•	Where employment agencies are used to recruit staff, failing to demonstrate a clear understanding of the checks these agencies carry out on prospective staff.
		•	Temporary or contract staff receiving less rigorous vetting than permanently employed colleagues carrying out similar roles.

13.3.9 Training and awareness

Examples of good practice	Examples of poor practice

•	Providing good quality, standard training on anti-bribery and corruption for all staff.	•	Failing to provide training on ABC that is targeted at staff with greater exposure to bribery and corruption risks.
•	Ensuring training covers relevant and practical examples.	•	Failing to monitor and measure the quality and effectiveness of training.
•	Keeping training material and staff knowledge up-to-date.		
•	Awareness-raising initiatives, such as special campaigns and events to support routine training, are organised.		

13.3.10 Remuneration structures

Examples of good practice		Examples of poor practice	
•	Remuneration takes account of good compliance behaviour, not simply the amount of business generated.	•	Failing to reflect poor staff compliance with anti-bribery and corruption policy and procedures in staff appraisals and remuneration.
•	Identifying higher-risk functions from a bribery and corruption perspective and reviewing remuneration structures to ensure they do not encourage unacceptable risk taking.		

13.3.11 Incident reporting and management

Examples of good practice		Examples of poor practice	
•	Clear procedures for whistleblowing and the reporting of suspicions, which are communicated to staff.	•	Failing to maintain proper records of incidents and complaints.
•	Details about whistleblowing hotlines are visible and accessible to staff.		

•	Where whistleblowing hotlines are not provided, firms should consider measures to allow staff to raise concerns in confidence or, where possible, anonymously, with adequate levels of protection and communicate this clearly to staff.		
•	Firms use information gathered from whistleblowing and internal complaints to assess the effectiveness of their anti-bribery and corruption policies and procedures.		

14 Banks' defences against investment fraud (2012)

14.1 Introduction

14.1.1 **Who should read this chapter?** This chapter is relevant, and its statements of good and poor practice apply, to deposit-taking institutions with retail customers.

14.1.2 The ~~FSA~~ *FSA*'s thematic review, Bank's defences against investment fraud, published in June 2012, set out the findings of its visits to seven retail banks and one building society to assess the systems and controls in place to contain the risks posed by investment fraudsters.

14.1.3 UK consumers are targeted by share-sale frauds and other scams including land-banking frauds, unauthorised collective investment schemes and Ponzi schemes. Customers of UK deposit-takers may fall victim to these frauds, or be complicit in them.

14.1.4 The contents of this report are reflected in ~~Box 4.5 in Chapter 4 of Part 1 of this Guide~~ *FCG* 4.2.5G).

14.2 The ~~FSA~~ *FSA's* findings

14.2.1 You can read the findings of the ~~FSA~~ *FSA*'s thematic review here: http://www.fsa.gov.uk/static/pubs/other/banks-defences-against-investment-fraud.pdf

14.3 Consolidated examples of good and poor practice

14.3.1 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 the ~~FSA~~ *FSA* particular concern. The case studies can be accessed via the link in the paragraph above.

14.3.2 Governance

Examples of good practice		Examples of poor practice	
•	A bank can demonstrate senior management ownership and understanding of fraud affecting customers, including investment fraud.	•	A bank lacks a clear structure for the governance of investment fraud or for escalating issues relating to investment fraud. Respective responsibilities are not clear.
•	There is a clear organisational structure for addressing the risk to customers and the bank arising from fraud, including investment fraud. There is evidence of appropriate information moving across this governance structure that demonstrates its effectiveness in use.	•	A bank lacks a clear rationale for allocating resources to protecting customers from investment fraud.
•	A bank has recognised subject matter experts on investment fraud supporting or leading the investigation process.	•	A bank lacks documented policies and procedures relating to investment fraud.
•	A bank seeks to measure its performance in preventing detriment to customers.	•	There is a lack of communication between a bank's AML and fraud teams on investment fraud.
•	When assessing the case for measures to prevent financial crime, a bank considers benefits to customers, as well as the financial impact on the bank.		

14.3.3 Risk assessment

Examples of good practice		Examples of poor practice	
•	A bank regularly assesses the risk to itself and its customers of losses from fraud, including investment fraud, in accordance with their established risk management	•	A bank has performed no risk assessment that considers the risk to customers from investment fraud.

	framework. The risk assessment does not only cover situations where the bank could suffer losses, but also where customers could lose and not be reimbursed by the bank. Resource allocation and mitigation measures are also informed by this assessment.		
•	A bank performs 'horizon scanning' work to identify changes in the fraud types relevant to the bank and its customers.	•	A bank's regulatory compliance, risk management and internal audit functions' assurance activities do not effectively challenge the risk assessment framework.

14.3.4 Detecting perpetrators

Examples of good practice		Examples of poor practice	
•	A bank's procedures for opening commercial accounts include an assessment of the risk of the customer, based on the proposed business type, location and structure.	•	A bank only performs the customer risk assessment at account set up and does not update this through the course of the relationship.
•	Account opening information is used to categorise a customer relationship according to its risk. The bank then applies different levels of transaction monitoring based on this assessment.	•	A bank does not use account set up information (such as anticipated turnover) in transaction monitoring.
•	A bank screens new customers to prevent the take-on of possible investment fraud perpetrators.	•	A bank allocates excessive numbers of commercial accounts to a staff member to monitor, rendering the ongoing monitoring ineffective.
		•	A bank allocates responsibility for the ongoing monitoring of the customer to customer-facing staff with many other conflicting responsibilities.

14.3.5 Automated monitoring

Examples of good practice		Examples of poor practice	
•	A bank undertakes real-time payment screening against data about investment fraud from credible sources.	•	A bank fails to use information about known or suspected perpetrators of investment fraud in its financial crime prevention systems.
•	There is clear governance of real time payment screening. The quality of alerts (rather than simply the volume of false positives) is actively considered.	•	A bank does not consider investment fraud in the development of monitoring rules.
•	Investment fraud subject matter experts are involved in the setting of monitoring rules.	•	The design of rules cannot be amended to reflect the changing nature of the risk being monitored.
•	Automated monitoring programmes reflect insights from risk assessments or vulnerable customer initiatives.		
•	A bank has monitoring rules designed to detect specific types of investment fraud e.g. boiler room fraud.		
•	A bank reviews accounts after risk triggers are tripped (such as the raising of a SAR) in a timely fashion.		
•	When alerts are raised, a bank checks against account-opening information to identify any inconsistencies with expectations.		

14.3.6 Protecting victims

Examples of good practice		Examples of poor practice	
•	A bank contacts customers in	•	Communication with customers

	the event they suspect a payment is being made to an investment fraudster.		on fraud just covers types of fraud for which the bank may be financially liable, rather than fraud the customer might be exposed to.
•	A bank places material on investment fraud on its website.	•	A bank has no material on investment fraud on its website.
•	A bank adopts alternative customer awareness approaches, such as mailing customers and branch awareness initiatives.	•	Failing to contact customers they suspect are making payments to investment fraudsters on grounds that this constitutes 'investment advice'.
•	Work to detect and prevent investment fraud is integrated with a bank's vulnerable customers initiative.		

14.3.7 Management reporting and escalation of suspicions

Examples of good practice		Examples of poor practice	
•	A specific team focuses on investigating the perpetrators of investment fraud.	•	There is little reporting to senior management on the extent of investment fraud (whether victims or perpetrators) in a bank's customer base.
•	A bank's fraud statistics include figures for losses known or suspected to have been incurred by customers.	•	A bank is unable to access information on how many of the bank's customers have become the victims of investment fraud.

14.3.8 Staff awareness

Examples of good practice		Examples of poor practice	
•	Making good use of internal experience of investment fraud to provide rich and engaging training material.	•	Training material only covers boiler rooms.
•	A wide-range of materials are available that cover investment fraud.	•	A bank's training material is out-of-date.

•	Awards are given on occasion to frontline staff when a noteworthy fraud is identified.		
•	Training material is tailored to the experience of specific areas such as branch and relationship management teams.		

14.3.9 Use of industry intelligence

Examples of good practice		Examples of poor practice	
•	A bank participates in cross-industry forums on fraud and boiler rooms and makes active use of intelligence gained from these initiatives in, for example, its transaction monitoring and screening efforts.	•	A bank fails to act on actionable, credible intelligence shared at industry forums or received from other authoritative sources such as the ~~FCA~~ *FCA* or City of London Police.
•	A bank takes measures to identify new fraud typologies. It joins-up internal intelligence, external intelligence, its own risk assessment and measures to address this risk.		

15 Banks' control of financial crime risks in trade finance (2013)

15.1 Introduction

15.1.1 **Who should read this chapter?** This chapter is relevant, and its statements of good and poor practice apply, to **banks carrying out trade finance business**.

15.1.2 In July 2013, we published the findings of our review of banks' control of financial crime risks in trade finance. We visited 17 commercial banks to assess the systems and controls they had in place to contain the risks of money laundering, terrorist financing and sanctions breaches in trade finance operations. Our review only considered Documentary Letters of Credit (LCs) and Documentary Bills for Collection (BCs).

15.1.3 We found that banks generally had effective controls to ensure they were not dealing with sanctioned individuals or entities. But most banks had inadequate systems and controls over dual-use goods and their anti-money laundering policies and procedures were often weak.

15.1.4 The following examples of good and poor practice should be read in

conjunction with ~~Part 1 of this Guide~~ *FCG*. ~~Part 1~~ *FCG* provides more general guidance, including on AML and sanctions systems and controls, that can be relevant in the context of banks' trade finance business. Not all examples of good and poor practice will be relevant to all banks that carry out trade finance business and banks should consider them in a risk-based and proportionate way.

15.2 The ~~FSA~~ *FSA*'s findings

15.2.1 You can read the findings of the ~~FSA~~ *FSA's* thematic review here: http://www.fca.org.uk/static/documents/thematic-reviews/tr-13-03.pdf

15.3 Consolidated examples of good and poor practice

15.3.1 Governance and MI

Examples of good practice		Examples of poor practice	
•	Roles and responsibilities for managing financial crime risks in trade finance are clear and documented.	•	Failure to produce management information on financial crime risk in trade finance.
•	The bank ensures that staff have the opportunity to share knowledge and information about financial crime risk in trade finance, for example by holding regular teleconferences with key trade finance staff or by including trade finance financial crime risk as an agenda item in relevant forums.	•	Internal audit fails to consider financial crime controls in trade finance.
		•	The culture of a bank does not encourage the sharing of information relevant to managing financial crime risk in trade finance.

15.3.2 Risk assessment

Examples of good practice		Examples of poor practice	
•	The bank assesses and documents both money laundering and sanctions risk in the bank's trade finance business. This assessment is	•	Failure to update risk assessments and keep them under regular review to take account of emerging risks in trade finance.

	tailored to the bank's role in trade transactions and can form part of the bank's wider financial crime risk assessment.		
		•	Only focusing on credit and reputational risk in trade finance.
		•	Not taking account of a customer's use of the bank's trade finance products and services in a financial crime risk assessment.

15.3.3 Policies and procedures

Examples of good practice		Examples of poor practice	
•	Staff are required to consider financial crime risks specific to trade finance transactions and identify the customers and transactions that present the highest risk at various stages of a transaction.	•	Staff are not required to consider trade specific money laundering risks (eg, FATF/Wolfsberg red flags).
•	Staff identify key parties to a transaction and screen them against sanctions lists. Key parties include the instructing party, but may include other parties on a risk-sensitive basis.	•	Procedures do not take account of money laundering risks and are focused on credit and operational risks.
•	The bank provides guidance on recognising red flags in trade finance transactions.	•	No clear escalation procedures for high-risk transactions.
		•	Procedures fail to take account of the parties involved in a transaction, the countries where they are based and the nature of the good involved.

15.3.4 Due diligence

Examples of good practice	Examples of poor practice

•	Banks' written procedures are clear about what due diligence checks are necessary on the instructing parties. They take account of the bank's role in a transaction, and when it is appropriate to apply due diligence checks to others, including non-client beneficiaries (or recipients) of an LC or BC.	•	Trade processing teams do not make adequate use of the significant knowledge of customers' activity possessed by relationship managers or trade sales teams when considering the financial crime risk in particular transactions.
		•	Lack of appropriate dialogue between CDD teams and trade processing teams whenever potential financial crime issues arise from the processing of a trade finance transaction.

15.3.5 Training and awareness

Examples of good practice		Examples of poor practice	
•	Tailored training is given that raises staff awareness and understanding of trade-specific money laundering, sanctions and terrorist financing risks.	•	Only providing generic training that does not take account of trade-specific AML risks (eg FATF/Wolfsberg red flags).
•	Relevant industry publications are used to raise awareness of emerging risks.	•	Failure to roll out trade specific financial crime training to all relevant staff engaged in trade finance activity, wherever located.
•	Processing staff are trained to look for suspicious variances in the pricing of comparable or analogous transactions.	•	Reliance on 'experienced' trade processing staff who have received no specific training on financial crime risk.

15.3.6 AML procedures

Examples of good practice		Examples of poor practice	
•	A formal consideration of money laundering risk is written into the operating procedures governing LCs and	•	Failure to assess transactions for money laundering risk.

	BCs.		
•	The money laundering risk in each transaction is considered and evidence of the assessment made is kept.	•	Reliance on customer due diligence procedures alone to mitigate the risk of money laundering in transactions.
•	Detailed guidance is available for relevant staff on what constitutes a potentially suspicious transaction, including indicative lists of red flags.	•	Reliance on training alone to ensure that staff escalate suspicious transactions, when there are no other procedures or controls in place.
•	Staff processing transactions have a good knowledge of a customer's expected activity; and a sound understanding of trade based money laundering risks.	•	Disregarding money laundering risk when transactions present little or no credit risk.
•	Processing teams are encouraged to escalate suspicions for investigation as soon as possible.	•	Money laundering risk is disregarded when transactions involve another group entity (especially if the group entity is in a high risk jurisdiction).
•	Those responsible for reviewing escalated transactions have an extensive knowledge of trade-based money laundering risk.	•	A focus on sanctions risk at the expense of money laundering risk.
•	Underlying trade documentation relevant to the financial instrument is obtained and reviewed on a risk-sensitive basis.	•	Failure to document adequately how money laundering risk has been considered or the steps taken to determine that a transaction is legitimate.
•	Third party data sources are used on a risk-sensitive basis to verify the information given in the LC or BC.	•	Trade-based money laundering checklists are used as 'tick lists' rather than as a starting point to think about the wider risks.
•	Using professional judgement to consider whether the pricing of goods makes commercial sense, in particular in relation to traded commodities for which reliable and up-to-date pricing information can be	•	Failure to investigate potentially suspicious transactions due to time constraints or commercial pressures.

	obtained.		
•	Regular, periodic quality assurance work is conducted by suitably qualified staff who assess the judgments made in relation to money laundering risk and potentially suspicious transactions.	•	Failure to ensure that relevant staff understand money laundering risk and are aware of relevant industry guidance or red flags.
•	•Trade processing staff keep up to date with emerging trade-based money laundering risks.	•	Failure to distinguish money laundering risk from sanctions risk.
•	Where red flags are used by banks as part of operational procedures, they are regularly updated and easily accessible to staff.	•	Ambiguous escalation procedures for potentially suspicious transactions, or procedures that only allow for escalation to be made to sanctions teams.
•	Expertise in trade-based money laundering is also held in a department outside of the trade finance business (e.g. Compliance) so that independent decisions can be made in relation to further investigation of escalations and possible SAR reporting.	•	Not taking account of other forms of potentially suspicious activity that may not be covered by the firm's guidance.
		•	Failure to make use of information held in CDD files and RMs' knowledge to identify potentially suspicious transactions.
		•	Trade processing teams are not given sufficient time to fully investigate potentially suspicious activity, particularly when there are commercial time pressures.
		•	Trade processing staff are not encouraged to keep up to date with emerging trade based money laundering risks.
		•	Failure to assess transactions for money laundering risk.

		•	Reliance on customer due diligence procedures alone to mitigate the risk of money laundering in transactions.

15.3.7 Sanctions procedures

Examples of good practice		Examples of poor practice	
•	Screening information is contained within trade documents against applicable sanctions lists.	•	Staff dealing with trade-related sanctions queries are not appropriately qualified and experienced to perform the role effectively.
•	Hits are Investigated before proceeding with a transaction (for example, obtaining confirmation from third parties that an entity is not sanctioned), and clearly documenting the rationale for any decisions made.	•	Failure to screen trade documentation.
•	Shipping container numbers are validated on a risk-sensitive basis.	•	Failure to screen against all relevant international sanctions lists.
•	Potential sanctions matches are screened for at several key stages of a transaction.	•	Failure to keep-up-to-date with the latest information regarding name changes for sanctioned entities, especially as the information may not be reflected immediately on relevant sanctions lists.
•	Previous sanction alerts are analysed to identify situations where true hits are most likely to occur and the bank focuses its sanctions resources accordingly.	•	Failure to record the rationale for decisions to discount false positives.
•	New or amended information about a transaction is captured and screened.	•	Failure to undertake risk-sensitive screening of information held on agents, insurance companies, shippers, freight forwarders, delivery agents, inspection agents, signatories, and parties mentioned

			in certificates of origin, as well as the main counterparties to a transaction.
		•	Failure to record the rationale for decisions that are taken not to screen particular entities and retaining that information for audit purposes.

15.3.8 Dual-use goods

Examples of good practice		Examples of poor practice	
•	Ensuring staff are aware of dual-use goods issues, common types of goods that have a dual use, and are capable of identifying red flags that suggest that dual-use goods risk being supplied for illicit purposes.	•	No clear dual-use goods policy.
•	Confirming with the exporter in higher risk situations whether a government licence is required for the transaction and seeking a copy of the licence where required.	•	Failure to undertake further research where goods descriptions are unclear or vague.
		•	Third party data sources are not used where possible to undertake checks on dual-use goods.

16 How small banks manage money laundering and sanctions risk – update (2014)

16.1 Introduction

16.1.1 **Who should read this chapter?** This chapter is relevant, and its statements of good practice apply, to **banks** we supervise under the Money Laundering Regulations ~~2007~~ 2017. It may be of interest to **other firms** we supervise under the Money Laundering Regulations ~~2007~~ 2017.

16.1.2 In November 2014 we published the findings of our thematic review of how small banks manage AML and sanctions risk. We assessed the adequacy of the AML and sanctions systems and controls of 21 small banks. We also looked at the extent to which the banks had considered our regulatory AML guidance, enforcement cases and the findings from our 2011 review of 'banks'

management of high money laundering risk situations'. To this end, our sample included five banks that had also been part of our sample in 2011.

16.1.3 A small number of banks in our sample had implemented effective AML and sanctions controls. But, despite our extensive work in this area over recent years, we found significant and widespread weaknesses in most of the sample banks' AML systems and controls and some banks' sanctions controls. We also found that AML resources were inadequate in one-third of all banks in our sample and that some overseas banks struggled to reconcile their group AML policies with UK AML standards and requirements.

16.1.4 The contents of this report are reflected in ~~Chapters 1, 2 and 3 of Part 1 of this Guide~~ *FCG* 1-3.

16.2 The ~~FCA~~ *FCA* findings

16.2.1 You can read the findings of our thematic review here: http://www.fca.org.uk/news/tr14-16-how-small-banks-manage-money-laundering-and-sanctions-risk

16.3 Themes

16.3.1 Management information (MI)

Useful MI provides senior management with the information they need to ensure that the firm effectively manages the money laundering and sanctions risks to which it is exposed. MI should be provided regularly, including as part of the MLRO report, and ad hoc, as risk dictates.

Examples of useful MI include:

- an overview of the money laundering and sanctions risks to which the bank is exposed, including information about emerging risks and any changes to the bank's risk assessment
- an overview of the systems and controls to mitigate those risks, including information about the effectiveness of these systems and controls and any changes to the bank's control environment
- legal and regulatory developments and the impact these have on the bank's approach
- relevant information about individual business relationships, for example:
    - the number and nature of new accounts opened, in particular where these are high risk
    - the number and nature of accounts closed, in particular where these have been closed for financial crime reasons
    - the number of dormant accounts and re-activated dormant accounts, and

- the number of transaction monitoring alerts and suspicious activity reports, including where the processing of these has fallen outside of agreed service level agreements.

16.3.2 Governance structures

Banks should have a governance structure that is appropriate to the size and nature of their business.

To be effective, a governance structure should enable the firm to:

- clearly allocate responsibilities for financial crime issues
- establish clear reporting lines and escalation paths
- identify and manage conflicts of interest, in particular where staff hold several functions cumulatively, and
- record and retain key decisions relating to the management of money laundering and sanctions risks, including, where appropriate, decisions resulting from informal conversations.

16.3.3 Culture and tone from the top

An effective AML and sanctions control framework depends on senior management setting and enforcing a clear level of risk appetite, and embedding a culture of compliance where financial crime is not acceptable.

Examples of good practice include:

- senior management taking leadership on AML and sanctions issues, for example through everyday decision-making and staff communications
- clearly articulating and enforcing the bank's risk appetite – this includes rejecting individual business relationships where the bank is not satisfied that it can manage the risk effectively
- allocating sufficient resources to the bank's compliance function
- ensuring that the bank's culture enables it to comply with the UK's legal and regulatory AML framework, and
- considering whether incentives reward unacceptable risk-taking or compliance breaches and, if they do, removing them.

16.3.4 Risk assessment

Banks must identify and assess the money laundering risk to which they are exposed. This will help them understand which parts of their business are most vulnerable to money laundering and which parts they should prioritise in their fight against financial crime. It will also help banks decide on the appropriate

level of CDD and monitoring for individual business relationships.

A business-wide risk assessment:

- must be comprehensive, meaning that it should consider a wide range of factors, including the risk associated with the bank's customers, products, and services – it is not normally enough to consider just one factor
- should draw on a wide range of relevant information – it is not normally enough to consider just one source, and
- must be proportionate to the nature, scale and complexity of the bank's activities.

Banks should build on their business-wide risk assessment to determine the level of CDD they should apply to individual business relationships or occasional transactions. CDD will help banks refine their assessment of risk associated with individual business relationships or occasional transactions and will determine whether additional CDD measures should be applied and the extent of monitoring that is required to mitigate that risk. An individual assessment of risk associated with a business relationship or occasional transaction can inform, but is no substitute for, a business-wide risk assessment.

A customer risk assessment:

- should enable banks to take a holistic view of the risk associated with a business relationship or occasional transaction by considering all relevant risk factors, and
- should be recorded – where the risk is high, banks should include the reason why they are content to accept the risk associated with the business relationship or occasional transaction and details of any steps the bank will take to mitigate the risks, such as restrictions on the account or enhanced monitoring.

See ~~ML Reg 20 SYSC 6.3.1R~~ regulation 20 of the Money Laundering Regulations 2007 and *SYSC* 6.3.1R

16.3.5 Enhanced due diligence (EDD)

The central objective of EDD is to enable a bank to better understand the risks associated with a high-risk customer and make an informed decision about whether to on-board or continue the business relationship or carry out the occasional transaction. It also helps the bank to manage the increased risk by deepening its understanding of the customer, the beneficial owner, and the nature and purpose of the relationship.

The extent of EDD must be commensurate with the risk associated with the business relationship or occasional transaction but banks can decide, in most cases, which aspects of CDD they should enhance.

Senior management should be provided with all relevant information (eg, source of wealth, source of funds, potential risks, adverse information and red

flags) before approving PEP relationships to ensure they understand the nature of, and the risks posed by, the relationship they are approving.

Examples of effective EDD measures we observed included:

- obtaining more information about the customer's or beneficial owner's business
- obtaining more robust verification of the beneficial owner's identity on the basis of information obtained from a reliable and independent source
- carrying out searches on a corporate customer's directors (or individuals exercising control) to understand whether their business or integrity affects the level of risk associated with the business relationship, for example because they also hold a public function
- using open source websites to gain a better understanding of the customer or beneficial owner, their reputation and their role in public life – where banks find information containing allegations of wrongdoing or court judgments, they should assess how this affects the level of risk associated with the business relationship
- establishing the source of wealth to be satisfied that this is legitimate – banks can establish the source of wealth through a combination of customer-provided information, open source information and documents such as evidence of title, copies of trust deeds and audited accounts (detailing dividends)
- establishing the source of funds used in the business relationship to be satisfied they do not constitute the proceeds of crime
- commissioning external third-party intelligence reports where it is not possible for the bank to easily obtain information through open source searches or there are doubts about the reliability of open source information, and
- where the bank considers whether to rely on another firm for EDD purposes, it ensures that the extent of EDD measures is commensurate with the risk it has identified and that it holds enough information about the customer to carry out meaningful enhanced ongoing monitoring of the business relationship – the bank must also be satisfied that the quality of EDD is sufficient to satisfy the UK's legal and regulatory requirements.

See ~~ML Reg 7~~ regulation 7 of the Money Laundering Regulations 2007.

16.3.6 Enhanced ongoing monitoring

In addition to guidance contained in ~~Part 1 Box 3.8~~ *FCG* 3.2.9G:

- compliance has adequate oversight over the quality and effectiveness of periodic and event-driven reviews, and
- the firm does not place reliance only on identifying large transactions and makes use of other 'red flags'.

Transaction monitoring

Examples of red flags in transaction monitoring can include (this list is not exhaustive):

- third parties making repayments on behalf of the customer, particularly when this is unexpected
- repayments being made from multiple bank accounts held by the customer
- transactions that are inconsistent with the business activities of the customer
- the purpose of the customer account changing without adequate explanation or oversight
- transactions unexpectedly involving high-risk jurisdictions, sectors or individuals
- early repayment of loans or increased frequency/size of repayments
- accounts with low balances but a high volume of large debits and credits
- cumulative turnover significantly exceeding the customer's income/expected activity
- debits being made shortly after credits of the same value are received
- the customer making frequent transactions just below transaction monitoring alert thresholds
- debits to and credits from third parties where there is no obvious explanation for the transaction, and
- the customer providing insufficient or misleading information when asked about a transaction, or being otherwise evasive.

Customer reviews

Banks must keep the documents, data or information obtained as part of the CDD process up to date. This will help banks ascertain that the level of risk associated with the business relationship has not changed, or enable them to

take appropriate steps where it has changed.

Examples of factors which banks may consider when conducting periodic reviews.

- Has the nature of the business relationship changed?
- Does the risk rating remain appropriate in the light of any changes to the business relationship since the last review?
- Does the business relationship remain within the firm's risk appetite?
- Does the actual account activity match the expected activity indicated at the start of the relationship? If it does not, what does this mean?

Examples of measures banks may take when reviewing business relationships:

- assessing the transactions flowing through the customer's accounts at a business relationship level rather than at an individual transaction level to identify any trends
- repeating screening for sanctions, PEPs and adverse media, and
- refreshing customer due diligence documentation, in particular where this is not in line with legal and regulatory standards.

See ~~ML Reg 8~~ regulation 8of the Money Laundering Regulations 2007.

16.3.7 Sanctions

In addition to guidance contained in ~~Part 1 Chapter 7~~ *FCG* 7, examples of good practice include:

- firms carrying out 'four-eye' checks on sanctions alerts before closing an alert or conducting quality assurance on sanctions alert closure on a sample basis
- firms regularly screening their customer database (including, where appropriate, associated persons, eg, directors) against sanctions lists using systems with fuzzy matching capabilities, and
- specified individuals having access to CDD information held on each of the bank's customers to enable adequate discounting of sanctions alerts.

17 Managing bribery and corruption risk in commercial insurance broking – update (2014)

17.1 Introduction

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

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

17.1.2 In November 2014 we published a thematic review of how commercial insurance intermediaries manage bribery and corruption risk. We looked at ten intermediaries' anti-corruption systems and controls and the extent to which these intermediaries had considered our existing guidance, enforcement cases and the findings from thematic work, particularly our 2010 review of 'anti-bribery and corruption in wholesale insurance broking'. This sample also included five intermediaries that had been part of the sample in 2010.

17.1.3 While most intermediaries had begun to look at their ABC systems and controls, this was work in progress and more improvement was needed. We found that most intermediaries we saw were still not managing their bribery and corruption risk effectively. Business-wide bribery and corruption risk assessments were based on a range of risk factors that were too narrow and many intermediaries failed to take a holistic view of the bribery and corruption risk associated with individual relationships. Half of the due diligence files we reviewed were inadequate and senior management oversight was often weak.

17.1.4 The contents of this report are reflected in ~~Chapters 1 and 2 of Part 1 of this Guide~~ *FCG* 1 and *FCG* 2.

17.2 The ~~FCA~~ *FCA* findings

17.2.1 You can read the findings of our thematic review here: http://www.fca.org.uk/news/tr14-17-managing-bribery-and-corruption-risk-in-commercial-insurance-broking

17.3 Themes

17.3.1 Governance

This section complements guidance in ~~Part 1, Boxes 2.1 and 6.1 and Part 2, Box 9.1~~ *FCG* 2.2.1G and *FCG* 6.2.1G and *FCTR* 9.3.1G

- As part of their ABC governance structures, intermediaries may consider appointing an ABC officer with technical expertise and professional credibility within the intermediary.
- Intermediaries should ensure that responsibility for oversight and management of third-party introducers and other intermediaries is clearly allocated.

17.3.2 Management information (MI)

This section complements guidance in ~~Part 1, Boxes 2.1 and 6.1 and Part 2, Box 9.1~~ *FCG* 2.2.2G *and FCTR* 9.3.1G

Examples of ABC MI which intermediaries may consider providing include:

- details of any business rejected in the relevant period because of bribery and corruption concerns, including the perception that the risk of bribery and corruption associated with the business might be increased, and
- details, using a risk-based approach, of staff expenses, gifts and hospitality and charitable donations, including claims that were rejected and cases of non-compliance with the intermediary's policies where relevant.

Intermediaries may consider providing ABC MI about third-party introducers and other intermediaries.

Examples of such MI include:

- a breakdown of third-party introducers and other intermediaries, in chains that are involved in business generation, with details of the business sectors and countries they work in
- the amount of business each third-party introducer or other intermediary generates
- how much the immediate third-party introducer or other intermediary with whom the intermediary has a direct relationship is paid and on what basis (fees, commission, etc), and
- details of the third-party introducer's role, including the services they provide and the basis of the commission or other remuneration they receive.

17.3.3 Risk assessment

This section complements guidance in ~~Part 1, Boxes 2.3 and 6.2 and Part 2, Boxes 9.2 and 9.3~~ *FCG* 2.2.4G, *FCG* 6.2.2G and *FCG* 6.2.4G and *FCTR* 9.3.2G and *FCTR* 9.3.3G

Business-wide risk assessments

Intermediaries should identify and assess the bribery and corruption risk across all aspects of their business.

Examples of factors which intermediaries should consider when assessing risk across their business.

- Risks associated with the jurisdictions the intermediary does business in, the sectors they do business with and how they generate business.

- Risks associated with insurance distribution chains, in particular where these are long. This includes taking steps to understand the risk associated with parties that are not immediate relationships, where these can be identified. Parties that are not immediate relationships may include, in addition to the insured and the insurer, entities such as introducers, sub-brokers, co-brokers, producing brokers, consultants, coverholders and agents.

- Risks arising from non-trading elements of the business, including staff recruitment and remuneration, corporate hospitality and charitable donations.

Risk assessments and due diligence for individual relationships

The risk-rating process for individual third-party introducer and client relationships, for example the producing broker, should build on the intermediary's business-wide risk assessment.

Examples of factors intermediaries may consider when assessing bribery and corruption risk associated with individual relationships include:

- the role that the party performs in the distribution chain

- the territory in which it is based or in which it does business

- how much and how the party is remunerated for this work

- the risk associated with the industry sector or class of business, and

- the governance and ownership of the third party, including any political or governmental connections.

Intermediaries should decide on the level of due diligence, and which party to apply due diligence to, based on their assessment of risk associated with the relationship. This may include other parties in the insurance chain and not just their immediate contact. Where it is not possible or feasible to conduct due diligence on other parties, intermediaries should consider alternative approaches, such as adjustments to the level of monitoring to identify unusual or suspicious payments.

Examples of the type of information which intermediaries may obtain as part of the due diligence process include:

- other intermediaries' terms of business and identification documentation, including information about their anti-corruption controls

- checks, as risk dictates, on company directors, controllers and ultimate beneficial owners, considering any individuals or companies linked to the client, PEP screening and status, links to a PEP or national government, sanctions screening, adverse media screening and action taken in relation to any screening hits, and

- for third-party introducers, details of the business rationale.

17.3.4 Ongoing monitoring and reviews

This section complements guidance in ~~Part 1, Boxes 2.4, 6.3 and 6.4 and Part 2, Box 9.3~~ *FCG* 2.2.5G, *FCG* 6.2.3G and *FCG* 6.2.4G and *FCTR* 9.3.3G

Examples of ongoing monitoring and review for ABC purposes include:

- payment monitoring, including a review of payments to identify unusual or suspicious payments
- refreshing due diligence documentation
- ensuring that the business rationale remains valid – this may include a review of third-party introducers' activities
- re-scoring risk where necessary, including based on the outcome of internal or external reviews or audits
- updating PEP screening, sanctions screening and adverse media screening, and
- taking a risk-based approach to ongoing monitoring measures applied to directors, controllers, ultimate beneficial owners and shareholders relevant to third-party relationships, which is consistent with the risk rating applied at the outset of a relationship.

17.3.5 Payment controls – insurance broking accounts

This section complements guidance in ~~Part 1, Boxes 6.3 and 6.4 and Part 2, Boxes 9.4 and 9.9~~ *FCG* 6.2.3G and *FCG* 6.2.4G and *FCTR* 9.3.4G and *FCTR* 9.3.9G

- Intermediaries should set meaningful thresholds for gifts and hospitality that reflect business practice and help identify potentially corrupt actions.
- When determining whether a payment is appropriate, staff responsible for approving payments should consider whether the payment is in line with the approved scope of the third-party relationship.

17.3.6 Payment controls – accounts payable

This section complements guidance in ~~Part 1, Boxes 6.3 and 6.4 and Part 2, Box 9.4~~ *FCG* 6.2.3G and *FCG* 6.2.4G and *FCTR* 9.3.4G

- Intermediaries should consider whether an absence of recorded gifts, entertainment, expenses and donations may be due to reporting thresholds being too high and/or staff being unaware of the requirement to report.

17.3.7 Training and awareness

This section complements guidance in ~~Part 1, Boxes 2.5 and 6.3 and Part 2, Boxes 9.6 and 9.9~~ *FCG* 2.2.6G and *FCG* 6.2.3G and *FCTR* 9.3.6G and *FCTR* 9.3.9G

Examples of initiatives to supplement ABC training and awareness include:

- creating a one-page aide-mémoire for staff, listing key points on preventing financial crime and the whistleblowing process, to which staff could easily refer, and
- appointing a compliance expert within each business area who provides ABC advice to staff.