Consultation Paper

CP11/12**

Financial Services Authority

Financial crime:

A guide for firms

Financial Services Authority

June 2011

Contents

© The Financial Services Authority 2011

The Financial Services Authority invites comments on this Consultation Paper. Comments should reach us by 21 September 2011.

Comments may be sent by electronic submission using the form on the FSA's website at: www.fsa.gov.uk/Pages/Library/Policy/CP/2011/cp11_12_response.shtml.

Alternatively, please send comments in writing to:

Kate Higginson
Financial Crime Policy and Risk Unit
Financial Services Authority
25 The North Colonnade
Canary Wharf
London E14 5HS

Telephone: 020 7066 4336
Fax: 020 7066 4337
Email: cp11_12@fsa.gov.uk

It is the FSA's policy to make all responses to formal consultation available for public inspection unless the respondent requests otherwise. A standard confidentiality statement in an email message will not be regarded as a request for non-disclosure.

A confidential response may be requested from us 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 Tribunal.

Copies of this Consultation Paper are available to download from our website – www.fsa.gov.uk. Alternatively, paper copies can be obtained by calling the FSA order line: 0845 608 2372.

Acronyms used in this paper

AML	anti-money laundering
CBA	cost benefit analysis
CDD	customer due diligence
CP	Consultation Paper
EU	European Union
FCA	Financial Conduct Authority
FSA	Financial Services Authority
FSMA	Financial Services and Markets Act 2000
JMLSG	Joint Money Laundering Steering Group
PEP	politically exposed person
SYSC	Senior Management Arrangements, Systems and Controls sourcebook

1 Overview

Purpose

1.1 This Consultation Paper (CP) seeks views on our proposal for a new regulatory guide, *Financial Crime: a guide for firms*, which is referred to throughout this CP as 'the Guide'.

What is the Guide?

1.2 The Guide provides guidance on steps firms can take to reduce their financial crime risk. It reflects the wide experience we have built up in the course of our work on financial crime prevention. We are publishing it for three main reasons:

a) transparency: to share more of our knowledge and explain and improve understanding about our expectations of firms' financial crime systems and controls;

b) accessibility: to collate existing FSA statements on financial crime and publish them in an easily accessible, user friendly format; and

c) reinforcement: to underline our ongoing commitment to tackling financial crime.

1.3 The Guide does not contain rules and imposes no new requirements on firms. It does, however, contain guidance, in the form of self-assessment questions and examples of good and poor practice, which firms can use to assess and improve their existing approaches to meeting their legal and regulatory obligations in relation to financial crime.

1.4 All FSA guidance is non-binding. There will therefore be no requirement for firms to 'comply' with the Guide's contents. But we will expect firms to be aware of the guidance it contains and, where appropriate, to consider how to translate it into more effective policies and controls. The Guide is not intended to compete or conflict with existing industry guidance like the Joint Money Laundering Steering Group's guidance for the financial services sector.

1.5 The Guide covers many types of financial crime risk, but it is not intended to be all-encompassing. It focuses more on the areas in which we have conducted thematic work; we have included other topics to make sure the material is more representative of our financial crime remit. The Guide does not deal with market misconduct, which is dealt with in detail in the FSA's Market Conduct (MAR) sourcebook. And there are other subjects on which we touch only lightly; for example, fraud against firms, where firms should have incentives to protect themselves. Our guidance focuses on areas in which firms are less likely to take unprompted preventative or remedial action.

1.6 The version of the Guide on which we are consulting includes guidance arising from two new thematic review reports, which are being published at the same time as this CP. They are: *Banks' management of high money-laundering risk situations* and *Mortgage fraud against lenders*.

1.7 We intend to keep the Guide under review and to expand and update it to include material from future thematic reviews and where new risks are identified.

Structure of this CP

1.8 The remainder of this CP is set out as follows:

- Chapter 2 sets out our proposals in relation to the Guide and discusses its structure, content and status in greater detail;
- Annexes 1 and 2 provide a cost benefit analysis and compatibility statement on our proposals;
- Annex 3 lists the questions asked in this CP; and
- Appendix 1 sets out the proposed text of the Guide.

Equality and diversity

1.9 Some of the guidance in this CP gives rise to possible equality and diversity issues relating to the classification of certain jurisdictions as 'high risk' for financial crime. Such classifications are necessary and justifiable but we urge firms to consider whether the approaches they have adopted to manage their risk are proportionate and whether there are steps they can take to mitigate any negative effects on individuals from the jurisdictions in question. These issues are discussed in more detail in Chapter 2.

Next steps

1.10 The consultation period for this CP ends on Wednesday 21 September 2011. We plan to publish feedback on this CP, along with the final amended text of the Guide, in a Policy Statement in Q4 of this year.

Who should read this CP?

1.11 This paper is important to all firms and their advisors as it explains steps that firms can take to reduce the risk of being used to further financial crime and by doing so help themselves to meet relevant legal obligations.

CONSUMERS

This CP is targeted at firms and will be of limited relevance to consumers. Some consumers or consumer groups may be interested in the guidance we propose to give to firms about their systems and controls to prevent fraud on or by their customers.

2

Financial crime: a guide for firms

2.1 This chapter sets out our proposals for a new regulatory guide, *Financial crime: a guide for firms*.

2.2 Firms are subject to numerous requirements relating to financial crime. For example, most are subject to the Money Laundering Regulations 2007; and all must comply with the Proceeds of Crime Act 2002 and the UK sanctions regime. When the Bribery Act 2010 comes into force on 1 July 2011, failing to prevent bribery will become a corporate offence.

2.3 In addition, FSA Principles require firms to conduct their business with integrity and with due skill, care and diligence; and, to take reasonable care to organise and control their affairs responsibly and effectively with adequate risk management systems. Rules in the Senior Management Arrangements, Systems and Controls (SYSC) sourcebook, SYSC 3.2.6R and 6.1.1R, also require firms to establish, implement and maintain adequate policies and procedures for countering the risk that they might be used to further financial crime. And there are further Handbook provisions in SYSC 3.2.6A – 3.2.6J and SYSC 6.3 relating specifically to firms' anti-money laundering systems and controls.

2.4 We already expect firms to have systems and controls in place to deal with the financial crime threats they face and we can, and do, take action against those who do not. The Guide is intended to be a useful, practical addition to our currently limited formal guidance on this subject, and to help firms better understand and meet their legal and regulatory obligations.

Why we are publishing the Guide

2.5 In the course of our work on financial crime, we have built up a lot of experience about the actions firms can take to protect themselves, their consumers and society from criminal behaviour. We have already shared much of this knowledge, for example, through reports

which set out the findings of our thematic reviews on topics related to financial crime. But there is scope for us to do more. By publishing the Guide, and doing so now, we want to:

- improve transparency and clarity by sharing more of our knowledge and increasing understanding about our financial crime expectations and focus;
- make existing published information more accessible by collating it in a form that is easy to find and use; and
- reinforce prominently our commitment to tackling financial crime.

2.6 **Transparency:** We want firms to understand our expectations and be familiar with the kind of issues and matters on which we will focus when we are considering firms' anti-financial crime systems and controls. The Guide will reflect our accumulated experience and help firms to assess better the adequacy of their existing arrangements; and, to identify for themselves areas where improvements might be made, reducing the risk that deficiencies will be drawn to their attention by supervisors or during thematic work.

2.7 **Accessibility:** Most of the material in the Guide is drawn from previously published thematic reviews. Our thematic work has been valuable in assisting firms to assess the appropriateness of their systems and controls to prevent financial crime. But as the number of thematic reports, and the period of time over which we have published them, grows, it becomes harder for firms to keep track of the useful information the reports contain. Also, many of the reviews focused on specific sectors, when we consider that much of the information they contain is also useful and relevant to other types of firm. We therefore consider it important to collate that material so that firms are easily able to find and use it. We have chosen a format and structure for the Guide that we consider will best achieve this aim.

2.8 **Reinforcement:** The FSA is on track to make the transition to a new regulatory structure at the end of 2012. The government has confirmed that, as part of that restructure, the FSA's responsibilities for financial crime will pass to the new Financial Conduct Authority (FCA).[1] It is intended that the FCA 'will have a free-standing duty in discharging its general functions to have regard to the importance of taking action intended to minimise the extent to which it is possible for regulated business to be used for purposes connected with financial crime'. The Prudential Regulation Authority will also 'be alert to risks arising to its objectives from firms being used for or themselves engaging in criminal activity'.

2.9 Publishing the Guide at this point provides an opportunity to confirm the FSA's focus on tackling financial crime – of all types, not just money laundering or the latest thematic review topic – through the transition period. This is a commitment which we expect the FCA will continue.

Q1: Do you support our proposal to publish the Guide? If not, why not?

1 See the government's consultation document '*A new approach to financial regulation: building a stronger system*': http://www.hm-treasury.gov.uk/d/consult_newfinancial_regulation170211.pdf, in particular paragraphs 4.32 ff.

Q2: Do you think the Guide will achieve our publication aims? If not, why not?

Framework, status and application of the Guide

2.10 The Guide does not contain rules and will not be part of the Handbook. But it will sit, along with other regulatory guides, on the Handbook pages of our website. The Guide contains guidance within the meaning of s.157 of the Financial Services and Markets Act 2000, much of which is guidance on rules. It is subject to FSA consultation disciplines.

2.11 The Guide imposes no new requirements on firms. It is largely derived from the findings and examples of good and poor practice contained in previously published thematic reviews. It should, therefore, contain no surprises for firms, who should already be considering the questions and examples provided when they assess their systems and controls.

2.12 We have also included guidance arising from the findings of two new thematic reviews on: *Banks' management of high money-laundering risk situations* and *Mortgage fraud against lenders*. Some further new material has been added so that the Guide reflects more fully our financial crime concerns: for example, the section on proliferation financing. While this is not material we have previously published, it does reflect our existing expectations. The Guide does not deal with market misconduct.

2.13 The guidance in the Guide is not binding. Its status is that of any other FSA guidance.[2] We will not presume that failure to follow a piece of guidance amounts, by itself, to a breach of our rules. The Guide is not a checklist of things that a firm must do or not do in order to meet its anti-financial crime obligations and should not be used as such by firms or FSA supervisors. But we will expect firms to be aware of guidance which *is* applicable to them and to consider applicable guidance when establishing, implementing and maintaining their anti-financial crime systems and controls. It is also reasonable to expect that we will continue to check that firms can explain how they are complying with our rules and their other legal obligations, whether or not that involves applying good practice included in the Guide.

2.14 The Guide will contain something of relevance to all firms. But the extent to which guidance applies will depend on the nature of a firm's business as well as the firm's size and complexity. Where guidance applies only (or particularly) to some firms, this is indicated in the text. In this way, we have tried to save firms time and uncertainty by enabling them to identify quickly guidance which is relevant for them. For example, the chapter on weapons proliferation is directed at UK banks carrying out trade finance business and those engaging in activities such as project finance and insurance.

2.15 The Guide is not intended to replace, compete or conflict with existing guidance on financial crime from other authorities or trade bodies. In particular, the FSA will continue

2 For further explanation on FSA guidance and its status, see p.24 of the *Reader's Guide: an introduction to the Handbook*, paragraphs 2.22-2.27 of the *Enforcement Guide*, and the following page of the FSA's website: www.fsa.gov.uk/Pages/About/What/guidance/index.shtml.

to consider whether firms have followed relevant provisions of the Joint Money Laundering Steering Group's guidance for the UK financial services sector when deciding whether conduct amounts to a breach of applicable requirements. The Guide has also been written with reference to guidance prepared by the Ministry of Justice on adequate procedures under the Bribery Act 2010.

Q3: Do you consider that the Guide sets out with sufficient clarity which of its provisions apply to which firms? If not, how could we make it clearer?

Structure and scope of the Guide

2.16 The Guide is divided into chapters, each dealing with a particular financial crime risk. Each chapter opens with a box clearly indicating the types of firm to which the material in the chapter is most relevant.

2.17 Chapters are divided into sections, each focusing on a particular aspect of firms' systems and controls. These sections provide:

a) self-assessment questions; and

b) examples of good and poor practice.

These enable a firm to understand our expectations and test the adequacy of their current arrangements. Most chapters also contain case studies where a firm's conduct failed to meet our requirements and resulted in enforcement action. All chapters provide links to further information.

Q4: Is the Guide's structure and the use of self-assessment questions, good and poor practice and cases studies, helpful and clear? How could we make it clearer or more useful?

Q5: What other comments do you have about the structure and scope of the Guide?

Updating the Guide

2.18 We will keep the Guide under review and will update it to add new material, including from future thematic reviews, and incorporate emerging risks; and to remove guidance which ceases to be relevant.

Contents of the Guide: Part 1

Introduction

2.19 The introduction to Part 1 of the Guide explains the Guide's structure and status. It discusses the uses to which it may be put (including by FSA supervisors).

Financial crime

2.20 The financial crime chapter of the Guide provides guidance which is relevant to financial crime generally rather than just to a specific risk. It draws on comments made in specific thematic reviews which could apply in a broader context. For example, several thematic reports note that it is good practice for firms to have written policies and procedures. We have stated this once, in the 'policies and procedures' section of the financial crime chapter rather than repeating it in each subsequent chapter.

2.21 The Chapter is divided into sections on:

a) governance;

b) structure;

c) risk assessment;

d) policies and procedures;

e) staff recruitment, vetting, training and awareness; and

f) quality of oversight.

2.22 Guidance that is more topic-specific (such as the role of the MLRO in governance) is included in the chapter of the Guide dealing with the relevant topic.

AML

2.23 The anti-money laundering chapter provides examples of systems and controls firms can, and in some cases must, have in place to meet obligations under the Money Laundering Regulations 2007, EU Regulation 1781/2006 (the Payer Information Regulation) and our money laundering rules in SYSC 3.2 and 6.3.

2.24 The chapter draws attention to the JMLSG's guidance for the UK financial sector and confirms that the FSA will, when considering a firm's systems and controls, consider whether the firm has followed the relevant provisions of the JMLSG guidance. It is divided into sections on:

a) governance;

b) the Money Laundering Reporting Officer;

c) the firm's assessment of the risks of money laundering;

d) customer due diligence (CDD) checks;

e) ongoing monitoring;

f) high-risk situations;

g) reporting suspicions; and

h) record-keeping and reliance on others.

Thematic review of high money-laundering risk situations

2.25 The AML chapter incorporates guidance proposed in our report on the FSA's thematic review of *Banks' management of high money-laundering risk situations,* which is being published at the same time as this CP. The review focused on how banks managed risks associated with correspondent banking relationships, wire transfer payments and high-risk customers, including politically exposed persons (PEPs).

2.26 The main objective of the review was to assess whether banks had robust and proportionate systems and controls in place to:

a) identify, detect and prevent the misuse of correspondent banking facilities;

b) meet the requirements to identify the originators of international wire transfers; and

c) reduce the risk of corrupt PEPs and other high-risk customers abusing the UK banking system.

Although we identified some examples of good AML risk management, we found serious weaknesses common to many firms, particularly in relation to the approach to, and quality of, enhanced due diligence and monitoring of high-risk relationships; and the weighting given to AML risk as considered against profitability of accounts and reputational or regulatory risk.

2.27 Although the thematic review focused solely on banking groups in the UK which engaged in significant international activity exposing them to high-risk business, the guidance arising from our findings will be relevant to any firm that is subject to the Money Laundering Regulations 2007 or our anti-money laundering provisions in SYSC. The findings of our review are not subject to consultation, but the resulting guidance is, and it is set out in full in the Annex to this CP, in Chapter 12 of Part 2 of the Guide.

Terrorist financing

2.28 This chapter focuses mainly on whether firms have systems and controls that enable them to meet legal requirements on the provision of information to authorities investigating terrorism and its funding. It also provides guidance on wire transfers.

Fraud

2.29 Guidance in the chapter on fraud is drawn from several places, including the thematic review report, *Firms' high-level management of fraud risk*. We do not propose to deal with fraud on firms in great detail as we consider that firms should have incentives to protect themselves and that the Guide is better focused on areas in which they are less motivated to take unprompted preventative or remedial action.

2.30 The Chapter is divided into sections on:

a) preventing losses from fraud;

b) mortgage fraud; and

c) investment fraud, which includes fraud involving share sales, unauthorised deposit taking or unauthorised collective investment schemes.

Thematic review of mortgage fraud against lenders

2.31 The fraud chapter incorporates guidance arising from our review of *Mortgage fraud against lenders,* which is being published at the same time as this CP. The aim of the review was to assess the adequacy of lenders' systems and controls to detect and prevent mortgage fraud. Although we saw examples of good management of mortgage fraud risks, we also identified weaknesses common to many firms. In particular, we identified vulnerabilities in relation to the management of third party relationships and the resourcing of frontline fraud prevention areas, such as firms' underwriting and anti-fraud teams.

2.32 As with the AML review, while we are not consulting on our findings, we welcome your comments on the guidance we propose to introduce as a result. This is included in the Annex to this CP, in Chapter 11 of Part 2 of the Guide.

Data security

2.33 This chapter is drawn from our April 2008 report, *Data security in financial services*, which found widespread weaknesses in firms' approach to data protection. Of particular concern was the failure of many firms to recognise the financial crime risk that poor data security controls presented. The chapter contains sections on:

a) governance;

b) fallacies of data loss and identity fraud; and

c) controls.

Bribery and corruption

2.34 The chapter on bribery and corruption is drawn from our May 2010 report, *Anti-bribery and corruption in commercial insurance broking*. The report stated that firms who were subject to the review needed to do more to minimise the risk of becoming involved in bribery or corruption. Weaknesses of systems and controls in relation to third parties were of particular concern, and this is reflected in the proposed guidance.

2.35 The chapter is divided into sections on:

a) governance;

b) risk assessment;

c) policies and procedures;

d) dealing with third parties; and

e) staff recruitment, vetting and training.

2.36 Although our thematic review focused on commercial insurance broking, we consider our proposed guidance relevant to all financial sectors. This chapter is therefore applicable to all firms. It is consistent with, but is not intended to replace or compete with, the Ministry of Justice's guidance on the Bribery Act 2010.

Sanctions

2.37 Guidance in the sanctions chapter is drawn from our April 2009 report, *Financial services firms' approach to UK financial sanctions*. The report found weaknesses in firms' (particularly small firms') awareness of the UK financial sanctions regime. This section therefore highlights some key requirements as well as guidance firms can put in place to help them comply with their sanctions obligations.

2.38 The chapter is divided into sections on:

a) governance;

b) risk assessment;

c) screening customers against sanctions lists; and

d) matches and escalation.

Proliferation financing

2.39 As noted in paragraph 2.14, the guidance in the proliferation chapter will be applicable to a narrow range of firms. It focuses on the quality and nature of firms' customer due diligence and assessment of risk.

Part 1 annex

2.40 Part 1 contains an annex explaining common terms relevant to financial crime. It is provided for reference purposes only and is not a list of defined terms used in the Guide. The Guide does not make use of Handbook Glossary definitions.

Q6: What comments do you have on the contents of the Guide? Do you have comments on the specific chapters or the annex of Part 1?

1) Introduction

2) Financial crime systems and controls

3) Anti-money laundering (including guidance arising from the AML thematic review)

4) Countering terrorist financing

5) Fighting fraud (including guidance arising from the mortgage fraud thematic review)

6) Data security

7) Combating bribery and corruption

8) Financial sanctions and asset freezes

9) Countering weapons proliferation financing

10) Annex 1

Contents of the Guide: Part 2

2.41 Part 2 of the Guide collates statements of good and poor practice from previous thematic reviews on topics related to financial crime which we consider still to be of relevance. This material is guidance and has the same status as the guidance in Part 1 of the Guide. Each chapter contains a short summary of the review with a table setting out the examples of good and poor practice we identified. For those who want more detail on a particular review, each chapter also includes a link to the published report.

Q7: Is the inclusion of Part 2 of the Guide useful? What comments do you have on its contents?

Q8: Are there are topics not covered in the Guide which you would find it useful for us to address?

Equality and diversity

2.42 We have conducted an initial assessment of the effect on equality of the publication of this guidance. This assessment suggests that the main effects arise in relation to race, in particular nationality, due to the risk of discrimination arising in connection with the identification of certain jurisdictions as high risk for financial crime. A summary is set out below. We will finalise our assessment, taking into account any comments we receive.

2.43 Effective risk assessment and management is fundamental to firms' compliance with their financial crime obligations. Jurisdiction is a key consideration for firms when determining the risks associated with entering or maintaining a particular business relationship, as certain jurisdictions present a higher money-laundering risk. There are various reasons why this might be the case, including that the jurisdiction's legal framework relating to anti-money laundering and counter terrorist financing is weak; because it is subject to sanctions; or, because it suffers from high levels of corruption or other crime.

2.44 There are important, objective reasons for classifying jurisdictions as high risk. But such a classification has the potential to impact negatively on individuals from those jurisdictions if, for example, it is harder for them to obtain financial services as a result. Firms have a duty not to discriminate against individuals with characteristics such as race that are protected under equality legislation. They should therefore consider what steps they can take to mitigate this potential negative impact.

- We would question the adoption of a blanket policy of refusing services solely on the basis that the applicant was a national of a high-risk jurisdiction; a case-by-case assessment based on appropriate, risk-based due diligence would lower the impact for affected individuals.
- Similarly, policies which require firms to consider a person's links with high-risk jurisdictions – for example, whether they are resident or conduct business there – will provide a more objective and comprehensive basis for identifying and assessing risk, and will better support a firm's efforts to reduce its financial crime risk than assessing on the basis of nationality alone.

Q9: What comments do you have on our assessment of the equality and diversity issues we have identified?

Annex 1:
Cost benefit analysis

Introduction

1. This annex sets out our estimates of the costs and analysis of the benefits associated with the introduction of the Guide. We are not obliged by FSMA to carry out a cost benefit analysis (CBA) when issuing guidance. However, we have publicly committed to do so when we consider that guidance meets at least one of the following criteria:

   - it may materially impact market structures;
   - it may change firms' behaviour in a way which is not already accepted in the market;
   - it is not reasonably predictable from the Principle (without it being a new requirement).[3]

2. The Guide includes both previously published and new guidance material.

3. We have carried out a CBA on the new guidance material because we considered that it may give rise to material costs and may also potentially change some firms' behaviour.

4. In respect of guidance material in the Guide previously published in FSA thematic reviews, fact sheets and one-minute guides, the Guide consolidates and clarifies this guidance to make it easier for firms to access and use. We considered that the inclusion of such material in the Guide would generate no material costs, and therefore is not likely to trigger any of the three criteria given above. This is because firms already consider, for example, the good and poor practice included in published thematic reviews. We carried out pre-consultation on this material to test the reasonableness of our assumption. The feedback we received broadly supports our view.

3 See our 2007 publication '*Principles based regulation: focusing on outcomes that matter*', http://www.fsa.gov.uk/pubs/other/principles.pdf.

Regulatory failure and benefits

5. The FSA's Handbook contains a small amount of rules and guidance related to financial crime. Firms may not always find these sufficient to understand fully their obligations or our expectations.

6. We have attempted to address this issue in the past by publishing additional material, particularly the findings of thematic reviews on topics related to financial crime. These reports have included examples of good practice that firms could adopt to meet their legal and regulatory obligations. Anecdotal evidence on recent thematic reviews suggests that firms value the reports and act upon them to improve their systems and controls. However, there are limitations to the effectiveness of providing information about our expectations to firms in this way. As time passes, firms may have less regard to the findings of thematic reviews: for example if they are less aware of older reviews or because they consider them less relevant. As the number of thematic reports grows, it becomes harder for firms to trace and use the information they contain than it would be if the material was collated in one place. Also, thematic reports are often specific to a particular sector. Where they contain information which may be useful and relevant to other types of firm, this may result in some uncertainty for these firms.

7. By reiterating and expanding applicable thematic material and by giving it the status of FSA guidance, the Guide is expected to improve the clarity and transparency of the FSA's expectations. By bringing guidance together in one place, the Guide will make it easier for firms to identify relevant guidance, which may slightly reduce compliance costs. By regularly updating the Guide we will ensure that firms are aware of our ongoing expectations.

8. Our two new thematic reviews, *Banks' management of high money-laundering risk situations* (the AML review) and *Mortgage fraud against lenders* (the mortgage fraud review) identified weaknesses in a number of firms' systems and controls to prevent financial crime. These weaknesses appeared in some cases partly to be due to firms' failure to understand fully their obligations and our expectations. Publishing new guidance in relation to high money-laundering risk situations and mortgage fraud prevention should improve firms' understanding of both.

9. In particular, the proposed guidance on high money-laundering risk situations explains how firms can manage risks associated with high-risk customers, correspondent banking relationships and wire transfer payments by having more robust and proportionate systems and controls. Implementation of this guidance would reduce the risk of UK banks handling the proceeds of corruption or other financial crime. This is discussed in more detail in paragraphs 2.25 to 2.27 of the main CP text.

10. The mortgage fraud review identified vulnerabilities, including in relation to the management of third party relationships and the resourcing of front-line fraud prevention areas such as lenders' underwriting and anti-fraud teams. The proposed guidance on mortgage fraud will help lenders assess the adequacy of their current systems and controls in detecting and preventing mortgage fraud in these particular areas.

11. The FSA will use the guidance included in the Guide in its normal supervisory process, as was the case with the statements of good and poor practice published in thematic reports in the past. It may improve the efficiency of the supervisory process, if firms understand our expectations better and are therefore better equipped to discuss with supervisors those areas of most concern for the FSA. As such, publication of the Guide may reduce the risk of firms being used to further financial crime to the extent that it is effectively used in the supervisory process and that, by improving firms' understanding of how to comply with requirements, it also improves their compliance. Better fraud prevention controls may also lead to a reduction in fraud losses for firms.

Costs

12. Sections below analyse the following types of costs: direct costs to the FSA, compliance costs to firms, and indirect costs.

Direct costs to the FSA

13. Publishing the Guide will generate no incremental costs to the FSA because any costs will be met from existing budgets. There may be some opportunity costs, however, from updating the guide periodically.

14. Also, we may receive more queries about the Guide than the other published materials from which its guidance is drawn because of its more prominent status and profile. But the additional resource required to respond to these queries is likely to be balanced by a reduction in queries from those previously unsure of our expectations about firms' financial crime systems and controls.

Compliance costs to firms

15. As part of pre-consultation, we sent three cost questionnaires to a number of trade associations and firms.

    1) The first questionnaire asked about costs firms may incur as a result of the inclusion in the Guide of: (1) previously published material; and (2) new material arising other than in relation to the AML and mortgage fraud reviews (in particular, the section on proliferation financing).

    2) The second and third questionnaires asked about firms' views on costs they may incur due to material in the Guide drawn from the AML and mortgage fraud reviews. In each case, we set out the guidance arising from the review which we considered might give rise to material costs. Respondents were asked to identify the types of incremental cost they might incur as a result of the guidance, and to provide estimates of their anticipated one-off and ongoing costs.

16. The analysis below assesses one-off and ongoing incremental compliance costs that firms may incur as a result of us publishing the Guide. Estimates, where available, are based on estimates provided by firms.

Previously published materials

17. The majority of the proposed Guide consolidates statements that have been published in the past, primarily in FSA thematic reviews on topics related to financial crime. We anticipate that this type of material will generate some one-off compliance costs to firms, primarily associated with carrying out gap analysis and updating internal publications and training. For example, including references to the Guide in training materials and process manuals.

18. Respondents to our first survey anticipated no material incremental costs attributable to gap analysis. This was because large firms that have specialised financial crime resources expected to absorb gap analysis costs as business as usual. While some respondents suggested there could be gap analysis costs for small firms, none provided estimates of these costs. Based on our experience we have estimated that gap analysis could result in one-off costs equivalent to one to five staff days per firm depending on the nature of its business. Based on a daily rate for a compliance officer of about £290 including overheads,[4] cost per firm could range between £290 and £1500.

19. Respondents to our survey indicated that they do not expect firms significantly to change their systems, practices or policies in light of the guidance already available in the public domain. We therefore expect no ongoing incremental compliance costs.

New guidance

20. The following sections of the Guide contain new guidance:

- Chapter 3, 'Anti-money laundering' (this chapter also includes previously published guidance);
- Box 5.2, 'Mortgage Fraud – Lenders'; and
- Chapter 9, 'Countering weapons proliferation financing'.

21. Responses to pre-consultation surveys indicated that, apart from those areas discussed below, the proposed new guidance would generate no material costs.

22. Firms and trade associations surveyed indicated several types of one-off costs that could be incurred because of the new guidance material on anti-money laundering and mortgage fraud. No respondents identified costs associated with the guidance on proliferation financing; we expect that if there are any costs, these would be absorbed as part of the general gap analysis of the Guide.

4 We based our estimate on an annual salary of £52,000 plus overheads at 30 per cent giving a daily rate of about £290.

23. Firms will incur a one-off cost from carrying out a gap analysis focused specifically on the new anti-money laundering and mortgage fraud guidance. That is, firms reviewing their existing systems and controls, policies and procedures to identify whether or not any improvements could be made.

24. Many respondents stated that gap analysis costs would not be material. Where a firm expected to incur material costs, this depended greatly on the nature of firm's business, in particular, the number of customers that could be classified as high-risk, its current anti-money laundering and mortgage fraud prevention practices and whether analysis would be carried out using internal or external resource. These factors explain the wide range of cost estimates provided below. These limitations also did not allow us to reliably estimate costs to industry.

25. Based on responses to the survey on AML guidance, the combined estimate of necessary staff time both to identify and make necessary improvements ranged from 2 to 170 man days, where necessary changes were identified. The estimates provided by firms did not vary based on firm size, with both smaller and larger firms providing estimates at either end of the range. Based on the daily rates provided by respondents, this would give a range of cost of £300 to £170,000 per firm for guidance associated with the AML review. Estimates from the mortgage fraud review survey were either not material or between 35 to 40 days, or £5,250 to £40,000.

26. Respondents to the AML review survey provided a wide range of estimates of one-off costs associated with introducing or improving – or improving firms' understanding of - automated transaction monitoring systems. These ranged from £2,000 to £150,000 per firm affected. However, most firms stated that appropriate systems were already in place. Respondents also identified one-off costs associated with commissioning reports or otherwise doing further enhanced due diligence in relation to existing very high-risk customers. Costs depended on the number of customers categorised as very high risk. Estimates ranged from a flat rate estimate of two to ten man days; to estimates of £500 to £10,000 per customer per firm. Again, as it is unclear what proportion of firms is likely to incur any costs at all, we have not been able to estimate the total one-off cost to industry.

27. The table below lists areas of guidance arising from the AML and mortgage fraud reviews where some firms have identified that they may incur greater than material incremental ongoing compliance costs. Ranges of cost estimates given below vary greatly because the impact of the guidance will vary depending on the nature of a firm's business including the level of its exposure to high money-laundering risk situations. Estimates are therefore indicative based on data provided by respondents. We have not always provided separate estimates for small, medium and large firms as costs did not always vary with the size of the firm for the reasons discussed above. We have not provided an aggregate estimate of ongoing incremental costs per firm as not all firms would incur costs in the range, and not all firms that would incur costs would incur each type of cost identified.

28. The guidance from the AML review will have more impact on firms who engage in business that presents a higher money-laundering risk. But we do not have data about the number of such firms, or the number of customers categorised as high risk that each firm has. For these reasons we have not estimated the number firms that may incur ongoing compliance costs as a result of the guidance arising from the AML review.

Part 1: Ongoing annual incremental compliance costs from both AML and mortgage fraud guidance

Annual incremental compliance costs incurred from:		Range of costs where material:
1	Providing additional, ongoing training about high money-laundering risk situations and mortgage fraud for staff in relevant roles.	£600 to £52,000 per firm Costs will depend on the firm's size and the extent to which it deals with high-risk customers; or its exposure to mortgage fraud.
2	Expanding internal audit functions or otherwise increasing the amount of quality assurance work carried out in relation to high money-laundering risk situations or mortgage fraud.	£150 to £50,000 for a small or medium firm Firms provided estimates of an extra two to ten staff days per year or an additional employee. These costs fall within the given range. We do not expect large firms to incur material costs. All large firms who responded to our survey indicated that they already had adequate procedures in place.

Part 2: Specific ongoing annual incremental costs from guidance on anti-money laundering

Annual incremental compliance costs incurred from:		Range of costs where material:
1	Improving policies and procedures better to identify and understand what a 'high-risk customer' is for AML purposes.	£150 to £500,000 per firm Costs will depend on the extent to which the firm is exposed to high money-laundering risk situations.
2	Carrying out more thorough reviews of high AML risk customers.	£1,500 to £500,000 per firm Costs per firm will depend on the number of high money-laundering risk customers. Firms did not indicate the number of affected customers. Where a firm indicated that they would commission external intelligence reports, cost per report could vary from £500 to £10,000.
3	Increasing the amount of senior management involvement in customer approval and review.	£750 to £48,000 for a small or medium firm Large firm respondents indicated either that they already had adequate procedures in place or that they had few high-risk customers.
4	Improving the identification of a customer's source of wealth and source of funds.	£225 to £60,000 for a small to medium firm We do not expect large firms to incur material costs. All large firms who responded to our survey indicated that they already had adequate procedures in place.

5	Enhanced due diligence on respondent banks.	£300 to £50,000 for a small to medium firm The estimate for small and medium firms varies greatly because some firms may incur travel costs in addition to staff costs. Survey responses indicated that large firms are less likely to incur costs as a result of this guidance; only one large firm identified an ongoing annual cost, of £500,000. This suggests that where larger firms identify the need for improvement, they will incur greater costs to the extent that they deal with more respondent banks.
6	Searching for phrases in payment messages which may indicate a bank or customer trying to conceal their identity.	£75 to £123,000 for a small to medium firm We do not expect large firms to incur material costs. All large firms who responded to our survey indicated that they already had adequate procedures in place.
7	Establishing a specialist team to undertake risk-based sampling of incoming customer payments, with subsequent detailed analysis to identify banks initiating cross-border payments containing inadequate or meaningless payer information (wire transfers guidance).	£300 to £371,000 for a small to medium firm All large firms who responded to our survey indicated that they already had adequate procedures in place, suggesting that large firms are not likely to incur material costs.

Part 3: Specific ongoing annual incremental costs from guidance on mortgage fraud

Annual incremental compliance costs incurred from:		**Range of costs where material:**
1	Seeking to identify when deterioration in employees' financial circumstances indicated increased vulnerability to involvement in fraud.	£150 to £132,000 per firm affected Estimates varied depending on whether firms would vet all staff or apply a more risk-based approach. We expect large firms to incur greater costs as they will have a greater number of staff to vet.
2	Engaging in cross-industry fraud prevention initiatives.	£6,500 to £10,000 for a small to medium firm No material costs expected for large firms as survey responses indicated that they are likely already to engage in such initiatives.
3	Reduction in the size of lenders' third party panels.	£750 to £11,220 for a small to medium firm No material costs expected for large firms as survey responses indicated that they are likely already to actively manage their panels.
4	Having systems that can detect brokers 'gaming' a firm's systems.	£300 to £10,000 for a small to medium firm No material costs expected for large firms as survey responses indicated that they are likely already to have such systems in place.
5	Having underwriting processes that can identify higher fraud risk applications.	£300 to £212,500 for a small to medium firm No material costs expected for large firms as survey responses indicated that they are likely already to have such processes in place.

6	Improving management information (MI) and its effectiveness.	£450 to £5,000 for a small to medium firm No material costs expected for large firms as survey responses indicated that they are likely already to have effective MI.

Indirect costs

29. We have not received any evidence from our pre-consultation exercise to suggest indirect costs such as material changes in firm incentives, or business models, so we do not expect any material indirect costs to arise. For this reason we also do not expect any impact on competition.

Q10: Do you have any comments on this cost benefit analysis?

Annex 2:
Compatibility statement

1. This section explains our reasons for concluding that the proposals set out in this Consultation Paper are compatible with our general duties under section 2 of the Financial Services and Markets Act 2000 (FSMA) and our regulatory objectives set out in sections 2(2) and 3 to 6 FSMA.

Compatibility with our statutory objectives

2. Our regulatory objectives are set out in section 2(2) FSMA. We believe that our proposals will further these objectives, including in the following ways:

The reduction of financial crime

3. The Guide provides guidance on systems and controls firms can put in place to reduce the risk of their being used to further financial crime. It consolidates existing FSA statements on this topic, making it easier for firms to understand our expectations and check the adequacy of their existing arrangements.

Securing the appropriate degree of protection for consumers

4. The Guide includes provisions relating to fraud, including mortgage and share sale fraud and data security, which can have a considerable and direct impact on consumers. It may encourage firms to consider whether they are doing enough to protect their customers from fraud and reduce the social harm caused by financial crime.

Maintaining confidence in the financial system

5. The failure of firms to establish, implement and maintain adequate financial crime systems and controls exposes the financial system to money laundering and increases the risk to society by facilitating other serious crimes, including drug and people trafficking and terrorism. This can impact on the reputation of individual firms or on UK financial services and the UK as a whole. By providing guidance to help firms assess the adequacy of their

systems and controls we are helping to mitigate this risk and encouraging confidence in the financial system.

Compatibility with the Principles of Good Regulation

6. Section 2(3) of FSMA requires that, in carrying out our general functions, we must have regard to a number of specific matters, known as the 'principles of good regulation'. We consider that our proposals are compatible with these principles, of which the following are particularly relevant:

The need to use our resources in the most efficient and economic way

7. The Guide will improve the efficiency with which we can supervise firms' compliance with their financial crime obligations by improving the transparency of our expectations, meaning firms will have a clearer understanding of what our expectations are and will be better prepared to discuss with us how they are meeting their obligations – whether or not by following the guidance in the Guide. The resource requirements of keeping the Guide up-to-date will not significantly exceed those of maintaining internal guidance on the topic and will be met from existing resources.

The responsibilities of those who manage the affairs of authorised persons

8. The Guide imposes no new requirements on senior executive management of firms. However, by collating guidance relating to our existing expectations, the Guide may make it easier for firms and their senior managers to understand the expectations we have of them.

The principle that a burden or restriction should be proportionate to the benefits, considered in general terms, which are expected to result from the imposition of that burden or restriction

9. The Guide does not impose additional requirements on firms. We have conducted a cost benefit analysis of the Guide and are satisfied that the costs involved in implementing our proposals will be proportionate to the benefits. As set out in the CBA in Annex 1 we do not expect any impact on competition.

The most appropriate way for us to meet our regulatory objectives

10. In line with section 2(1) FSMA, we believe our proposals to be the most appropriate way of meeting our regulatory objectives. We have considered not collating guidance material from thematic reviews. However, as discussed in the CP, this option would reduce the clarity and accessibility of the guidance. For this reason, we considered that publishing the Guide would prove a more efficient way of meeting our objectives.

Annex 3:
List of questions

Q1: Do you support our proposal to publish the Guide? If not, why not?

Q2: Do you think the Guide will achieve our publication aims? If not, why not?

Q3: Do you consider that the Guide sets out with sufficient clarity which of its provisions apply to which firms? If not, how could we make it clearer?

Q4: Is the Guide's structure and the use of self-assessment questions, good and poor practice and cases studies, helpful and clear? How could we make it clearer or more useful?

Q5: What other comments do you have about the structure of the Guide?

Q6: What comments do you have on the contents of the Guide? Do you have comments on the specific chapters or the annex of Part 1?

1) Introduction

2) Financial crime systems and controls

3) Anti-money laundering (including guidance arising from the AML thematic review)

4) Countering terrorist financing

5) Fighting fraud (including guidance arising from the mortgage fraud thematic review)

6) Data security

7) Combating bribery and corruption

8) Financial sanctions and asset freezes

9) Countering weapons proliferation financing

10) Annex 1

Q7: Is the inclusion of Part 2 of the Guide useful? What comments do you have on its contents?

Q8: Are there are topics not covered in the Guide which you would find it useful for us to address?

Q9: What comments do you have on our assessment of the equality and diversity issues we have identified?

Q10: Do you have any comments on this cost benefit analysis?

Appendix 1:

Draft text of *Financial crime: a guide for firms*

Financial Crime: a guide for firms

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

Contents

1 Introduction

1.1 This Guide provides practical assistance and information for firms of all sizes and across all sectors on actions they can take to counter the risk that they might be used to further financial crime. Its contents are drawn primarily from FSA thematic reviews, with some additional material included to reflect other aspects of our financial crime remit. The Guide does not cover market misconduct, detailed rules and guidance on which are contained in the Market Conduct (MAR) sourcebook.

1.2 Part 1 provides guidance on financial crime systems and controls, both generally and in relation to specific risks such as money laundering, bribery and corruption and fraud. Annexed to Part 1 is a list of common and useful terms. It is provided for reference purposes only and is not a list of 'defined terms'. Nor does the Guide use the Handbook Glossary of definitions.

1.3 Part 2 provides summaries of, and links to, FSA thematic reviews of various financial crime risks and sets out the full examples of good and poor practice that were included with the reviews' findings.

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

This Guide is not a checklist of things that all firms should be doing or not doing to reduce their financial crime risk, and will not be used as such by FSA supervisors.

1.5 The material in the Guide does not form part of the Handbook, but much of it is guidance on rules and it is 'general guidance' as defined in section 158 of the Financial Services and Markets Act 2000 (FSMA). The guidance is not binding and we will not presume that a firm's departure from our guidance indicates that it has breached our rules. But we do expect firms to take account 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. Firms should also expect us to check that they can explain how they are complying with our rules and their other legal obligations, whether or not that involves applying good practice included in the Guide.

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

1.7 The FSA will continue to have regard to whether firms have followed the relevant provisions of the Joint Money Laundering Steering Group's guidance for the UK financial sector on the prevention of money laundering and combating terrorist financing when deciding whether conduct amounts to a breach of relevant requirements.

How to use this Guide

1.8 Throughout this Guide, material is set out as follows:

This box indicates the **types of firm** to which the material is most relevant.

1.9 Each section discusses how firms tackle a different type of financial crime. Sections open with a short passage giving context to what follows. Where the word 'must' is used, this indicates a legal obligation under applicable legislation or a regulatory requirement in the FSA's Handbook.

Box 1.1: Financial crime: a guide for firms

The Guide looks at key aspects of firms' efforts to counter different types of crime.

Self-assessment questions:

- These questions will help you to consider whether your firm's approach is appropriate.
- The FSA may follow similar lines of inquiry when discussing financial crime issues with firms. (Text in brackets expands on this; the examples of good and poor practice below may also help.)
- This guide is aimed at firms big and small; material will not necessarily apply to all situations. If a self-assessment question applies to certain types of firm, this is indicated by *italics*.

Good practice:

- This box provides illustrative examples of **good practices**.
- We would draw comfort from seeing **evidence** that these practices take place.
- Note that **if these practices are lacking** it may not be a problem.The FSA would consider whether a firm has taken other measures to meet its obligations.

Poor practice:

- This box provides illustrative examples of **poor practices**.
- Some show a lack of commitment, others fall short of regulatory requirements and expectations; some, as indicated in the text, may be **criminal offences**.

Box 1.1: Case studies

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

1.10 Where to find out more:

- Most sections close with some sources of further information.

2 Financial crime systems and controls

This section is relevant to **all firms**.

2.1 All firms must take steps to defend themselves against financial crime, but a variety of approaches is possible.

Box 2.1: Governance

Senior management should 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, 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.)
- What **drives** the firm's financial crime efforts? What outcomes does it seek to achieve?

Good practice:

- Senior management **set the right tone** and demonstrate leadership on financial crime issues.
- A firm takes **active steps** to prevent criminals taking advantage of its services.
- A firm has a **strategy** for self-improvement on financial crime.
- There are clear criteria for **escalating** financial crime issues.

Poor practice:

- There is little evidence of senior management **involvement** and **challenge** in practice.
- A firm concentrates on **narrow compliance** with **minimum regulatory standards**: little engagement with the issues.
- Financial crime issues are dealt with on a purely **reactive** basis.

Box 2.2: Structure

Firms' **organisational structures** to combat financial crime may differ. Some large firms will have a single unit that coordinates efforts and which may report to the head of risk, the head of compliance or directly to the CEO. Other firms may spread responsibilities more widely. There is no '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.)

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's financial crime work is adequately **resourced** (staff, IT systems, etc).

Poor practice:

- Defences against financial crime are **uncoordinated** and **fragmented**, with no effort made to understand where gaps exist.
- Financial crime officers are relatively **junior** and lack access to senior management. They are often **overruled** without documented justification.
- Financial crime departments are **under resourced** and senior management are reluctant to address this.

Box 2.3: Risk assessment

In order that firms apply proportionate systems and controls, they need to gain a **thorough understanding of their financial crime risks**.

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**?
- 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?)

Good practice:

- Risk assessment is a **continuous** process based on the best-available information from internal and external sources.
- The firm assesses where risks are greater and **concentrates its resources** accordingly.
- The firm actively considers the **costs of crime** to customers.

Poor practice:

- Risk assessment is a **one-off** exercise.
- Efforts to understand risk are **piecemeal** and lack coordination.
- 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).

Box 2.4: Policies and procedures

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

Self-assessment questions:

- How often are your firm's policies and procedures **reviewed**, and at what level of seniority?
- 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?
- For *larger groups*, how does your firm ensure that policies and procedures are **disseminated** and **applied** throughout the business?

Good practice:

- There is **clear documentation** of a firm's approach to complying with its legal and regulatory requirements in relation to financial crime.
- Policies and procedures are **regularly reviewed** and **updated**.
- **Internal audit** or another independent party monitors the effectiveness of policies, procedures, systems and controls.

Poor practice:

- A firm has **no written policies** and **procedures**.
- The firm **does not tailor** externally produced policies and procedures to suit its business.
- The firm takes **inadequate steps** to **communicate** policies and procedures to relevant staff.
- The firm **fails to review** policies and procedures in light of events.
- The firm **fails to check** whether policies and procedures are applied consistently and effectively.

Box 2.5: Staff recruitment, vetting, training and awareness

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.

Self-assessment questions:

- What is your approach to **vetting** staff? (Vetting should be proportionate and risk-based and should be repeated or ongoing where appropriate, for example for staff in high-risk roles.)
- How does your firm ensure that its employees are **aware of financial crime risks**? (Look for appropriate training programmes covering AML, fraud control, data security, etc, both when staff join and on an ongoing basis. Firms should be able to identify which staff have been trained and when.)
- How does the firm ensure that training is of **consistent quality** and is kept up to date?
- Is training **tailored** to particular roles?

Good practice:

- Staff in higher-risk roles are subject to **more thorough vetting**.
- **Tailored** training is in place to ensure staff knowledge is adequate and up to date.
- New staff in **customer-facing** positions receive financial crime training tailored to their role before being able to interact with customers.
- Training has a strong **practical** dimension (e.g. case studies) and some form of testing.
- There is **evidence** that staff **understand** their responsibilities (e.g. computerised training contains a test).
- **Whistleblowing** procedures are clear and accessible, and protect staff confidentiality.

Poor practice:

- Staff are **not competent** to carry out preventative functions effectively, exposing the firm to financial crime risk.
- Training dwells unduly on **legislation and regulations** rather than practical examples.
- Training material is **not kept up to date**.
- The firm **fails to identify** training needs.
- There are no **training logs** or tracking of employees' training history.
- Training **content** lacks management sign-off.
- Training does not cover **whistleblowing** and **escalation** procedures.

Box 2.6: Quality of oversight

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

Self-assessment questions:

- How does your firm ensure that its approach to reviewing the effectiveness of financial crime systems controls is **comprehensive**?
- What are the **findings** of recent internal audits and compliance reviews on topics related to financial crime?
- How has the firm progressed **remedial measures**?

Good practice:

- **Internal audit** and **compliance** routinely test the firm's defences against financial crime, including specific financial crime threats.
- Decisions on allocation of compliance and audit resource are **risk-based**.
- Management **engage constructively** with this process.
- *Smaller firms* seek **external help** if needed.

Poor practice:

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

3 Anti-money laundering (AML)

This section is relevant to **all firms who are subject to the Money Laundering Regulations 2007 or the money laundering provisions in SYSC (see Annex 1 for common terms)**. Mortgage brokers, general insurers and general insurance intermediaries have more limited responsibilities, but may still find the guidance useful. For example, it may assist them in establishing and maintaining systems and controls which will help them to meet the requirements of the Proceeds of Crime Act 2002 to which they are subject.

3.1 The Money Laundering Regulations 2007 (referred to in this chapter as the Regulations) impose a range of requirements on firms.

3.2 The Joint Money Laundering Steering Group (JMLSG) produces guidance for firms in the UK financial sector on how to comply with their legal and regulatory obligations related to anti-money laundering and terrorist financing. When considering a firm's systems and controls, we will consider whether the firm has followed relevant provisions of the JMLSG's guidance.

Box 3.1: Governance

We expect **senior management** to take responsibility for the firm's anti-money laundering (AML) measures.

Self-assessment questions:

- Who has **overall responsibility** for establishing and maintaining effective AML controls? Are they sufficiently senior?
- What are the **reporting lines**? Is there evidence that issues have been escalated where warranted?
- How regularly does senior management commission **reports** from the **Money Laundering Reporting Officer (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?

Good practice:

- Decisions on accepting or maintaining high money-laundering risk relationships are reviewed and challenged **independently** of the business relationship and escalated to senior management or committees.
- **Reward structures** for relationship managers take account of any failings related to anti-money laundering compliance.
- The firm identifies and manages the risk that a relationship manager might become **too close** to customers.

Poor practice:

- There is **little evidence** that AML is **taken seriously** by senior management. It is seen as a legal or **regulatory necessity** rather than a matter of true concern for the business.
- The board **never considers** MLRO reports.
- There is **no meaningful record** or evidence of senior management considering money laundering risk.
- **Remuneration structures** for relationship managers give rise to potential conflicts of interest.

Box 3.2: The Money Laundering Reporting Officer (MLRO)

This section applies to firms who are required to appoint an MLRO.

Firms must appoint an individual as MLRO. The MLRO should have oversight of the firm's compliance with its anti-money laundering obligations.

Self-assessment question:

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

Good practice:

- The **MLRO** is independent, knowledgeable, robust and well-resourced, and can pose effective challenge where warranted.
- The MLRO has a **direct reporting line** to executive management or the board.

Poor practice:

- The MLRO **lacks credibility** and has insufficient clout to pose effective challenge, whether because of **inexperience** or **lack of seniority**.

Box 3.3: The firm's assessment of the risks of money laundering

Firms must put in place systems and controls to identify, assess and monitor money-laundering risk. They 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 considered the risks associated with different types of customer, product, business line, geographical location, and delivery channel e.g. internet, telephone, branches?)
- How does your firm identify high-risk customers? Do your processes ensure that **all high-risk situations**, not just those singled out by the Regulations, are picked up?
- Are risk assessments, including updates, **reviewed, challenged, approved** and **documented** appropriately?
- Is there evidence that the firm's risk assessment **informed its decisions** about accepting or maintaining relationships?

Good practice:

- The firm's risk assessment **informs** the **design** of anti-money laundering controls.
- The firm has identified **good sources of information** on money laundering risks.
- 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 reputation;
  - source of wealth;
  - source of funds;
  - expected account activity;
  - sector risk; and
  - involvement in public contracts.

Poor practice:

- Risk assessment is a **one-off exercise**.
- Risk assessments **fail to assess meaningfully** the risk of doing business with customers/respondent banks located in higher-risk countries.
- An inappropriate **customer classification system** makes it almost impossible for a customer to be classified as 'high-risk'.
- Higher-risk countries are allocated low-risk scores to **avoid enhanced due diligence measures**.
- Allowing relationship managers to **override customer risk** scores without sufficient evidence to support their decision.
- Risk assessments on money laundering are influenced by the **potential profitability** of new or existing relationships.
- No clear **audit trail** to show why customers are rated as high, medium or low risk.

Box 3.4: Customer due diligence (CDD) checks

Firms must **identify** their customers, and, where applicable, the beneficial owner, and then **verify** their identity. Firms must also understand the **purpose** and intended nature of the customer's relationship with the firm in order to obtain a complete picture of the risk associated with the business relationship and to provide a meaningful basis for subsequent monitoring. We expect *all firms* to identify and manage the financial crime risk their customers present.

Box 3.7 below considers enhanced due diligence.

Self-assessment questions:

- Does your firm apply **customer due diligence** procedures in a risk-sensitive way?
- How does the firm identify the customer's **beneficial owner(s)**?
- Are procedures **sufficiently flexible** to cope with customers who cannot provide more common forms of ID?

Good practice:

- Where **electronic checks are used** for CDD purposes, the firm understands their limitations.
- The firm can cater for **customers who lack common forms of ID** (such as the socially excluded, those in care, etc).
- The firm **does not rely entirely on a single source**, such as a commercial PEP database, to identify riskier customers.
- 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.

Poor practice:

- Procedures are **not risk-based**: the firm applies the same CDD measures to products and customers of varying risk.
- The firm has **no method for tracking** whether checks on customers are complete.
- The firm allows '**cultural difficulties**' to get in the way of proper questioning to obtain necessary CDD information.
- Staff do **less CDD** because a customer is referred by senior executives or influential people.
- The firm has **no procedures** for dealing with situations requiring enhanced due diligence. **This breaches the Regulations**.
- The firm does not look beyond the 25% shareholding threshold when identifying the customer's beneficial owner. **This breaches the Regulations**.

Box 3.5: Ongoing monitoring

A firm must **scrutinise transactions** to ensure that they are consistent with what was revealed by customer due diligence checks. It must also take steps to ensure its knowledge about the customer remains current.

Box 3.8 looks at enhanced ongoing monitoring.

Self-assessment questions:

- How are transactions **monitored** to spot potential money laundering?
- What is the mix between **manual monitoring** and **automated systems**? Is this effective?
- 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?)

Good practice:

- *A large retail firm* complements its other efforts to spot potential money laundering by using an **automated system** to monitor transactions.
- *Small firms* are able to apply credible **manual procedures** to scrutinise customers' behaviour.
- The '**rules**' underpinning monitoring systems are understood by the relevant staff and updated to reflect new trends.
- The firm 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.

Poor practice:

- The firm does not have qualitative information about the business relationship and is therefore **unable to conduct meaningful monitoring**.
- The MLRO can provide **little evidence** that **unusual transactions** are brought to their attention.
- Staff **always accept a customer's explanation** for unusual transactions at face value and do not probe further.
- No effort is made to ensure CDD information is **up to date. This is a breach of the Regulations**.
- The firm places **unwarranted faith** in the effectiveness of automated monitoring systems.

Box 3.6: 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 complex or opaque beneficial ownership structures, as well as transactions which are unusual, lack an obvious economic or lawful purpose, are complex or large or might lend themselves to anonymity.

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

- **Non-face-to-face CDD**: this is where the customer has not been physically present for identification purposes, perhaps because business is conducted by telephone or on the internet.
- **Correspondent banking:** where a correspondent bank is outside the EEA, the UK bank should thoroughly understand its correspondent's business, reputation, and the quality of its defences against money laundering and terrorist financing. Senior management must give approval to each new correspondent banking relationship.
- **Politically exposed persons (PEPs)**: a customer may be a PEP if they hold, or are related to or associated with someone who holds, certain prominent public offices. In these circumstances a firm must apply extra due diligence and monitoring measures to ensure it does not handle the proceeds of crime. A senior manager 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.

Box 3.7: 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 is who they say they are and that the purposes of the business relationship are legitimate; as well as increasing opportunities to identify and deal with concerns that they are not. **Box 3.3** considers risk assessment.

Self assessment questions:

- How does EDD differ from standard CDD? How are issues flagged during the due diligence process **followed up** and **resolved**? Is this adequately documented?
- How is EDD information **gathered, used** and **stored**?
- What involvement do senior management or committees have in **approving high-risk customers**? Are their decisions based on **impartial assessments** of money laundering risks?

Good practice:

- All high-risk relationships are **checked** by the MLRO or their team.
- The firm establishes the legitimacy of, and documents, high-risk customers' **source of wealth** and **source of funds**.
- Where money laundering risk is very high, the firm obtains **independent** internal or external **intelligence reports**.
- '**Staff knowledge**' is documented and challenged during the CDD process.
- The firm satisfies itself that it is appropriate to rely on due diligence performed by **other entities** in the same group.
- The firm proactively **follows up gaps in, and updates**, CDD during the course of a relationship.
- A *correspondent bank* seeks to identify PEPs associated with their respondents.
- A *correspondent bank* takes a view on the strength of the **AML regime** in a respondent bank's home country, drawing on discussions with the respondent, overseas regulators and other relevant bodies.
- A *correspondent bank* gathers information about **respondent banks' procedures** for sanctions screening, PEP identification and management, account monitoring, and suspicious activity reporting.

Poor practice:

- Senior management **does not give approval** for taking on high-risk customers. **If the customer is a PEP or a non-EEA correspondent bank, this breaches the Regulations**.
- The firm fails to consider whether a customer's **political connections** mean that they are high risk despite falling outside the Regulations' definition of a PEP.
- The firm **does not distinguish** between the customer's source of funds and their source of wealth.
- A firm relies on intra-group introductions where **overseas standards are not UK-equivalent** or where due diligence data is **inaccessible** because of legal constraints.
- The firm considers the **credit risk** posed by the customer, but not the money laundering risk.
- The firm disregards allegations of **criminal activity** from reputable sources.
- The firm ignores adverse allegations simply because customers hold a UK **investment visa**.
- A firm grants **waivers** from establishing a customer's source of funds, source of wealth and other due diligence without good reason.
- A *correspondent bank* conducts inadequate due diligence on **parents and affiliates** of respondents.
- A *correspondent bank* **over-relies** on the Wolfsberg Group AML questionnaire without making use of other material from the Wolfsberg Group or other sources.

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

Firms must enhance their ongoing monitoring in high-risk situations. The guidance below will be of most relevance to firms who are subject to the Regulations, but *all firms* should take adequate steps to monitor the financial crime risk posed to their business by their customers.

Self-assessment questions:

- How does your firm **monitor** its high-risk business relationships? Are reviews carried out **independently** of relationship managers?
- What **information** do you store in the files of high-risk customers? Is it **meaningful**? 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?

Good practice:

- Key AML staff have a **good understanding** of, and **easy access** to, information about a bank's highest risk/PEP customers.
- New high-risk clients are more closely monitored to confirm or amend **expected account activity**.
- **Alert thresholds** on automated monitoring systems are lower for PEPs and other higher-risk customers. Exceptions are **escalated** to more senior staff.
- Decisions across a group on whether to keep or exit high-risk relationships are **consistent** and in line with the firm's overall risk appetite or assessment.
- The firm carries out **reviews** in light of material changes to a customer's risk profile.

Poor practice:

- The firm treats annual reviews as a **tick-box exercise** and copies information from previous reviews without thought.
- *A firm in a group* relies on others in the group to carry out monitoring **without understanding** what they did and what they found.
- There is **insufficient challenge** to explanations from relationship managers and customers about unusual transactions.
- The firm **focuses too much** on **reputational or business issues** when deciding whether to exit relationships with a high money laundering risk.
- The firm makes no enquiries when accounts are used for purposes **inconsistent with expected activity** (e.g. personal accounts being used for business).

Box 3.9: Reporting suspicions

Firms must **report any knowledge or suspicions** of money laundering to the Serious Organised Crime Agency (SOCA) through a 'Suspicious Activity Report', also known as a 'SAR'. Staff must report their concerns to the firm's nominated officer (see the Annex 1 list of common terms), who must consider whether a report to SOCA is necessary based on all the information at their disposal.

Self-assessment questions:

- How does the **decision-making** process related to **SARs** work in the firm?
- Is the **procedure** clear to staff?
- Does the **nominated officer** receive reports from within the firm? If not, do they 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?

Good practice:

- All staff **understand escalation procedures** and follow them as required.
- The firm's **SARs** set out a clear narrative of events and include detail that law enforcement authorities can use (e.g. names, addresses, passport numbers, phone numbers, email addresses, car registrations).
- There is a clear process for **documenting** decisions.

Poor practice:

- The nominated officer **passes all internal reports** to SOCA without considering whether they truly are suspicious. These 'defensive' reports are likely to be of little value.
- The nominated officer **dismisses concerns** escalated by staff without reasons being documented.
- The firm **does not train** staff to make internal reports, thereby exposing them to personal legal liability and increasing the risk that suspicious activity goes unreported.
- The nominated officer **turns a blind eye** where a SAR might harm the business.
- A *third party administrator* **passes SARs on** to its principal rather than report itself.

Box 3.10: Record keeping and reliance on others

Firms must keep copies or references to a customer's identity documents, as well as transaction records, for **five years** after the business relationship ends. Where a firm is **relied on by others** to do due diligence checks, it must keep its records of those checks for five years from the date it was relied on. Firms must also keep records of their business sufficient to enable the FSA to monitor their compliance with regulatory requirements.

Self-assessment questions:

- Can your firm retrieve records **promptly** in response to a Production Order (see Annex 1 for common terms)?
- If the firm **relies on others** to carry out AML checks (see 'Reliance' in Annex 1), is this within the limits permitted by the Regulations? And how does it gain satisfaction that it can rely on these firms?

Good practice:

- Records of customer ID and transaction data can be **retrieved quickly**.
- Where the firm routinely relies on checks done by a third parties (for example, a fund provider relies on an IFA's checks), it **requests sample documents** to test their reliability.

Poor practice:

- The firm keeps customer records and related information in a way that **restricts** the **firm's access** to these records or their timely sharing with authorities. **Access to CDD and related records is required under the Regulations.**
- When tested, significant proportions of customer ID records **cannot be retrieved** in good time.
- The firm cannot provide evidence of a **third party** agreeing to be relied upon.
- There are **gaps** in customer records.

Box 3.11: Case study – poor controls

We fined Alpari (UK) Ltd, an online provider of foreign exchange services, £140,000 in May 2010 for poor anti-money laundering controls. It 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 the firm did business over the internet and had customers from higher-risk jurisdictions. The firm failed to ensure that resources in its compliance and anti-money laundering areas kept pace with the firm's significant growth. Alpari's former money laundering reporting officer was also fined £14,000 for failing to fulfil his duties.

See our press release for more information: www.fsa.gov.uk/pages/Library/Communication/PR/2010/077.shtml

3.3 To find out more, see:

- The Money Laundering Regulations 2007: www.legislation.gov.uk/uksi/2007/2157/contents/made
- EU Regulation 1781/2006 on information on the payer accompanying transfers of funds: www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:345:0001:0009:EN:PDF
- SOCA's website contains information on how to report suspicions of money landering: www.soca.go.uk
- The **Joint Money Laundering Steering Group's** guidance on measures firms can take to meet their anti-money laundering obligations is available from its website: www.jmlsg.org.uk
- The findings of the FSA's thematic review of banks' management of high money laundering risk situations: www.fsa.gov.uk/pubs/other/aml_ final_report.pdf

4 Countering terrorist financing

All firms are at risk of their services being used by terrorists.

4.1 Firms have an important role to play in providing information that can assist authorities with their counter-terrorist investigations.

Box 4.1: Countering the finance of terrorism

Many of the controls firms have in place in relation to terrorism will overlap with their anti-money laundering measures. Policies and procedures may cover a) reporting suspicions of terrorist financing to the authorities, b) responding to requests from the authorities for information (such as Production Orders), c) internal escalation of issues (e.g. when a customer is arrested or charged with terrorism offences) and d) transaction monitoring.

Self-assessment questions:

- Is it clear who is responsible for **liaison with the authorities**?
- Is there a documented process for responding to **Production Orders**, with clear timetables?
- Is there evidence the firm is able to **retrieve records** in a **timely** manner?

Good practice:

- An **incident response plan** sets out the firm's plan if a customer is arrested on suspicion of a terrorist offence or charged.
- A firm identifies **sources of information** on terrorist financing risks: court judgments, press reports, SOCA alerts, Financial Action Task Force (FATF) typologies etc. This information informs the design of **transaction monitoring systems**.
- In *larger firms*, the intelligence unit works effectively with **other teams** such as counter-fraud staff.

Poor practice:

- A firm provides **extraneous** and **irrelevant detail** in responding to a Production Order.
- A firm cannot retrieve **customer records**.
- **Training** programmes do not discuss terrorist financing.
- *An international firm* has not identified known terrorist groups operating in **countries** in which it has a presence or done business.
- A firm **assumes** that terrorist funds flow only *into* the UK and does not consider the risks of **outbound payments** being linked to terrorism.

Box 4.2: Customer payments

This section is relevant to *firms that process electronic cross-border payments for customers*.

Self-assessment questions:

- How does your firm ensure that customer payment instructions contain complete payer information? (For example, does it have proportionate checking procedures in place for payments received?)
- Does the firm review its respondent banks' track record on providing payer data and making appropriate use of cover payments?

Good practice:

- Following processing, banks conduct **risk-based sampling** for inward payments to identify inadequate payer information.
- An intermediary or beneficiary *bank* chases up **missing** information.
- A *bank* sends **dummy** messages to test the effectiveness of filters.
- A *bank* is aware of guidance from **Basel** 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.
- Active engagement in **peer discussions** about taking appropriate action against banks which persistently fail to provide complete payer information.

Poor practice:

- A *bank* fails to make use of the correct **SWIFT message type** for cover payments.
- Compliance with regulations related to international customer payments has not been reviewed by the firm's internal audit or compliance departments.

The following practices breach EU Regulation 1781/2006 on information on the payer accompanying transfers of funds (the Wire Transfer Regulation):

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

Box 4.3: Case study – wire transfer failures

A UK bank that falls short of our expectations when using payment messages does not just risk FSA enforcement action or prosecution; it can also open an institution to 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.

4.2 To find out more, see:

- A FATF report on terrorist financing: www.fatf-gafi.org/dataoecd/28/43/40285899.pdf
- The JMLSG's guidance, a link to which is included at the end of Chapter 3, is also relevant to counter-terrorist financing.
- EU Regulation 1781/2006 on information on the payer accompanying transfers of funds: www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:345:0001:0009:EN:PDF

5 Fighting fraud

This section applies to **all firms**.

5.1 All financial institutions are at risk of being defrauded. The main types of fraud are described in our Annex 1 entry for 'fraud'. The industry has a clear self-interest in guarding against such losses; so we focus our attention on those frauds where third parties can suffer or there is less incentive for firms to take unprompted preventative or remedial action.

Box 5.1: 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 fraud risks it faces, which may have wider effects on its reputation, its customers and the markets in which it operates.

Self-assessment questions:

- What **information** does 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?

Good practice:

- The firm takes a view on what areas of the firm are most **vulnerable** to fraudsters, and tailors defences accordingly.
- Controls adapt to **new fraud threats**.
- The firm engages with **cross-industry efforts** to combat fraud (e.g.: data-sharing initiatives like CIFAS and the Insurance Fraud Bureau; collaboration to strengthen payment systems etc).
- **Fraud response plans** set out how the firm will respond to incidents of fraud.
- **Lessons** are learnt from incidents of fraud.
- **Anti-fraud good practice** is shared widely within the firm.
- To guard against **insider fraud**, staff in high-risk positions (e.g. finance department, trading floor) are subject to enhanced vetting and closer scrutiny. 'Four eyes' procedures (see Annex 1 for common terms) are in place.

Poor practice:

- Senior management appear **unaware** of fraud incidents and trends. No management information is produced.
- **Fraud losses are buried** in bad debts or other losses.
- There is no clear and consistent **definition** of fraud across the business, so reporting is haphazard.
- Fraud risks are not explored when **new products** and **delivery channels** are developed.
- Staff **lack awareness** of what constitutes fraudulent behaviour (e.g. for a salesman to misreport a customer's salary to secure a loan would be fraud).
- **Sales incentives** act to encourage staff or management to turn a blind eye to potential fraud.

• **Enhanced due diligence** is performed on higher-risk customers (e.g. commercial customers with limited financial history - see 'long firm fraud' in Annex 1).	• *Banks* fail to implement the requirements of **Payment Services Regulations** and **Banking Conduct of Business rules**, leaving customers out of pocket after fraudulent transactions are made. • Staff vetting is a **one-off** exercise. • **Remuneration structures** may incentivise behaviour that increases the risk of mortgage fraud.

Box 5.2: Mortgage fraud – lenders

This section is most relevant to *mortgage lenders*.

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 **solicitors, brokers and valuers**?
- Does your firm engage with **cross-industry information-sharing** exercises?

Good practice:	Poor practice:
• A firm's underwriting process can **identify** applications that may present a **higher risk** of mortgage fraud. • Membership of a *lender's* **panels** of brokers, solicitors and valuers is subject to ongoing review. Dormant third parties are identified. • A *lender* **reviews existing mortgage books** to identify and assess mortgage fraud indicators. • A *lender* verifies that funds are being dispersed **in line with instructions** before it releases them. • A *lender* checks whether solicitors register charges with the **Land Registry** in good time.	• A *lender* fails to engage with the FSA's **Information from Lenders** project. • A *lender* **lacks a clear definition** of mortgage fraud, undermining data collection and trend analysis. • A *lender's* panels of solicitors, brokers and valuers are **unmanageably large**. • A *lender* relies solely on the FSA Register when **vetting brokers**. • Underwriters' demanding work targets **undermine** efforts to contain mortgage fraud.

Box 5.3: Mortgage fraud – intermediaries

This section is most relevant to *mortgage intermediaries*.

Self-assessment questions:

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

Good practice:	Poor practice:
• Asking to see **original documentation** whether or not this is required by lenders. • Finding out why a lender has **declined** an application.	• Failing to undertake due diligence on **introducers.** • Accepting all applicant information at **face value.** • Treating due diligence as the **lender's responsibility**.

- Using the FSA's **Information from Brokers** scheme to report intermediaries suspected of involvement in mortgage fraud.

Box 5.4: Enforcement action against mortgage brokers

Since we began regulating mortgage brokers in October 2004, we have banned over 100 mortgage brokers for breaches including deliberately submitting to lenders applications containing false or misleading information and failing to have adequate systems and controls in place to deal with the risk of mortgage fraud. We have referred numerous cases to law enforcement, a number of which have resulted in criminal convictions.

Box 5.5: Investment fraud

This section is relevant to *retail deposit takers*.

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

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

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

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

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

What procedures does your firm have in place to avoid facilitating payments to boiler rooms, unauthorised deposit taking and unauthorised collective investment schemes?

5.2 To find out more, see:

- Details of the FSA's Information from Lenders scheme: www.fsa.gov.uk/pages/doing/regulated/supervise/mortgage_fraud.shtml
- Details of the FSA's Information from Brokers scheme: www.fsa.gov.uk/smallfirms/your_firm_type/mortgage/fraud/report.shtml
- The findings of the FSA's thematic review on mortgage fraud against lenders: www.fsa.gov.uk/pubs/other/mortgage_fraud.pdf
- A fact sheet for mortgage brokers on mortgage fraud: www.fsa.gov.uk/smallfirms/resources/factsheets/pdfs/mortgage_fraud.pdf

6 Data security

This section applies to **all firms**.

6.1 Customers routinely entrust financial firms with sensitive personal data; if this falls into criminal hands, fraudsters can attempt to undertake financial transactions in the customer's name. The Payment Services Regulations 2009 and Banking Conduct of Business rules mean victims of unauthorised payments should not lose their money, but they may nonetheless suffer worry and inconvenience because of identity theft.

Box 6.1: Governance

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?

Good practice:

- There is a clear **figurehead** championing the issue of data security.
- Work, including by internal audit and compliance, is **coordinated** across the firm, with compliance, audit, HR, security and IT all playing a role.
- **Incident response plans** are clear and include notifying customers affected by data loss and offering advice to those customers about protective measures. Accounts are monitored following a data loss to spot unusual transactions.
- The firm seeks **external assistance** if it does not have the necessary resource or expertise to assess data security risk or monitor compliance with standards.
- The firm looks at **outsourcers'** data security practices before doing business, and monitors compliance.

Poor practice:

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

Box 6.2: 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 which successfully detect data loss do so because they have effective risk-management systems. Firms with weak controls or monitoring are likely to be oblivious to any loss. Furthermore, when fraud does occur, a victim rarely has the means to identify where their data was lost because data is held in so many places.

Box 6.3: Controls

Firms have a responsibility to assess the risk of data loss and take reasonable steps to prevent that risk occurring. 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. Firms should 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**?

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

Box 6.4: Case study – protecting customers' accounts from criminals

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

Fraudsters used public information to impersonate customers and obtain policy and bank details from Norwich Union call centres. They were then able to amend customer records (such as address and bank account details) and subsequently request the surrender of customers' policies. Over the course of 2006, 74 policies totalling £3.3m were fraudulently surrendered.

For more, see our press release: www.fsa.gov.uk/pages/Library/Communication/PR/2007/130.shtml

Box 6.5: Case study – data security failings

In August 2010, we fined Zurich Insurance plc £2,275,000 following the loss of 46,000 policyholders' personal details. The firm did not discover that another Zurich company in South Africa had lost an unencrypted back-up tape until a year after it happened.

Our press release has more details: www.fsa.gov.uk/pages/Library/Communication/PR/2010/134.shtml

6.2 To find out more, see:

- The findings of the FSA's thematic review on data security in financial institutions: www.fsa.gov.uk/pubs/other/data_security.pdf
- A one-minute guide for small firms on data security: www.fsa.gov.uk/smallfirms/resources/one_minute_guides/info_gathering/data_security.shtml
- The website of the Information Commissioner's Office: www.ico.gov.uk

7 Combating bribery and corruption

This section is relevant to **all firms**.

7.1 Bribery, whether committed in the UK or abroad, is a criminal offence. Authorised firms are under an additional, regulatory obligation to put in place systems and controls to mitigate corruption risk and to conduct their business with integrity.

7.2 When considering whether their anti-corruption and bribery systems and controls are adequate, firms should also have regard to the Ministry of Justice's guidance on adequate anti-corruption procedures under section 9 of the Bribery Act 2010.

Box 7.1: 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.

Self-assessment questions:

- 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 work?
- Do senior managers lead anti-corruption and bribery efforts **by example**?
- Are **integrity** and **compliance** with relevant anti-corruption legislation considered when discussing **business opportunities**?
- What **information** does senior management receive in relation to bribery and corruption, and how frequently?

Good practice:

- The firm is **committed** to carrying out business fairly, honestly and openly.
- Responsibility for anti-bribery and corruption systems and controls is **clearly documented** and apportioned to a single senior manager with appropriate terms of reference who reports ultimately to the Board.
- Anti-bribery systems and controls are **subject to audit**.
- Management information submitted to the Board ensures they are **adequately informed** of external developments relevant to bribery and corruption and respond to these swiftly and effectively.

Poor practice:

- There is a **lack of awareness** of, or engagement in, anti-bribery and corruption at senior management or Board level.
- An 'ask no questions' culture sees management turn a **blind eye** to how new business is generated.
- **Little or no management information** is sent to the Board about higher-risk third-party relationships or payments.

Box 7.2: Risk assessment

We expect firms to identify and assess their bribery and corruption risks.

Self-assessment questions:

- 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 you do business with and your own business practices, for example your approach to providing corporate hospitality?
- Has the risk of **staff** or **third parties** acting on the firm's behalf **offering** or **receiving bribes** been assessed across the business?
- Could **remuneration structures** increase the risk of bribery and corruption?

Good practice:

- The firm continuously assesses whether **external events** may help it to refine its risk assessments and anti-bribery and corruption systems and controls.
- Corruption risks are assessed in **all jurisdictions** where the firm operates and across all business channels.

Poor practice:

- Compliance departments are **ill equipped** to identify and assess corruption risk.
- For fear of harming the business, the firm classifies as **low risk** a jurisdiction generally associated with **high risk**.
- There is a failure to bolster insufficient in-house knowledge or resource with **external expertise.**

Box 7.3: Policies and procedures

Firms must take adequate steps to prevent their corruption and bribery risks crystallising.

Self-assessment questions:

- When did your firm last **review** its anti-corruption policies and procedures?
- How do you **mitigate** the corruption risks you identified?
- 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?

Good practice:

- The firm **clearly sets out** behaviour expected of those acting on its behalf, with appropriate sanctions.
- There are **unambiguous consequences** for breaches of the firm's anti-corruption policy.
- The firm's staff have access to an anonymous **whistleblowing** hotline to report suspicions of corruption.
- Risk-based, appropriate additional monitoring and due diligence is undertaken for jurisdictions, sectors and business relationships identified as **higher risk**.

Poor practice:

- The firm's anti-corruption function is **under-resourced** and lacks expertise to carry out their role effectively.
- The firm **does not assess** the extent to which staff comply with its anti-corruption policies and procedures.
- The firm's anti-corruption policies and procedures are **out of date**.
- A firm relies on passages in the staff code of conduct that prohibit improper payments, but has no other **controls**.
- The firm **does not respond** to external events that may highlight weaknesses in its anti-corruption systems and controls.

Box 7.4: Dealing with third parties

Firms must 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' and the due diligence required when establishing and reviewing third party relationships?
- How is the use of **third-party introducers** controlled?
- Do you **know** your third party?

Good practice:	Poor practice:
• Where a firm uses third parties to generate business, these relationships are subject to **thorough due diligence** and management oversight. • Third parties are **paid directly** for their work. • Payments to third parties are reviewed and **monitored** by management. The purpose of third-party payments is **recorded**. • There are higher or extra levels of due diligence and approval for **high-risk third-party relationships**.	• *A firm using intermediaries* fails to satisfy itself that those businesses have **adequate controls** to detect and prevent where staff have used bribery to generate business. • The firm is **unable to produce a list** of approved third parties, associated due diligence and details of payments made to them. • The giving or receipt of **cash gifts**. • There is **no checking** of compliance's operational role in approving new third-party relationships and accounts. • A firm **assumes** that long-standing third-party relationships present no bribery or corruption risk.

Box 7.5: Staff recruitment, vetting and training

A firm's systems and controls should enable it to satisfy itself of the suitability of anyone who acts for it. This includes assessing an individual's honesty and competence. The firm should also equip staff with the knowledge and tools to tackle bribery and corruption risks effectively.

Self-assessment questions:

- How has your firm assessed which of its staff are exposed to a **higher risk** for bribery and corruption and how regularly is this assessment reviewed?
- How do you **train** staff in anti-corruption matters? How is training **targeted**?

Good practice:	Poor practice:
• Staff are vetted using a risk-based approach which takes into account financial crime risk. There is **enhanced vetting** for staff in roles with higher bribery and corruption risk. • Staff in relevant roles (e.g. overseas salespeople) receive **targeted** training and guidance on bribery and corruption issues.	• The firm relies on contracts with employment agencies covering staff vetting standards **without checking** periodically that the agency is adhering to them. • The firm fails to provide **meaningful training** on anti-bribery and corruption, especially to staff in higher risk positions.

Box 7.6: 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 Aon failed to question their nature and purpose when it ought to have been reasonably obvious to Aon Ltd that there was a significant risk corruption risk. See our press release: www.fsa.gov.uk/pages/Library/Communication/PR/2009/004.shtml

7.3 To find out more, see:

- The Bribery Act 2010: www.legislation.gov.uk/ukpga/2010/23/contents
- Ministry of Justice guidance: www.justice.gov.uk/downloads/guidance/making-reviewing-law/bribery-act-2010-guidance.pdf (full version) www.justice.gov.uk/downloads/guidance/making-reviewing-law/bribery-act-2010-quick-start-guide.pdf (quick-start guide)
- The findings of our thematic review on anti-bribery and corruption measures in commercial insurance brokers: www.fsa.gov.uk/pubs/anti_bribery.pdf

8 Financial sanctions and asset freezes

All firms are required to comply with the UK's financial sanctions regime. The FSA's role is to ensure that firms have adequate systems and controls to comply with the regime.

8.1 The UK's financial sanctions regime, which freezes the UK assets of certain individuals and entities, is one aspect of the government's wider approach to economic sanctions: other elements include export controls (see the Annex 1 list of common terms) and measures to prevent the proliferation of weapons of mass destruction (see Chapter 9).

8.2 The Treasury maintains a consolidated list of individuals and businesses subject to financial sanctions. This list includes people and organisations based in the UK. Providing funds to any person on the list is a breach of sanctions; a licence must first be obtained from the Treasury's dedicated Asset Freezing Unit for the payment to be legal.[1] If firms become aware of a breach, they must notify the Asset Freezing Unit.

Box 8.1: Governance

An individual of sufficient authority should be responsible for sanctions compliance.

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.)

Good practice:

- An individual of **sufficient authority** is responsible for adherence to the sanctions regime.
- Senior management is **adequately involved** in devising and approving the procedures and policies for financial sanctions screening in the firm.
- It is clear who is **responsible for screening** against lists in different situations (e.g. when being passed customers from agents or other companies in the group).

Poor practice:

- Senior management is **not made aware of target matches**, breaches or weaknesses in screening systems.
- The firm believes payments to sanctioned individuals and entities are **permitted** when the sums are small. Without a licence from the Asset Freezing Unit, this could be a **criminal offence**.
- No **internal audit** resource is allocated to monitoring sanctions compliance.
- Some business units in a *large organisation* think they are **exempt**.

1 Where sanctioned individuals are designated under the Terrorism Orders, it is prohibited to provide any financial service, although general licences are in place to allow these individuals 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).

Box 8.2: Risk assessment

A firm should consider which areas of its business are most likely to provide 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?

Good practice:

- The firm's risk assessment is **comprehensive**.
- *A firm with international operations*, or that deals in currencies other than sterling, understands the requirements of relevant **local financial sanctions** regimes.
- *Small firms*: the firm is **aware** of the sanctions regime and where it is most vulnerable, even if risk assessment is only informal.

Poor practice:

- There is **no process** for updating the risk assessment.
- A *UK firm operating in another currency* has **not considered** whether it is subject to that country's financial sanctions regime.
- The firm assumes financial sanctions **only apply to money transfers** and so has not assessed its risks.

Box 8.3: 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 has granted a licence.)

Self-assessment questions:

- When are customers screened against the **consolidated list?** (Screening should take place at the time of customer take-on. Good reasons are needed to justify the risk posed by retrospective screening.)
- If a customer was **referred** to the firm, how does the firm ensure the person is not on the sanctions list? (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?)

Good practice:

- The firm has considered what **mixture** of manual and automated screening is most appropriate.
- There are quality control checks over **manual screening**.
- Where a firm uses automated systems these can make '**fuzzy matches**' (able to identify similar spellings of names).
- Where customers are companies, the firm screens **directors** and known **beneficial owners**.
- Where the firm maintains an account for a listed individual, the status of this account is **clearly flagged** to staff.

Poor practice:

- The firm only screens customers **retrospectively**.
- The firm assumes that an intermediary has screened a customer, but **does not check** this.
- Where a firm uses automated systems, it does not understand how to **calibrate** them and does not check whether the number of hits is unexpectedly high or low.
- An *insurance company* **only screens when claims are made** on a policy and not when customers are first taken on, thereby running the risk of providing financial services to designated terrorists.
- Screening of customer databases is a **one-off** exercise.

• Firms relying on **third parties** for screening take reasonable steps to satisfy themselves that the third party is screening effectively.	• Updating from the Treasury list is **haphazard.** Some business units use out-of-date lists. • The firm has **no means** of monitoring payment instructions.

Box 8.4: Matches and escalation

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

Self-assessment questions:

- What steps does your firm take to identify whether a **name match** is **real**? (For example, does the firm look at a range of identifier information such as name, date of birth, address or other customer data?)
- Is there a **clear procedure** if there is a breach? (This might cover, for example, alerting senior management, the Treasury and the FSA, and giving consideration to a Suspicious Activity Report.)

Good practice:	Poor practice:
• Sufficient resources are available to identify '**false positives**'. • An account is **frozen** as soon as a positive match is confirmed. (Note that freezing the account of a sanctioned individual is not 'tipping off'). • The firm trains **all relevant** staff (claims handlers, for example) on the financial sanctions regime. • After a breach, as well as meeting its formal obligation to notify the **Asset Freezing Unit**, the firm considers whether to notify the **FSA**.	• The firm **does not report a breach** of the financial sanctions regime to the Asset Freezing Unit: **this could be a criminal offence**. • An account is **not frozen** when a match with the consolidated list is identified. **This could also 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.

Box 8.5: Case study – deficient sanctions systems and controls

In August 2010, we fined Royal Bank of Scotland £5.6m for deficiencies in its systems and controls to prevent breaches of UK financial sanctions. RBS failed adequately to screen its customers – and the payments they made and received – against the sanctions list, thereby running the risk that it could have facilitated payments to or from sanctioned people and organisations. The bank did not, for example, screen cross-border payments made by its customers in sterling or euros; it also failed to ensure its 'fuzzy matching' software remained effective, and, in many cases, did not screen the names of directors and beneficial owners of customer companies.

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

For more information see our press release:
www.fsa.gov.uk/pages/Library/Communication/PR/2010/130.shtml

8.3 To find out more, see:

- The findings of the FSA's 2009 thematic work on financial services firms' approach to UK financial sanctions: www.fsa.gov.uk/pubs/other/Sanctions%20Final%20Report.pdf
- Our leaflet on financial sanctions is aimed at small firms: www.fsa.gov.uk/smallfirms/resources/pdfs/Sanctions.pdf
- The website of the Treasury's Asset Freezing Unit: www.hm-treasury.gov.uk/documents/financial_services/sanctions/faqs/fin_sanctions_role.cfm

9 Countering weapons proliferation financing

This section is most relevant to *UK banks carrying out trade finance business*. Other activities such as *project finance* and *insurance* may also be vulnerable. Sanctions against Iran will impose requirements on all firms conducting business linked to that country.

9.1 The export of goods and services for use in nuclear, radiological, chemical or biological weapons programmes is subject to strict controls. Weapons proliferators seek to gain access to this technology illegally; 'proliferation financing' is the provision of financial services to facilitate this activity.[2]

9.2 *Firms involved in trade finance* can take steps to counter the risk of involvement. It should be acknowledged, however, that it is not easy to identify transactions related to weapons proliferation: goods may have other legitimate commercial uses, while proliferators may hide their tracks using front companies in third countries.

9.3 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, establishing subsidiaries in Iran, buying Iranian bonds, making loans to Iranian oil companies, and insuring Iranian organisations (but not individuals). Fund transfers involving Iran over €10,000 in value need to be notified to the Treasury, or, in some cases, submitted to them for approval.[3] Firms are also required to report any suspicions of transactions involving proliferation financing to the Serious Organised Crime Agency (SOCA).

2 Aiding proliferators is an offence in the Anti-Terrorism, Crime and Security Act 2001.

3 Note that the Treasury can also use powers under the Counter-Terrorism Act 2008 (see Annex 1) to direct financial firms to, say, cease business with certain customers involved in proliferation activity, although no direction of this sort is in place at time of writing.

Box 9.1: Proliferation financing

Firms' systems and controls should address proliferation risks.

Self-assessment questions:

- Does your firm finance trade with **countries of concern**, like Iran?
- If so, has **enhanced due diligence** been carried out on counterparties and goods?
- Where doubt remains, is evidence sought from **exporters** that the trade is legitimate?
- What **other business** takes place with these jurisdictions, and what measures are in place to contain the risks of transactions being related to proliferation?

Good practice:

- A *bank* has identified if its customers export goods to countries of concern, and subjects transactions to **enhanced scrutiny** by identifying, for example, whether goods may be subject to export restrictions, or end-users may be of concern.
- Where **doubt exists**, the *bank* asks the customer to **demonstrate** that appropriate assurances have been gained from relevant government authorities.
- The firm has considered **how to respond** if the government takes action under the Counter-Terrorism Act 2008 against one of its customers.
- An *insurer* has identified whether **EU Regulation 961/2010** affects its relationship with its customers.

Poor practice:

- A *correspondent bank* accepts payment instructions from a respondent **without having assured itself** of the quality of the respondent's customer due diligence checks.
- 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.

9.4 To find out more, see:

- The website of the UK's **Export Control Organisation**, which contains lots of useful information, including lists of equipment requiring an export licence to be exported to any destination, because they are either military items or 'dual use' (see the Annex 1 list of common terms). For Iran, the website also lists goods that require a licence for that destination, and provides guidance on end users of concern. See: www.businesslink.gov.uk/bdotg/action/layer?r.s=tl&r.l1=1079717544&r.lc=en&r.l2=1084228483&topicId=1084302974
- SOCA's website contains guidelines on how to report your suspicions: www.soca.gov.uk
- The **BIS Iran List** shows 'end users' in Iran who have had export licenses declined: www.bis.gov.uk/policies/export-control-organisation/eco-notices-exporters
- In June 2008, **FATF** launched a 'Proliferation Financing Report' that includes case studies of past proliferation cases, including some involving UK banks: www.fatf-gafi.org/dataoecd/32/40/45049911.pdf
- Part III of the Joint Money Laundering Steering Groups guidance on the prevention of money laundering and terrorist financing contains a chapter on proliferation financing: www.jmlsg.org.uk/download/6130

Annex 1: Common terms

Term	Meaning
419 fraud	See 'advance fee fraud'.
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. This fraud is often referred to as a '419 fraud'.
AFU	See 'Asset Freezing Unit'.
AML	Anti-money laundering. See 'money laundering'.
Annex I financial institution	The Money Laundering Regulations 2007 give the FSA responsibility for supervising the anti-money laundering controls of 'Annex I financial institutions' (a reference to Annex I to the Banking Consolidation Directive, where they are listed). In practice, this includes businesses that offer finance leases, commercial lender and providers of safe deposit boxes. Where a firm we authorise offers such services, we are responsible for overseeing whether these activities are performed in a manner that complies with the requirements of the Money Laundering Regulations 2007. Authorised firms are not formally required to inform us that they perform these activities, although some may choose to do so for the sake of transparency. Where these businesses are not authorised, we are responsible for supervising their activities. For more information on this, see our website: www.fsa.gov.uk/pages/About/What/financial_crime/money_laundering/3mld/registered/index.shtml
asset freezing	See 'financial sanctions regime'.
Asset Freezing Unit	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	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 EU's Third Money Laundering Directive.
beneficial owner	The natural person who ultimately owns or controls the customer. An entity may have more than one beneficial owner. 'Beneficial owner' is defined in Regulation 6 of the Money Laundering Regulations 2007.

Term	Meaning
boiler room	An unauthorised firm which defrauds the public by using hard-sell tactics, usually over the telephone, to sell shares as an investment opportunity while knowing that they are worthless or fictional. www.fsa.gov.uk/Pages/consumerinformation/scamsandswindles/sharescams/index.shtml
bribery	Bribery is the offering or acceptance of an undue advantage in exchange for the improper performance of a function or activity.
Bribery Act 2010	The Bribery Act comes into force in July 2011. It outlaws offering and receiving bribes, at home and abroad, as well as creating a corporate offence of failure to prevent bribery. The Ministry of Justice has issued guidance about procedures which firms can put in place to prevent bribery: www.justice.gov.uk/downloads/guidance/making-reviewing-law/bribery-act-2010-guidance.pdf
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.
consent	If a firm is concerned that it may be assisting in the laundering of funds it can file a Suspicious Activity Report and apply to SOCA for consent to continue the transaction. The Proceeds of Crime Act 2002 gives SOCA seven working days to respond. SOCA will either agree that the transaction can go ahead or it will refuse consent. In the latter case SOCA has 31 calendar days in which to take further action: for example, to seek a court order to restrain the assets in question.
corruption	Corruption is the abuse of public or private office to obtain an undue advantage. Corruption includes bribery.
Counter-Terrorism Act 2008	On 12 October 2009, the government required UK financial firms to cease business with two Iranian entities: Bank Mellat and Islamic Republic or Iran Shipping Lines. This was the first occasion the Treasury used its 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. (The Mellat/IRISL action has now lapsed, having been superseded by new EU sanctions with the same effect). Use of this power can be triggered if a) money laundering or terrorist financing deficiencies are identified in a country, or b) if 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 firms' 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'.
CPS	See 'Crown Prosecution Service'

Term	Meaning
Crown Prosecution Service	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.
CTF	Combating terrorist financing/countering the finance of terrorism.
customer due diligence	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. 'Customer due diligence' and 'Know Your Customer' (KYC) are sometimes used interchangeably. See Regulation 7 of the Money Laundering Regulations 2007.
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	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.
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 FSA's Handbook and of the Money Laundering Regulations 2007. However, an EEA firm that only provides services on a cross-border basis (and so does not have a UK branch) will not be subject to the Money Laundering Regulations 2007, unless it carries on its business through representatives who are temporarily located in the UK.
Egmont Group	A forum for financial intelligence units from across the world.
enhanced due diligence	The Money Laundering Regulations 2007 require firms to apply additional, 'enhanced' customer due diligence measures in higher-risk situations (see Boxes 3.6 to 3.8).
equivalent jurisdiction	A jurisdiction (other than an EEA state) whose law contains equivalent provisions to those contained in the EU's Third Money Laundering Directive. The JMLSG has prepared advice for firms on how to identify which jurisdictions are equivalent. Equivalent jurisdictions are significant because a firm is able to apply 'simplified due diligence' to financial institutions from these places. They 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. If a financial firm authorised by us were to finance or insure these illegal exports, it would arguably have been used to further financial crime.
FATF	See 'Financial Action Task Force'.

Term	Meaning
FATF Recommendations	Forty Recommendations issued by the FATF on the structural, supervisory and operational procedures that countries should have in place to combat money laundering. The Forty Recommendations can be downloaded from the FATF's website: www.fatf-gafi.org/dataoecd/7/40/34849567.PDF
FATF Special Recommendations	Nine Recommendations on the prevention of terrorist financing. The Nine Special Recommendations can be downloaded from the FATF's website: www.fatf-gafi.org/dataoecd/8/17/34849466.pdf
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	An intergovernmental body that develops and promotes anti-money laundering and counter terrorist financing standards worldwide. Further information is available on its website: www.fatf-gafi.org
financial crime	Financial crime is any crime involving money. More formally, the Financial Services and Markets Act 2000 defines financial crime 'to include any offence involving (a) fraud or dishonesty; (b) misconduct in, or misuse of information relating to, a financial market; or (c) handling the proceeds of crime'. The use of the term 'to include' means financial crime can be interpreted widely to include, for example, corruption or funding terrorism.
financial intelligence unit	The IMF uses the following definition: 'a central national agency responsible for receiving, analyzing, and transmitting disclosures on suspicious transactions to the competent authorities.' SOCA has this role in the UK.
Financial Investigator	Financial Investigators (FIs) are accredited people able under the relevant legislation to investigate financial offences and recover the proceeds of crime.
financial sanctions regime	This prohibits firms from providing funds and other economic resources (and, in the case of designated terrorists, financial services) to individuals and entities on a consolidated list maintained by the Asset Freezing Unit of the Treasury. The Asset Freezing Unit is responsible for ensuring compliance with the UK's financial sanctions regime; our role is to ensure firms have appropriate systems and controls to enable compliance.
Financial Services and Markets Act 2000	The Financial Services and Markets Act 2000 (FSMA) creates the Financial Services Authority and sets out its objectives, duties and powers.
Financial Services Authority	The Financial Services Authority (FSA) has statutory objectives under FSMA that include the reduction of financial crime. We have supervisory responsibilities under the Money Laundering Regulations 2007 for authorised firms and businesses such as leasing companies and providers of safe deposit boxes. We also have functions under other legislation such as the Transfer of Funds (Information on the Payer) Regulations 2007, in relation to the EU's Wire Transfer Regulation, and schedule 7 of the Counter-Terrorism Act 2008.

Term	Meaning
FIU	See 'financial intelligence unit'.
four-eyes procedures	Procedures that require the oversight of two people, to lessen the risk of fraudulent behaviour, financial mismanagement or incompetence going unchecked.
fraud (types of)	Fraud can affect firms and their customers in many ways: • 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. crooks evade security measures to gain access to a customer's account); • a firm's customers are defrauded by a third party because of 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:'419 fraud', 'advance fee fraud', 'boiler room', 'long firm fraud', 'Missing Trader Inter-Community Fraud'.
Fraud Act 2006	The Fraud Act 2006 sets out a series of fraud offences such as fraud by false representation, fraud by failing to disclose information and fraud by abuse of position.
FSA	See 'Financial Services Authority'.
FSMA	See 'Financial Services and Markets Act 2000'.
FSRB	See 'FATF-style regional bodies'.
High-value dealer	A firm trading in goods (e.g. cars, jewellery and antiques) that accepts cash of more than €15,000 (or equivalent) in payment (whether in one go or in several payments which appear to be linked). HMRC is the supervisory authority for high value dealers.
HM Revenue and Customs	HM Revenue and Customs (HMRC) has supervisory responsibilities under the Money Laundering Regulations 2007. It oversees money service businesses, dealers in high value goods and trust or company service providers, amongst others.
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	The Information Commissioner's Office is tasked with protecting the public's personal information.

Term	Meaning
Information From Lenders project	This scheme enables mortgage lenders to inform the FSA of suspected fraud by mortgage brokers. Details are here: www.fsa.gov.uk/pages/doing/regulated/supervise/mortgage_fraud.shtml
insider dealing	Trading on the basis of, or disseminating, inside information. For information to be inside information it must be precise information which: is not generally available; relates to an issuer (firm) of a qualifying investment; and would, if generally available, be likely to have a significant effect on the price of the qualifying or related investment.
Institute of Chartered Accountants in England and Wales	The Institute of Chartered Accountants in England and Wales has supervisory responsibility for its members under the Money Laundering Regulations 2007, as do other professional bodies for accountants and book-keepers.
integration	See 'placement, layering, integration'.
JMLSG	See 'Joint Money Laundering Steering Group'.
Joint Money Laundering Steering Group	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.
Know Your Customer (KYC)	This term is often used as a synonym for 'customer due diligence' checks. The term can also refer to suitability checks related to the regulated sales of financial products. The Money Laundering Regulations 2007 refer to 'customer due diligence' and not to KYC.
KYC	See 'Know Your Customer'.
layering	See 'placement, layering, integration'.
long firm fraud	A fraud where an apparently legitimate company is established and, over a period of time, builds up a good credit record with wholesalers, paying promptly for modest transactions. Correspondence from bankers may be used by them as evidence of good standing. The company then places a large order, takes delivery, but disappears without paying. This type of fraud is not limited to wholesalers of physical goods: financial firms have been victim to variants of this scam.
Missing Trader Inter-Community Fraud	This fraud exploits the EU system for rebating Value Added Tax payments in situations where goods have moved across borders within the EU. National authorities are misled into giving rebates to import-export companies that are not entitled to them.
MLRO	See 'Money Laundering Reporting Officer'.

Term	Meaning
money laundering	The process by which the proceeds of crime are converted into assets which appear to have a legitimate origin, so that they can be retained permanently, or recycled to fund further crime.
Money Laundering Directive	See 'Third Money Laundering Directive'.
Money Laundering Regulations 2007	The Money Laundering Regulations 2007 transpose the requirements of the EU's Third Money Laundering Directive into UK law. The Regulations require firms to take specified steps to detect and prevent both money laundering and terrorist financing. The Regulations identify the firms we supervise and impose on us a duty to take measures to secure those firms' compliance with the Regulations' requirements.
Money Laundering Reporting Officer (MLRO)	The MLRO is responsible for ensuring that measures to combat money laundering within the firm are effective. The MLRO is also usually the 'nominated officer' under the Proceeds of Crime Act (POCA). The MLRO is a 'controlled function' under the Approved Persons Regime.
money service business (MSB)	An undertaking which by way of business operates a currency exchange office, transmits money (or any representations of monetary value) by any means or which cashes cheques which are made payable to customers. (See Regulation 2(1) of the Money Laundering Regulations 2007). Firms that are authorised by the FSA must inform us if they provide MSB services. For more information about this, see: www.fsa.gov.uk/pages/About/What/financial_crime/money_laundering/3mld/authorised/index.shtml Money service businesses providers that are not authorised under FSMA have their anti-money laundering controls supervised by HM Revenue and Customs. More information about registration with HMRC can be found on its website: www.hmrc.gov.uk/mlr
mortgage brokers, general insurers and general insurance intermediaries (and financial crime)	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. However, they are not subject to the Money Laundering Regulations 2007 or the provisions of the FSA Handbook that specifically relate to money laundering. Firms offering these services alongside other products that are subject to the Regulations (such as banking and stock broking services) can hence apply different customer due diligence checks in both situations, although, in practice, many will choose to apply a consistent approach for the sake of operational convenience.
MSB	See 'money service business'.
MTIC	See 'Missing Trader Inter-Community Fraud'.
National Fraud Authority	The National Fraud Authority is responsible for devising and implementing a national fraud strategy.
NCCT	See 'non-cooperative countries or territories'.

Term	Meaning
NFA	See 'National Fraud Authority'.
nominated officer	A person in a firm nominated to receive disclosures (whether under section 330 of POCA, Part 3 of the Terrorism Act 2000 and/or Regulation 20(2)(d)(i) of the Money Laundering Regulations 2007) from others within the firm who know or suspect that a person is engaged in money laundering or terrorist financing.
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. At present, no countries are designated under the NCCT list; however, the FATF has issued public statements highlighting the AML/CFT risks
posed by certain countries. An up-to-date statement can be found on the FATF website. The JMLSG has prepared guidance for firms on	how to judge the risks of conducting business in different countries.
occasional transaction	Any transaction (carried out other than as part of a business relationship) amounting to €15,000 or more, whether the transaction is carried out in a single operation or several operations which appear to be linked. (See Regulation 2(1) of the Money Laundering Regulations 2007).
Office of Fair Trading (and financial crime)	The Office of Fair Trading has responsibilities under the Money Laundering Regulations 2007 to supervise many lenders and estate agents.
OFT	See 'Office of Fair Trading'.
ongoing monitoring	The Money Laundering Regulations 2007 require ongoing monitoring of business relationships. This means that the transactions performed by a customer, and other aspects of their behaviour, are scrutinised throughout the course of their relationship with the firm. The intention is to spot where a customer's actions are inconsistent with what might be expected of a customer of that type, given what is known about their business, risk profile etc. Where the risk associated with the business relationship is increased, firms must enhance their ongoing monitoring on a risk-sensitive basis. Firms must also update the information they hold on customers for anti-money laundering purposes.
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 export of small arms) 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'.

Term	Meaning
politically exposed person	A person entrusted with a prominent public function in a foreign state; 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).
Proceeds of Crime Act 2002	This Act criminalises all forms of money laundering and creates other offences such as failing to report a suspicion of money laundering and 'tipping off'.
Production Order	The Proceeds of Crime Act 2002 allows Financial Investigators to use production orders to obtain information from financial firms about an individual's financial affairs.
proliferation finance	Funding the proliferation of weapons of mass destruction in contravention of international law.
recognised investment exchanges, and recognised clearing houses (and inancial crime)	To be recognised by the FSA, exchanges and clearing houses must, among other things, adopt appropriate measures to: • reduce the extent to which their facilities can be used for a purpose connected with market abuse or financial crime, • monitor the incidence of market abuse or financial crime, and facilitate its detection. Measures should include the monitoring of transactions. This is set out in the Recognised Investment Exchanges and Recognised Clearing Houses module (REC) of the FSA Handbook, which contains our guidance on our interpretation of the recognition requirements. It also explains the factors we may consider when assessing a recognised body's compliance with the requirements. The guidance in REC 2.10.4G provides that the Money Laundering Regulations 2007, among other laws, apply to Recognised Bodies.
reliance	The Money Laundering Regulations 2007 allow a firm to rely on customer due diligence checks performed by others. However, there are many limitations on how this can be done. First, the relying firm nonetheless remains liable for any failure to apply these checks. Second, the firm being relied upon must give its consent. Third, the law sets out exactly what kinds of firms may be relied upon. See Regulation 17 of the Money Laundering Regulations 2007 and the JMLSG guidance for more detail.
safe deposit boxes	The FSA is responsible for supervising anti-money laundering controls of safe custody services; this includes the provision of safe deposit boxes.
sanctions	See 'financial sanctions regime'.
SAR	See 'Suspicious Activity Report'.
Senior Management Arrangements, Systems and Controls sourcebook	See 'SYSC'.
Serious Organised Crime Agency (SOCA):	Created in 2006, SOCA brought together various agencies including the National Crime Squad, National Criminal Intelligence Service and HMRC's investigative branches. As the UK's financial intelligence unit it receives suspicious activity reports about money laundering and terrorist financing.

Term	Meaning
simplified due diligence	The Money Laundering Regulations 2007 allow firms, in certain specific situations which present a very low money-laundering risk, not to apply customer due diligence measures to their customers and, where applicable, their beneficial owners. See Regulation 13 of the Money Laundering Regulations 2007 for more detail. Applying simplified due diligence does not exempt the firm from the need for ongoing monitoring of the customer relationship, and a firm will have to obtain sufficient information to have a meaningful basis for monitoring. Firms also need to report any suspicious transactions. Also, in practice, firms may have other reasons to satisfy themselves that a customer is who they purport to be: for example, in order to control fraud or credit losses.
SOCA	See 'Serious Organised Crime Agency'.
Solicitors Regulation Authority	The Solicitors Regulation Authority has supervisory responsibility for solicitors under the Money Laundering Regulations 2007. The Bar Council and other professional bodies for the legal sector perform a similar role for their members.
Special Recommendations	See 'FATF Special Recommendations'.
source of funds and source of wealth	As part of their customer due diligence and monitoring obligations, firms should establish that the source of wealth and source of funds involved in a business relationship or occasional transaction is legitimate. They are required to do so when the customer is a PEP. 'Source of wealth' describes how a customer acquired their total wealth, while 'source of funds' refers to the origin of the funds involved in the business relationship or occasional transaction.
SRA	See 'Solicitors Regulation Authority'.
STR	See 'Suspicious Transaction Report'.
Suspicious Activity Report	A report made to SOCA about suspicions of money laundering or terrorist financing. This is commonly known as a 'SAR'. See also 'Suspicious Transaction Report'.
Suspicious Transaction Report	When applied to money laundering reporting, the term 'Suspicious Transaction Report' is used commonly outside of the UK in place of 'Suspicious Activity Report'. Both terms have substantially the same meaning. In the UK, the term 'Suspicious Transaction Report' (STR) tends to be used in connection with market abuse reporting.
SYSC	SYSC is the Senior Management Arrangements, Systems and Controls sourcebook of the FSA's Handbook. It sets out the responsibilities of directors and senior management. SYSC includes rules and guidance about firms' anti-financial crime systems and controls. All authorised firms 'must take reasonable care to establish and maintain effective systems and controls for countering the risk that the firm might be used to further financial crime' (see SYSC 6.1.1R, or for insurers, managing agents and Lloyd's, SYSC 3.2.6R). SYSC 6.3 contains anti-money laundering specific rules and guidance. These provisions are also set out in SYSC 3.2.6A to SYSC 3.2.6J as they apply to certain insurers, managing agents and Lloyd's. The money-laundering specific provisions of SYSC do not apply to mortgage brokers, general insurers and general insurance intermediaries.
terrorist finance	The provision of funds or other assets to support a terrorist ideology, a terrorist infrastructure or individual operations. It applies to domestic and international terrorism.

Term	Meaning
TF	Terrorist financing (also 'CTF').
Third Money Laundering Directive	The EU's Third Money Laundering Directive, adopted in 2005 (2005/60/EC), translated the FATF's Recommendations into EC legislation. The UK has implemented this Directive through the Money Laundering Regulations 2007.
tipping off	The offence of tipping off is committed where a person discloses that: • any person has made a report under the Proceeds of Crime Act 2002 to the Police, HM Revenue and Customs or SOCA concerning money laundering, where that disclosure is likely to prejudice any investigation into the report; or • an investigation into allegations that an offence of money laundering has been committed is being contemplated or is being carried out. See section 333A of the Proceeds of Crime Act 2002. A similar offence exists in relation to terrorism (including terrorism financing) by virtue of section 21D of the Terrorism Act 2000.
Transfer of Funds (Information on the Payer) Regulation 2007	The Transfer of Funds (Information on the Payer) Regulation 2007 allows the FSA to place penalties on banks that fail to include data about the payer in payment instructions, as is required by the EU's Wire Transfer Regulation. See also 'Wire Transfer Regulation'.
Treasury	The Treasury is the UK government's AML policy lead. It also implements the UK's financial sanctions regime through its Asset Freezing Unit.
trust or company service provision	A formal legal definition of 'trust or company service provider' is given in Regulation 3(10) of the Money Laundering Regulations 2007. A simple definition might be 'a enterprise whose business creates, or enables the creation of, trusts and companies on behalf of others for a fee'. International standard setters have judged that such services can be abused by those seeking to set up corporate entities designed to disguise the true origins of illicit funds. The firms we authorise must inform us if they provide trust or company services. For more information about this, see: www.fsa.gov.uk/pages/About/What/financial_crime/money_laundering/3mld/authorised/index.shtml Trust or company service providers that are not authorised by us have their anti-money laundering controls supervised by HM Revenue and Customs. More information can be found at its website: www.hmrc.gov.uk/mlr
verification	Making sure the customer or beneficial owner is who they claim to be. The Money Laundering Regulations 2007 require the customer's identity to be identified on the basis or reliable and independent information, and the beneficial owner's in a way that the firm is satisfied that it knows who the beneficial owner is. See Regulation 5 of the Money Laundering Regulations 2007.
Wire Transfer Regulation	This EU Regulation is formally titled 'Regulation 1781/2006 on information on the payer accompanying transfers of funds'. It implements FATF's 'Special Recommendation VII' in the EU and requires firms to accompany the transfer of funds with specified information identifying the payer. We were given enforcement powers under this regulation by the Transfer of Funds (Information on the Payer) Regulations 2007. The Wire Transfer Regulation is also known as the Payer Information Regulation or the Payment Regulation and should not be confused with the Payment Services Directive.

Term	Meaning
Wolfsberg Group	An association of global banks, including UK institutions, which aims to 'develop financial services industry standards, and related products, for Know Your Customer, Anti-Money Laundering and Counter Terrorist Financing policies'. See its website for more: www.wolfsberg-principles.com

Financial crime: a guide for firms

Part 2: Financial crime thematic reviews

Contents

1 Introduction

1.1 Part 2 of *Financial Crime: a guide for firms* contains summaries of, and links to, FSA thematic reviews of various financial crime risks. It includes the consolidated examples of good and poor practice that were included with the reviews' findings.

1.2 The statements of our expectations and the examples of good and poor practice in Part 2 have the same status as in Part 1: they are guidance which we expect firms to take into account where it applies to them. Part 2 is not binding and imposes no requirements on firms. Please refer to Chapter 1 of Part 1 of this guide for more information.

1.3 Not all thematic reviews contain consolidated examples of good and poor practice. All reports do, however, discuss what we found about the practices in place at the firms 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 reviews can find more information on this in the original reports.

2 Firms' high-level management of fraud risk

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

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

2.3 The report emphasised that fraud is more than just a financial crime issue for firms; it is also a reputational one for the industry as a whole. The report concluded that whilst 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.

Our findings

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

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

Consolidated examples of good and poor practice

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

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

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

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

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

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

Our findings

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

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

Consolidated examples of good and poor practice

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

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

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

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

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

Our findings

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

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

Consolidated examples of good and poor practice

Box 4.1: Firms' implementation of a risk-based approach to AML	
Good practice: • One large firm's procedures required it to undertake periodic KYC/Customer Due Diligence reviews of existing clients. The depth of the review is determined by the risk ranking assigned to the client. Clients rated A and B are reviewed every three years; Cs every two years; and Ds and	Poor practice: • 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

Box 4.1: Firms' implementation of a risk-based approach to AML

Good practice:

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.

- One building society undertook a comprehensive policy review following the publication of the 2006 JMLSG guidance, in order to identify which parts of the business were affected and what action was needed. It identified eight core business areas, which represented the key operational areas exposed to risk from money laundering. These business areas were ranked in order of risk and formed into work streams. The local managers from each workstream business area were then trained by the Compliance Policy Team, using a series of presentations and individual workshops, to understand the impact of the risk-based approach, their individual responsibilities and the appropriate customer due diligence policies. These managers were then required to apply this awareness and their existing knowledge of their workstreams' business activities to create documented risk profiles covering customers, products, delivery channels and geography. The risk profiles were graded as Red, Amber and Green and customer due diligence and monitoring requirements set at appropriate levels.
- In response to the SYSC changes, one major bank decided to appoint the MLRO's[1] 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

Poor practice:

the Middle East. Another firm's risk-assessment procedures provided that the Compliance Officer or MLRO would determine the risk category for each client and would record the basis of the assessment for each client. However, a file review showed no evidence that risk assessments had actually been carried out.

- Some small firms had produced inadequate annual MLRO reports, which failed to demonstrate to their governing body and senior management that the firms' AML systems and controls were operating effectively. In one case, the MLRO stated categorically that there had been no perceived deficiencies in the suspicious activity reporting process. However, he was unable even to describe that process to us, so it was highly unlikely that he had ever reviewed the SAR[2] process for possible deficiencies.
- In one small firm, the MLRO was clearly not fully engaged in his role. For example, he was unaware that we had removed the Money Laundering sourcebook and he was still using an outdated (2003) edition of the JMLSG Guidance. It was not entirely clear whether this arose from a lack of interest in his MLRO function or from inadequate compliance resources at the firm, which left him with insufficient time to keep up to date with AML matters, or a combination of both.
- We found some cases of medium-sized and smaller firms documenting their client take-on procedures but not regularly updating those procedures and not always following them. For example, one firm told us that CDD information on clients was refreshed every time clients 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.

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

2 Suspicious Activity Report. See Part 1 Annex 1 for common terms.

Box 4.1: Firms' implementation of a risk-based approach to AML

Good practice:

senior manager to this position was viewed as reinforcing the importance of having in place a robust AML control framework. Following his appointment, the director decided that the management information (MI) on AML issues he had hitherto received was too ad hoc and fragmented. So the SYSC/JMLSG[3] changes proved to be a catalyst for the bank establishing more organised MI and a Group-level Financial Risk Committee to consider relevant issues. (In the past, various Risk Committees had considered such issues.) The new Committee's remit covered fraud, money laundering and sanctions issues; however, its primary focus was AML.

- One large bank judged that staff AML training and awareness were suitable for the development of a risk-based approach. It saw a need to differentiate between AML requirements in various business units, so that training could be adapted to the needs of the job. So in Retail, training had been re-designed to produce a more balanced package. Accordingly, staff were required to undertake one training module per quarter, with the emphasis on a different area in each module and a test taken every quarter. The aim was to see what impact this constant 'drip feed' of training had on suspicious activity reporting. At the time of our visit, this bank was also in the throes of merging its anti-fraud and AML training. The overall objective was to make it more difficult for criminals to do business with the bank undetected.

Poor practice:

- 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.

3 Joint Money Laundering Steering Group. See Part 1 Annex 1 for common terms.

5 Automated Anti-Money Laundering Transaction Monitoring Systems

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

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

5.3 The report confirmed 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 included transaction monitoring and profiling; especially ensuring unusual patterns of customer activity are identified.

Our findings

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

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

Consolidated examples of good and poor practice

5.5 This report contained the following examples of good practice:

Box 5.1: 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.

Box 5.1: Statement of good practice
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 ensuring 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.

Box 5.1: Statement of good practice
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.

6 Data security in Financial Services

6.1 In April 2008 we published our findings on our thematic review on how financial services firms in the UK are addressing the risk that customer data may be lost or stolen and used to commit fraud or other financial crime. We visited 39 firms, retail and wholesale banks, investment firms, insurance companies, financial advisers and credit unions. We also took into account our experience of data loss incidents dealt with by our Financial Crime Operations Team: during 2007, the team dealt with 56 cases of lost or stolen data from financial services firms.

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

6.3 The report concluded that poor data security was a serious, widespread and high-impact risk, and firms were often failing to consider the wider risks of identity fraud which could occur from cases of significant data loss and the impact on consumers. We found that firms lacked a clear understanding of these risks and were therefore failing properly to inform customers, resulting in a lack of transparency.

Our findings

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

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

Consolidated examples of good and poor practice

Box 6.1: Governance	
Good practice: • Identification of data security as a key specific risk, subject to its own governance, policies and procedures and risk assessment. • A senior manager with overall responsibility for data security, specifically mandated to manage data security risk assessment and communication between the key stakeholders within the firm such as: senior management, information security, Human Resources, financial crime, security, IT, compliance and internal audit.	Poor practice: • Treating data security as an IT issue and failing to involve other key staff from across the business in the risk assessment process. • No written policies and procedures on data security. • Firms do not understand the need for knowledge-sharing on data security.

Box 6.1: Governance

Good practice:

- A specific committee with representation from relevant business areas to assess, monitor and control data security risk, which reports to the firm's Board. As well as ensuring coordinated risk management, this structure sends a clear message to all staff about the importance of data security.
- Written data security policies and procedures that are proportionate, accurate and relevant to staff's day-to-day work.
- An open and honest culture of communication with pre-determined reporting mechanisms that make it easy for all staff and third parties to report data security concerns and data loss without fear of blame or recrimination.
- Firms seeking external assistance if they feel they do not have the necessary expertise to complete a data security risk assessment themselves.
- Firms liaising with peers and others to increase their awareness of data security risk and the implementation of good systems and controls.
- Detailed plans for reacting to a data loss including when and how to communicate with affected customers.
- Firms writing to affected customers promptly after a data loss, telling them what has been lost and how it was lost.
- Firms offering advice on protective measures against identity fraud to consumers affected by data loss and, where appropriate, paying for such services to be put in place.

Poor practice:

- Failing to take opportunities to share information with, and learn from, peers and others about data security risk and not recognising the need to do so.
- A 'blame culture' that discourages staff from reporting data security concerns and data losses.
- Failure to notify customers affected by data loss in case the details are picked up by the media.

Box 6.2: Training and awareness

Good practice:

- Innovative training and awareness campaigns that focus on the financial crime risks arising from poor data security, as well as the legal and regulatory requirements to protect customer data.
- Clear understanding among staff about why data security is relevant to their work and what they must do to comply with relevant policies and procedures.

Poor practice:

- No training to communicate policies and procedures.
- Managers assuming that employees understand data security risk without any training.
- Data security policies which are very lengthy, complicated and difficult to read.

Box 6.2: Training and awareness

Good practice:

- Simple, memorable and easily digestible guidance for staff on good data security practice.
- Testing of staff understanding of data security policies on induction and once a year after that.
- Competitions, posters, screensavers and group discussion to raise interest in the subject.

Poor practice:

- Reliance on staff signing an annual declaration stating that they have read policy documents without any further testing.
- Staff being given no incentive to learn about data security.

Box 6.3: Staff recruitment and vetting

Good practice:

- Vetting staff on a risk-based approach, taking into account data security and other fraud risk.
- Enhanced vetting – including checks of credit records, criminal records, financial sanctions lists and the CIFAS Staff Fraud Database – for staff in roles with access to large amounts of customer data.
- Liaison between HR and Financial Crime to ensure that financial crime risk indicators are considered during the vetting process.
- A good understanding of vetting conducted by employment agencies for 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.

Poor practice:

- Allowing new recruits to access customer data before vetting has been completed.
- Temporary staff receiving less rigorous vetting than permanently employed colleagues carrying out similar roles.
- Failing to consider continually whether staff in higher-risk positions are becoming vulnerable to committing fraud or being coerced by criminals.

Box 6.4: Controls – Access rights

Good practice:

- Specific IT access profiles for each role in the firm, which set out exactly what level of IT access is required for an individual to do their job.
- If a staff member changes roles or responsibilities, all IT access rights are deleted from the system and the user is set up using the same process as if they were a new joiner at the firm. The complexity of this process is significantly reduced if role-based IT access profiles are in place – the old one can simply be replaced with the new.

Poor practice:

- Staff having access to customer data that they do not require to do their job.
- User access rights set up on a case-by-case basis with no independent check that they are appropriate.
- Redundant access rights being allowed to remain in force when a member of staff changes roles.
- User accounts being left 'live' or only suspended (i.e. not permanently disabled) when a staff member leaves.

Box 6.4: Controls – Access rights

Good practice:

- A clearly-defined process to notify IT of forthcoming staff departures in order that IT accesses can be permanently disabled or deleted on a timely and accurate basis.
- A regular reconciliation of HR and IT user records to act as a failsafe in the event of a failure in the firm's leavers process.
- Regular reviews of staff IT access rights to ensure that there are no anomalies.
- 'Least privilege' access to call recordings and copies of scanned documents obtained for 'know your customer' purposes.
- Authentication of customers' identities using, for example, touch-tone telephone before a conversation with a call centre adviser takes place. This limits the amount 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.

Poor practice:

- A lack of independent check of changes effected at any stage in the joiners, movers and leavers process.

Box 6.5: Controls – passwords and user accounts

Good practice:

- Individual user accounts – requiring passwords – in place for all systems containing customer data.
- Password standards at least equivalent to those recommended by Get Safe Online – a government-backed campaign group. At present, their recommended standard for passwords is a combination of letters, numbers and keyboard symbols at least seven characters in length and changed regularly.
- Measures to ensure passwords are robust. These might include controls to ensure that passwords can only be set in accordance with policy and the use of password-cracking software on a risk-based approach.
- 'Straight-through processing', but only if complemented by accurate role-based access profiles and strong passwords.

Poor practice:

- The same user account and password used by multiple users to access particular systems.
- Names and dictionary words used as passwords.
- Systems that allow passwords to be set which do not comply with password policy.
- Password sharing of any kind.

Box 6.6: Controls – monitoring access to customer data

Good 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.
- The use of software designed to spot suspicious activity by employees with access to customer data. Such software may not be useful in its 'off-the-shelf' format so it is good practice for firms to ensure that it is tailored to their business profile.
- Strict controls over superusers' access to customer data and independent checks of their work to ensure they have not accessed, manipulated or extracted data that was not required for a particular task.

Poor practice:

- Assuming that vetted staff with appropriate access rights will always act appropriately. Staff can breach procedures, for example by looking at account information relating to celebrities, be tempted to commit fraud themselves or be bribed or threatened to give customer data to criminals.
- Failure to make regular use of management information about access to customer data.
- Failing to monitor superusers or other employees with access to large amounts of customer data.

Box 6.7: Controls – data back-up

Good practice:

- Firms conducting a proper risk assessment of threats to data security arising from the data back-up process – from the point that back-up tapes are produced, through the transit process to the ultimate place of storage.
- Firms encrypting backed-up data that is held offsite, including while in transit.
- Regular reviews of the level of encryption to ensure it remains appropriate to the current risk environment.
- Back-up data being transferred by secure Internet links.
- Due diligence on third parties that handle backed-up customer data so the firm has a good understanding of how it is secured, exactly who has access to it and how staff with access to it are vetted.
- Staff with responsibility for holding backed-up data off-site being given assistance to do so securely. For example, 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 done so in accordance with accepted policies and procedures.

Poor practice:

- Firms failing to consider data security risk arising from the backing up of customer data.
- A lack of clear and consistent procedures for backing up data, resulting in data being backed up in several different ways at different times. This makes it difficult for firms to keep track of copies of their data.
- Unrestricted access to back-up tapes for large numbers of staff at third party firms.
- Back-up tapes being held insecurely by firm's employees; for example, being left in their cars or at home on the kitchen table.

Box 6.8: Controls – access to the Internet and email

Good practice:

- Giving Internet and email access only to staff with a genuine business need.
- Considering the risk of data compromise when monitoring external email traffic, for example by looking for strings of numbers that might be credit card details.
- Where proportionate, using specialist IT software to detect data leakage via email.
- Completely blocking access to all Internet content which allows web-based communication. This content includes web-based email, messaging facilities on social networking sites, external instant messaging and 'peer-to-peer' file-sharing software.
- Firms that provide cyber-cafes for staff to use during breaks ensuring that web-based communications are blocked or that data cannot be transferred into the cyber-cafe, either in electronic or paper format.

Poor practice:

- Allowing staff who handle customer data to have access to the Internet and email if there is no business reason for this.
- Allowing access to web-based communication Internet sites. This content includes web-based email, messaging facilities on social networking sites, external instant messaging and 'peer-to-peer' file-sharing software.

Box 6.9: Controls – key logging devices

Good 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.

Poor practice:

Box 6.10: Controls – laptop

Good practice:

- The encryption of laptops and other portable devices containing customer data.
- Controls that mitigate the risk of employees failing to follow policies and procedures. We have dealt with several cases of lost or stolen laptops in the past year that arose from staff not doing what they should.
- Maintaining an accurate register of laptops issued to staff.
- Regular audits of the contents of laptops to ensure that only staff who are authorised to hold customer data on their laptops are doing so and that this is for genuine business reasons.
- The wiping of shared laptops' hard drives between uses.

Poor practice:

- Unencrypted customer data on laptops.
- A poor understanding of which employees have been issued or are using laptops to hold customer data.
- Shared laptops used by staff without being signed out or wiped between uses.

Box 6.11: Controls – portable media including USB devices and CDs

Good practice:

- Ensuring that only staff with a genuine business need can download customer data to portable media such as USB devices and CDs.
- Ensuring that staff authorised to hold customer data on portable media can only do so if it is encrypted.
- Maintaining an accurate register of staff allowed to use USB devices and staff who have been issued USB devices.
- The use of software to prevent and/or detect individuals using personal USB devices.
- Firms reviewing regularly and on a risk-based approach the copying of customer data to portable media to ensure there is a genuine business reason for it.
- The automatic encryption of portable media attached to firms' computers.
- Providing lockers for higher-risk staff such as call centre staff and superusers and restricting them from taking personal effects to their desks.

Poor practice:

- Allowing staff with access to bulk customer data – for example, superusers – to download to unencrypted portable media.
- Failing to review regularly threats posed by increasingly sophisticated and quickly evolving personal technology such as mobile phones.

Box 6.12: Physical security

Good practice:

- Appropriately restricted access to areas where large amounts of customer data is accessible, such as server rooms, call centres and filing areas.
- Using robust intruder deterrents such as keypad entry doors, alarm systems, grilles or barred windows, and closed circuit television (CCTV).
- Robust procedures for logging visitors and ensuring adequate supervision of them while on-site.
- Training and awareness programmes for staff to ensure they are fully aware of more basic risks to customer data arising from poor physical security.
- Employing security guards, cleaners etc directly to ensure an appropriate level of vetting and reduce risks that can arise through third party suppliers accessing customer data.
- Using electronic swipe card records to spot unusual behaviour or access to high risk areas.
- Keeping filing cabinets locked during the day and leaving the key with a trusted member of staff.
- An enforced clear-desk policy.

Poor practice:

- Allowing staff or other persons with no genuine business need to access areas where customer data is held.
- Failure to check electronic records showing who has accessed sensitive areas of the office.
- Failure to lock away customer records and files when the office is left unattended.

Box: 6.13: Disposal of customer data

Good practice:

- Procedures that result in the production of as little paper-based customer data as possible.
- Treating all paper as 'confidential waste' to eliminate confusion among employees about which type of bin to use.
- All customer data disposed of by employees securely, for example by using shredders (preferably cross-cut rather than straight-line shredders) or confidential waste bins.
- Checking general waste bins for the accidental disposal of customer data.
- Using a third party supplier, preferably one with BSIA[4] 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.

Poor practice:

- Poor awareness among staff about how to dispose of customer data securely.
- Slack procedures that present opportunities for fraudsters, for instance when confidential waste is left unguarded on the premises before it is destroyed.
- Staff working remotely failing to dispose of customer data securely.
- Firms failing to provide guidance or assistance to remote workers who need to dispose of an obsolete home computer.
- Firms stockpiling obsolete computers and other portable media for too long and in insecure environments.

4 British Security Industry Association

Box: 6.13: Disposal of customer data

Good practice:

- Providing guidance for travelling or home-based staff on the secure disposal of customer data.
- Computer hard drives and portable media being properly wiped (using specialist software) or destroyed as soon as they become obsolete.

Poor practice:

- Firms relying on others to erase or destroy their hard drives and other portable media securely without evidence that this has been done competently.

Box 6.14: Managing third party suppliers

Good practice:

- Conducting due diligence of data security standards at third party suppliers before contracts are agreed.
- Regular reviews of third party suppliers' data security systems and controls, with the frequency of review dependent on data security risks identified.
- Ensuring third party suppliers' vetting standards are adequate by testing the checks performed on a sample of staff with access to customer data.
- Only allowing third party IT suppliers access to customer databases for specific tasks on a case-by-case basis.
- Third party suppliers being subject to procedures for reporting data security breaches within an agreed timeframe.
- The use of secure Internet links to transfer data to third parties.

Poor practice:

- Allowing third party suppliers to access customer data when no due diligence of data security arrangements has been performed.
- Firms not knowing exactly which third party staff have access to their customer data.
- Firms not knowing how third party suppliers' staff have been vetted.
- Allowing third party staff unsupervised access to areas where customer data is held when they have not been vetted to the same standards as employees.
- Allowing IT suppliers unrestricted or unmonitored access to customer data.
- A lack of awareness of when/how third party suppliers can access customer data and failure to monitor such access.
- Unencrypted customer data being sent to third parties using unregistered post.

Box 6.15: Internal audit and compliance monitoring

Good practice:

- Firms seeking external assistance where they do not have the necessary in-house expertise or resources.
- Compliance and internal audit conducting specific reviews of data security which cover all relevant areas of the business including IT, security, HR, training and awareness, governance and third party suppliers.
- Firms using expertise from across the business to help with the more technical aspects of data security audits and compliance monitoring.

Poor practice:

- Compliance focusing only on compliance with data protection legislation and failing to consider adherence to data security policies and procedures.
- Compliance consultants adopting a 'one size fits all' approach to different clients' businesses.

7 Review of financial crime controls in offshore centres

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

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

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

Our findings

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

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

Consolidated examples of good and poor practice

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

8 Financial services firms' approach to UK financial sanctions

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

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

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

Our findings

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

www.fsa.gov.uk/pubs/other/Sanctions%20Final%20Report.pdf

Consolidated examples of good and poor practice

Box 8.1: Senior management responsibility	
Good practice: • Full senior management and/or Board-level involvement in approving and taking responsibility for policies and procedures. • High level of senior management awareness of the firms' obligations regarding financial sanctions.	Poor practice: • No senior management involvement or understanding regarding the firm's obligations under the UK financial sanctions regime, or its systems and controls to comply with it. • No, or insufficient management oversight of the day-to-day operation of systems and controls.

Box 8.1: Senior management responsibility	
Good practice: • Senior management involvement in cases where a potential target match cannot easily be verified. • Adequate and appropriate resources allocated by senior management. • Senior management notified of all actual matches and, if it should arise, all breaches of UK financial sanctions in an appropriate and timely manner.	Poor practice: • Failure to include assessments of the financial sanctions systems and controls as a normal part of internal audit programmes. • No senior management involvement in cases where a potential target match cannot easily be verified. • Senior management not being made aware of a target match for an existing customer. • Inadequate or inappropriate resources allocated to financial sanctions compliance with our requirements.

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

Box 8.3: Policies and procedures	
Good practice: • Documented policies and procedures in place, which clearly set out a firm's approach to complying with its legal and regulatory requirements in this area. • Group-wide policies for UK financial sanctions screening across the group, to ensure that business unit-specific policies and procedures reflect at the very least the minimum standard set out in group policy. • Effective procedures to screen against the Treasury list that are appropriate for the business, covering customers, transactions and services across all products and business lines. • Clear, simple and well understood escalation procedures to enable staff to raise financial sanctions concerns with management.	Poor practice: • No policies or procedures in place for complying with the legal and regulatory requirements of the UK financial sanctions regime. • Internal audits of procedures carried out by persons with responsibility for oversight of financial sanctions procedures, rather than an independent party.

Box 8.3: Policies and procedures

Good practice:	Poor practice:
• 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.	

Box 8.4: Staff training and awareness

Good practice:	Poor practice:
• Regularly updated training and awareness programmes that are relevant and appropriate for employees' particular roles. • Testing to ensure that employees have a good understanding of financial sanctions risks and procedures. • Ongoing monitoring of employees' work to ensure they understand the financial sanctions procedures and are adhering to them. • Training provided to each business unit covering both the group-wide and business unit-specific policies on financial sanctions.	• No training on financial sanctions. • Relevant staff unaware of the firm's policies and procedures to comply with the UK financial sanctions regime. • Changes to the financial sanctions policies, procedures, systems and controls are not communicated to relevant staff.

Box 8.5: Screening during client take-on

Good practice:	Poor practice:
• An effective screening system appropriate to the nature, size and risk of the firm's business. • Screening against the Treasury list at the time of client take-on before providing any services or undertaking any transactions for a customer. • Screening directors and beneficial owners of corporate customers. • Screening third party payees where adequate information is available. • Where the firm's procedures require dual control (e.g. a 'four eyes' check) to be used, having in place an effective process to ensure this happens.	• Screening retrospectively, rather than at the time of client take-on. • Screening only on notification of a claim on an insurance policy, rather than during client take-on. • Relying on other FSA-authorised firms and compliance consultants to screen clients against the Treasury list without taking reasonable steps to ensure that they are doing so effectively. • Assuming that AML customer due diligence checks include screening against the Treasury list.

Box 8.5: Screening during client take-on

Good practice:

- The use of 'fuzzy matching' where automated screening systems are used.
- Where a commercially available automated screening system is implemented, making sure that there is a full understanding of the capabilities and limits of the system.

Poor practice:

- Failing to screen UK-based clients on the assumption that there are no UK-based persons or entities on the Treasury list or failure to screen due to any other misconception.
- Large global institutions with millions of clients using manual screening, increasing the likelihood of human error and leading to matches being missed.
- IT systems that cannot flag potential matches clearly and prominently.
- Firms calibrating their screening rules too narrowly or too widely so that they, for example, match only exact names with the Treasury list or generate large numbers of resource intensive false positives.
- Regarding the implementation of a commercially available sanctions screening system as a panacea, with no further work required by the firm.
- Failing to tailor a commercially available sanctions screening system to the firm's requirements.

Box 8.6: Ongoing screening

Good practice:

- Screening of the entire client base within a reasonable time following updates to the Treasury list.
- Ensuring that customer data used for ongoing screening is up to date and correct.
- Processes that include screening for indirect as well as direct customers and also third party payees, wherever possible.
- Processes that include screening changes to corporate customers' data (e.g. when new directors are appointed or if there are changes to beneficial owners).
- Regular reviews of the calibration and rules of automated systems to ensure they are operating effectively.
- Screening systems calibrated in accordance with the firm's risk appetite, rather than the settings suggested by external software providers.

Poor practice:

- No ongoing screening of customer databases or transactions.
- Failure to screen directors and beneficial owners of corporate customers and/or third party payees where adequate information is available.
- Failure to review the calibration and rules of automated systems, or to set the calibration in accordance with the firm's risk appetite.
- Flags on systems that are dependent on staff looking for them.
- Controls on systems that can be overridden without referral to compliance.

Box 8.6: Ongoing screening	
Good practice: • 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.	Poor practice:

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

9 Anti-bribery and corruption in commercial insurance broking

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

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

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

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

Our findings

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

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

Consolidated examples of good and poor practice

Box 9.1: Governance and management information	
Good practice: • Clear, documented responsibility for anti-bribery and corruption apportioned to either a single senior manager or a committee with appropriate Terms of Reference and senior management membership, reporting ultimately to the Board. • Good Board level and senior management understanding of the bribery and corruption risks faced by the firm, the materiality to their business and how to apply a risk-based approach to anti-bribery and corruption work.	Poor practice: • Failing to allocate official responsibility for anti-bribery and corruption to a single senior manager or appropriately formed committee. • A lack of awareness and/or engagement in anti-bribery and corruption at senior management or Board level. • Little or no MI sent to the Board about higher risk third party relationships or payments.

Box 9.1: Governance and management information

Good practice:

- Swift and effective senior management-led response to significant bribery and corruption events, which highlight potential areas for improvement in systems and controls.
- Regular MI to the Board and other relevant senior management forums.
- MI includes information about third parties including (but not limited to) new third party accounts, their risk classification, higher risk third party payments for the preceding period, changes to third-party bank account details and unusually high commission paid to third parties.
- MI submitted to the Board ensures they are adequately informed of any external developments relevant to bribery and corruption.
- Actions taken or proposed in response to issues highlighted by MI are minuted and acted on appropriately.

Poor practice:

- Failing to include details of wider issues, such as new legislation or regulatory developments in MI.
- IT systems unable to produce the necessary MI.

Box 9.2: Risk assessment and responses to significant bribery and corruption events

Good practice:

- Regular assessments of bribery and corruption risks with a specific senior person responsible for ensuring this is done, taking into account the country and class of business involved as well as other relevant factors.
- More robust due diligence on and monitoring of higher risk third-party relationships.
- Thorough reviews and gap analyses of systems and controls against relevant external events, with strong senior management involvement or sponsorship.
- Ensuring review teams have sufficient knowledge of relevant issues and supplementing this with external expertise where necessary.
- Establishing clear plans to implement improvements arising from reviews, including updating policies, procedures and staff training.
- Adequate and prompt reporting to SOCA[5] and us of any inappropriate payments identified during business practice review.

Poor practice:

- Failing to consider the bribery and corruption risks posed by third parties used to win business.
- Failing to allocate formal responsibility for anti-bribery and corruption risk assessments.
- A 'one size fits all' approach to third-party due diligence.
- Failing to respond to external events which may draw attention to weaknesses in systems and controls.
- Taking too long to implement changes to systems and controls after analysing external events.
- Failure to bolster insufficient in-house knowledge or resource with external expertise.
- Failure to report inappropriate payments to SOCA and a lack of openness in dealing with us concerning any material issues identified.

5 Serious Organised Crime Agency. See Part 1 Annex 1 for common terms.

Box 9.3: Due diligence on third-party relationships

Good 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.
- More robust due diligence on third parties which pose the greatest risk of bribery and corruption, including a detailed understanding of the business case for using them.
- Having a clear understanding of the roles clients, reinsurers, solicitors and loss adjusters play in transactions to ensure they are not carrying out higher risk activities.
- Taking reasonable steps to verify the information provided by third parties during the due diligence process.
- Using third party forms which ask relevant questions and clearly state which fields are mandatory.
- Having third party account opening forms reviewed and approved by compliance, risk or committees involving these areas.
- Using commercially-available intelligence tools, databases and/or other research techniques such as Internet search engines to check third-party declarations about connections to public officials, clients or the assured.
- Routinely informing all parties involved in the insurance transaction about the involvement of third parties being paid commission.
- Ensuring current third-party due diligence standards are appropriate when business is acquired that is higher risk than existing business.
- Considering the level of bribery and corruption risk posed by a third party when agreeing the level of commission.
- Setting commission limits or guidelines which take into account risk factors related to the role of the third party, the country involved and the class of business.
- Paying commission to third parties on a one-off fee basis where there role is pure introduction.

Poor practice:

- Failing to carry out or document due diligence on third-party relationships.
- Relying heavily on the informal 'market view' of the integrity of third parties as due diligence.
- Relying on the fact that third-party relationships are longstanding when no due diligence has ever been carried out.
- Carrying out only very basic identity checks as due diligence on higher risk third parties.
- Asking third parties to fill in account opening forms which are not relevant to them (e.g. individuals filling in forms aimed at corporate entities).
- Accepting vague explanations of the business case for using third parties.
- Approvers of third-party relationships working within the broking department or being too close to it to provide adequate challenge.
- Accepting instructions from third parties to pay commission to other individuals or entities which have not been subject to due diligence.
- Assuming that third-party relationships acquired from other firms have been subject to adequate due diligence.
- Paying high levels of commission to third parties used to obtain or retain higher risk business, especially if their only role is to introduce the business.
- Receiving bank details from third parties via informal channels such as email, particularly if email addresses are from webmail (e.g. Hotmail) accounts or do not appear to be obviously connected to the third party.
- Leaving redundant third-party accounts 'live' on the accounting systems because third-party relationships have not been regularly reviewed.
- Being unable to produce a list of approved third parties, associated due diligence and details of payments made to them.

Box 9.3: Due diligence on third-party relationships

Good practice:	Poor practice:
• Taking reasonable steps to ensure that bank accounts used by third parties to receive payments are, in fact, controlled by the third party for which the payment is meant. For example, broker firms might wish to see the third party's bank statement or have the third party write them a low value cheque. • Higher or extra levels of approval for high risk third-party relationships. • Regularly reviewing third-party relationships to identify the nature and risk profile of third-party relationships. • Maintaining accurate central records of approved third parties, the due diligence conducted on the relationship and evidence of periodic reviews.	

Box 9.4: Payment controls

Good practice:	Poor practice:
• Ensuring adequate due diligence and approval of third-party relationships before payments are made to the third party. • Risk-based approval procedures for payments and a clear understanding of why payments are made. • Checking third-party payments individually prior to approval, to ensure consistency with the business case for that account. • Regular and thorough monitoring of third-party payments to check, for example, whether a payment is unusual in the context of previous similar payments. • A healthily sceptical approach to approving third-party payments. • Adequate due diligence on new suppliers being added to the Accounts Payable system. • Clear limits on staff expenditure, which are fully documented, communicated to staff and enforced. • Limiting third-party payments from Accounts Payable to reimbursements of genuine business-related costs or reasonable entertainment.	• Failing to check whether third parties to whom payments are due have been subject to appropriate due diligence and approval. • The inability to produce regular third-party payment schedules for review. • Failing to check thoroughly the nature, reasonableness and appropriateness of gifts and hospitality. • No absolute limits on different types of expenditure, combined with inadequate scrutiny during the approvals process. • The giving or receipt of cash gifts.

Box 9.4: Payment controls	
Good practice: • 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.	Poor practice:

Box 9.5: Staff recruitment and vetting	
Good practice: • Vetting staff on a risk-based approach, taking into account financial crime risk. • Enhanced vetting – including checks of credit records, criminal records, financial sanctions lists, commercially available intelligence databases and the CIFAS Staff Fraud Database – for staff in roles with higher bribery and corruption risk. • A risk-based approach to dealing with adverse information raised by vetting checks, taking into account its seriousness and relevance in the context of the individual's role or proposed role. • Where employment agencies are used to recruit staff in higher risk positions, having a clear understanding of the checks they carry out on prospective staff. • Conducting periodic checks to ensure that agencies are complying with agreed vetting standards. • A formal process for identifying changes in existing employees' financial soundness which might make them more vulnerable to becoming involved in, or committing, corrupt practices.	Poor practice: • Relying entirely on an individual's market reputation or market gossip as the basis for recruiting staff. • Carrying out enhanced vetting only for senior staff when more junior staff are working in positions where they could be exposed to bribery or corruption issues. • Failing to consider on a continuing basis whether staff in higher risk positions are becoming vulnerable to committing fraud or being coerced by criminals. • Relying on contracts with employment agencies covering staff vetting standards without checking periodically that the agency is adhering to them. • Temporary or contract staff receiving less rigorous vetting than permanently employed colleagues carrying out similar roles.

Box 9.6: Training and awareness	
Good practice: • Providing good quality, standard training on anti-bribery and corruption for all staff. • Additional anti-bribery and corruption training for staff in higher risk positions. • Ensuring staff responsible for training others have adequate training themselves.	Poor practice: • Failing to provide training on anti-bribery and corruption, especially to staff in higher risk positions. • Training staff on legislative and regulatory requirements but failing to provide practical examples of how to comply with them.

Box 9.6: Training and awareness	
Good practice: • Ensuring training covers practical examples of risk and how to comply with policies. • Testing staff understanding and using the results to assess individual training needs and the overall quality of the training. • Staff records setting out what training was completed and when. • Providing refresher training and ensuring it is kept up-to-date.	Poor practice: • Failing to ensure anti-bribery and corruption policies and procedures are easily accessible to staff. • Neglecting the need for appropriate staff training in the belief that robust payment controls are sufficient to combat anti-bribery and corruption.

Box 9.7: Risk arising from remuneration structures	
Good practice: • Assessing whether remuneration structures give rise to increased risk of bribery and corruption. • Determining individual bonus awards on the basis of several factors, including a good standard of compliance, not just the amount of income generated. • Deferral and clawback provisions for bonuses paid to staff in higher risk positions.	Poor practice: • 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.

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

Box 9.8: Incident reporting	
Good practice: • Financial crime training covers whistleblowing procedures and how to report suspicious activity.	Poor practice:

Box 9.9: The role of compliance and internal audit	
Good practice: • Compliance and internal audit staff receiving specialist training to achieve a very good knowledge of bribery and corruption risks. • Effective compliance monitoring and internal audit reviews which challenge not only whether processes to mitigate bribery and corruption have been followed but also the effectiveness of the processes themselves. • Independent checking of compliance's operational role in approving third party relationships and accounts, where relevant. • Routine compliance and/or internal audit checks of higher risk third party payments to ensure there is appropriate supporting documentation and adequate justification to pay.	Poor practice: • Failing to carry out compliance or internal audit work on anti-bribery and corruption. • Compliance, in effect, signing off their own work, by approving new third party accounts and carrying out compliance monitoring on the same accounts. • Compliance and internal audit not recognising or acting on the need for a risk-based approach.

10 The Small Firms Financial Crime Review

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

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

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

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

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

Our findings

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

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

Consolidated examples of good and poor practice

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

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

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

Box 10.4: Suspicious activity reporting	
Good practice:	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 Sanctions list he should carry on as normal and just report as a SAR to SOCA.

Box 10.5: Records

Good practice:

- An advising-only intermediary firm used a web-based system as its database of leads, contact names and addresses. It also stored telephone and meeting notes there which were accessed by staff using individual passwords.
- A home finance broker classified customers as A, B or C for record keeping purposes. A's being Active, B's being 'one-off or infrequent business' who he maintained contact with via a regular newsletter and C's being archived customers, the records for which he kept in his loft in the house.

Poor practice:

- A file review at an IFA revealed disorganised files and missing KYC documentation in three of five files reviewed. Files did not always include a checklist. The firm was advised that KYC information should be kept together in the file so that it was easily identifiable and auditable.

Box 10.6: Training

Good practice:

- A GI Intermediary used an online 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 online.
- An IFA (sole trader) carried out online training on various financial crime topics. He also participated in conference call training where a trainer talked trainees through various topics while online; this was both time and travel efficient.

Poor practice:

- A GI Intermediary explained that the compliance manager carried out regular audits to confirm staff knowledge was sufficient. However, on inspection of the training files it appeared that training was largely limited to product information and customer service and did not sufficiently cover financial crime.
- One credit union, apart from on-the-job training for new staff members, had no regular training in place and no method to test staff knowledge of financial crime issues.

Box 10.7: Responsibilities and risk assessments

Good 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 discouraging of the over-use of portable media devices, the secure disposal of data, and the logging of customer files removed and returned to the office.
- An IFA had produced a written data security review of its business which had been prompted by their external consultants and largely followed the small firms' factsheet material on data security, provided by the FSA in April 2008.

Poor practice:

- 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 risks inherent in that business.
- An advising-only intermediary had its policies and procedures drawn up by an external consultant but these had not been tailored to the firm's business. The MLRO was unclear about investigating and reporting suspicious activity to SOCA. The firm's staff had not received formal training in AML or reporting suspicious activity to SOCA.

Box 10.7: Responsibilities and risk assessments	
Good practice: • In a personal pension operator, there was a full and comprehensive anti-fraud strategy in place and a full risk assessment had been carried 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.	Poor practice:

Box 10.8: Access to systems	
Good practice: • In a Discretionary Investment Management firm, the Chief Executive ensured that he signed off on all data user profiles ensuring that systems accesses were authorised by him. • A discretionary investment manager conducted five year referencing on new staff, verified personal addresses and obtained character references from acquaintances not selected by the candidate. They also carried out annual credit checks, CRB checks and open source Internet searches on staff. They were role profiles for each job within the firm and these were reviewed monthly for accuracy. • In a venture capital firm they imposed a minimum ten character (alpha/numeric, upper/lower case) password for systems access which had a 45-day enforced change period.	Poor practice: • In a financial advisory firm there was no minimum length for passwords, (although these had to be alpha/numeric) and the principal of the firm plus one other colleague knew all staff members' passwords. • In an advising-only intermediary, staff set their own systems passwords which had no defined length or complexity and were only changed every six months.

Box 10.9: Outsourcing	
Good practice: • A discretionary investment manager used an external firm for IT support and had conducted its own on-site review of the IT firm's security arrangements. The same firm also insisted on CRB checks for cleaners. • An IFA had received a request from an introducer to provide names of customers who had bought a certain financial product. The firm refused to provide the data as it considered the request unnecessary and wanted to protect its customer data. It also referred the matter to the Information Commissioner who supported the firm's actions.	Poor practice: • An authorised professional firm employed the services of third-party cleaners, security staff, and an offsite confidential waste company, but had carried out no due diligence on any of these parties. • An IFA allowed a third-party IT consultant full access rights to its customer databank. Although the firm had a service agreement in place that allowed full audit rights between the advisor and the IT company to monitor the security arrangements put in place by the IT company, this had not been invoked by the IFA, in contrast to other firms visited where such audits had been undertaken.

Box 10.9: Outsourcing	
Good practice: • A general insurance intermediary employed office cleaners supplied by an agency that conducts due diligence including CRB checks. Office door codes were regularly changed and always if there was a change in staff. • In an authorised professional firm, unauthorised data access attempts by staff were monitored by the IT manager and email alerts sent to staff and management when identified. • In a general insurance intermediary the two directors had recently visited the offsite data storage facility to satisfy themselves about the security arrangements at the premises.	Poor practice: • In an authorised professional firm, Internet and Hotmail usage was only monitored if it was for longer than 20 minutes at any one time. There was also no clear-desk policy within the firm. • In an authorised professional firm there had been two incidents where people had walked into the office and stolen staff wallets and lap tops.

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

Box 10.11: Data disposal	
Good practice: • An advising and arranging intermediary used a third party company for all paper disposals, using secure locked bins provided by the third party. All paper in the firm was treated as confidential and 'secure paper management' was encouraged throughout the firm, enhanced by a monitored clear-desk policy. The firm was also aware that it needed to consider a process for secure disposal of electronic media as it was due to undergo a systems refit in the near future.	Poor practice: • In an IFA there was a clear-desk policy that was not enforced and customer data was stored in unlocked cabinets which were situated in a part of the office accessible to all visitors to the firm.

Box 10.11: Data disposal	
Good practice: • 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.	Poor practice: • In an IFA there was a clear-desk policy that was not enforced and customer data was stored in unlocked cabinets which were situated in a part of the office accessible to all visitors to the firm.

Box 10.12: Data compromise incidents	
Good 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.	Poor practice: • In a general insurance intermediary, the IT manager said he would take responsibility for any data security incidents although there was no procedures in place for how to handle such occurrences. When asked about data security, the compliance officer was unable to articulate the financial crime risks that lax data security processes posed to the firm and said it would be something he would discuss with his IT manager.

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

Box 10.13: General fraud	
Good practice: • 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.	Poor practice:

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

Box 10.15: Investment fraud	
Good practice: • An IFA had undertaken a risk assessment for all high net worth customers. • A discretionary investment manager referred higher risk decisions (in respect of a high risk customer/value of funds involved) to a specific senior manager. • A personal pension operator carried out a financial crime risk assessment for newly introduced investment products.	Poor practice: • An IFA had a 'one size fits all' approach to identifying the risks associated with customers and investments.

Box 10.16: Mortgage fraud	
Good practice: • The majority of firms conducted customer fact finds. This allowed them to know their customers sufficiently to identify any suspicious behaviour. CDD[6] (including source of funds information) was also obtained early in the application process before the application was completed and submitted to the lender. • A home finance broker would not conduct any remote business – meeting all customers face-to-face. • An IFA had informally assessed the mortgage fraud risks the business faced and was aware of potentially suspicious indicators. The IFA also looked at the fraud risks associated with how the company approached the firm – e.g. the firm felt that a cold call from a customer may pose a greater risk than those which had been referred by longstanding customers.	Poor practice: • An IFA did not undertake any KYC checks, considering this to be the responsibility of the lender. • An IFA did not investigate source of funds. The firm stated this was because 'a bank would pick it up and report it.' • An IFA did not undertake extra verification of its non face-to-face customers.

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

6 Customer Due Diligence. See Part 1 Annex 1 for common terms.

11 Mortgage fraud against lenders

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

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

Our findings

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

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

Consolidated examples of good and poor practice

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

Box 11.2: Applications processing and underwriting

Good practice:

- A firm's underwriting process can identify applications that may, based on a thorough assessment of risk flags relevant to the firm, present a higher risk of mortgage fraud.
- Underwriters can contact all parties to the application process (customers, brokers, valuers etc.) to clarify aspects of the application.
- The firm verifies that deposit monies for a mortgage transaction are from a legitimate source.
- New or inexperienced underwriters receive training about mortgage fraud risks, potential risk indicators, and the firm's approach to tackling the issue.

Poor practice:

- A firm's underwriters have a poor understanding of potential fraud indicators, whether through inexperience or poor training.
- Underwriters' demanding work targets undermine efforts to contain mortgage fraud.
- Communication between the fraud team and mortgage processing staff is weak.
- A firm relying on manual underwriting has no checklists to ensure the application process is complete.
- A firm requires underwriters to justify all declined applications to brokers.

Box 11.3: Mortgage fraud prevention, investigations, and recoveries

Good 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 reviews existing mortgage books to identify fraud indicators.
- Applications that are declined for fraudulent reasons result in a review of pipeline and back book cases where associated fraudulent parties are identified.
- A firm has planned how counter-fraud resources could be increased in response to future growth in lending volumes, including consideration of the implications for training, recruitment and information technology.
- A firm documents the criteria for initiating a fraud investigation.
- Seeking consent from the Serious Organised Crime Agency (SOCA) to accept mortgage payments wherever fraud is identified.

Poor practice:

- A firm's anti-fraud efforts are uncoordinated and under-resourced.
- Fraud investigators lack relevant experience or knowledge of mortgage fraud issues, and have received insufficient training.
- A firm's internal escalation procedures are unclear and leave staff confused about when and how to report their concerns about mortgage fraud.

Box 11.4: Managing relationships with solicitors, brokers and valuers

Good practice:

- A firm has identified third parties they will not deal with, drawing on a range of internal and external information.
- A third party reinstated to a panel after termination is subject to fresh due diligence checks.
- A firm checks that solicitors register charges over property with the Land Registry in good time, and chases this up.
- Where a solicitor is changed during the processing of an application, lenders contact both the original and new solicitor to ensure the change is for a legitimate reason.
- 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.

Poor practice:

- A firm's scrutiny of third parties is a one-off exercise; membership of a panel is not subject to ongoing review.
- A firm's panels are too large to be manageable. No work is undertaken to identify dormant third parties.
- A firm solely relies on the FSA Register to check mortgage brokers, while scrutiny of solicitors only involves a check of public material from the Law Society or Solicitors Regulation Authority.
- A firm that uses divisional sales managers to oversee brokers has not considered how to manage conflicts of interest that may arise.

Box 11.5: Compliance and internal audit

Good practice:

- A firm has subjected anti-fraud measures to 'end-to-end' scrutiny, to assess whether defences are coordinated, rather than solely reviewing adherence to specific procedures in isolation.
- There is a degree of specialist anti-fraud expertise within the compliance and internal audit functions.

Poor practice:

- A firm's management of third party relationships is subject to only cursory oversight by compliance and internal audit.
- Compliance and internal audit staff demonstrate a weak understanding of mortgage fraud risks, because of inexperience or deficient training.

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

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

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

12 Banks' management of high money-laundering risk situations

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

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

12.3 However, our main conclusion was that around three-quarters of banks in our sample, including the majority of major banks, were not always managing high-risk customers and PEP relationships effectively and had to do more to ensure they were not used for money laundering purposes. We identified serious weaknesses in banks' systems and controls, as well as indications that some banks were willing to enter into very high-risk business relationships without adequate controls when there were potentially large profits to be made. This meant that we found it likely that some banks were handling the proceeds of corruption or other financial crime.

Our findings

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

www.fsa.gov.uk/pubs/other/aml_%20final_report.pdf

Consolidated examples of good and poor practice

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

Box 12.1: High risk customers and PEPs – AML policies and procedures	
Good practice: • Senior management take money laundering risk seriously and understand what the Regulations are trying to achieve. • Keeping AML policies and procedures up-to-date to ensure compliance with evolving legal and regulatory obligations.	Poor practice: • A lack of commitment to AML risk management among senior management and key AML staff. • Failing to conduct quality assurance work to ensure AML policies and procedures are fit for purpose and working in practice.

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

Good practice:

- A clearly articulated definition of a PEP (and any relevant sub-categories) which is well understood by relevant staff.
- Considering the risk posed by former PEPs and 'domestic PEPs' on a case-by-case basis.
- Ensuring adequate due diligence has been carried out on all customers, even if they have been referred by somebody who is powerful or influential or a senior manager.
- Providing good quality training to relevant staff on the risks posed by higher risk customers including PEPs and correspondent banks.
- Ensuring RMs and other relevant staff understand how to manage high money laundering risk customers by training them on practical examples of risk and how to mitigate it.
- Keeping training material comprehensive and up-to-date, and repeating training where necessary to ensure relevant staff are aware of changes to policy and emerging risks.

Poor practice:

- Informal, undocumented processes for identifying, classifying and declassifying customers as PEPs.
- Failing to carry out enhanced due diligence on customers with political connections who, although they do not meet the legal definition of a PEP, still represent a high risk of money laundering.
- Giving waivers from AML policies without good reason.
- Considering the reputational risk rather than the AML risk presented by customers.
- Using group policies which do not comply fully with UK AML legislation and regulatory requirements.
- Using consultants to draw up policies which are then not implemented.
- Failing to allocate adequate resources to AML.
- Failing to provide training to relevant staff on how to comply with AML policies and procedures for managing high risk customers.
- Failing to ensure policies and procedures are easily accessible to staff.

Box 12.2: High risk customers and PEPs – Risk assessment

Good practice:

- Using robust risk assessment systems and controls appropriate to the nature, scale and complexities of the bank's business.
- Considering the money-laundering risk presented by customers, taking into account a variety of factors including, but not limited to, company structures; political connections; country risk; the customer's reputation; source of wealth/funds; expected account activity; sector risk; and involvement in public contracts.
- Risk assessment policies which reflect the bank's risk assessment procedures and risk appetite.
- Clear understanding and awareness of risk assessment policies, procedures, systems and controls among relevant staff.
- Quality assurance work to ensure risk assessment policies, procedures, systems and controls are working effectively in practice.
- Appropriately-weighted scores for risk factors which feed in to the overall customer risk assessment.
- A clear audit trail to show why customers are rated as high, medium or low risk.

Poor practice:

- Allocating higher risk countries with low risk scores to avoid having to conduct EDD.
- MLROs who are too stretched or under resourced to carry out their function appropriately.
- Failing to risk assess customers until shortly before an FSA visit.
- Allowing RMs to override customer risk scores without sufficient evidence to support their decision.
- Inappropriate customer classification systems which make it almost impossible for a customer to be classified as high risk.

Box 12.3: High risk customers and PEPs – Customer take-on

Good practice:

- Ensuring files contain a customer overview covering risk assessment, documentation, verification, expected account activity, profile of customer or business relationship and ultimate beneficial owner.
- Having all new PEP or other high-risk relationships checked by the MLRO or the AML team.
- Clear processes for escalating the approval of high risk and all PEP customer relationships to senior management or committees which consider AML risk and give appropriate challenge to RMs and the business.
- Using, where available, local knowledge and open source internet checks to supplement commercially available databases when researching potential high risk customers including PEPs.
- Having clear risk-based policies and procedures setting out the EDD required for higher risk and PEP customers, particularly in relation to source of wealth.
- Effective challenge of RMs and business units by banks' AML and compliance teams, and senior management.
- Reward structures for RMs which take into account good AML/compliance practice rather than simply the amount of profit generated.
- Clearly establishing and documenting PEP and other high-risk customers' source of wealth.
- Where money laundering risk is very high, supplementing CDD with independent intelligence reports and fully exploring and reviewing any credible allegations of criminal conduct by the customer.
- Understanding and documenting ownership structures complex or opaque corporate structures and the reasons for them.
- Face-to-face meetings and discussions with high-risk and PEP prospects before accepting them as a customer.
- Making clear judgements on money-laundering risk which are not compromised by the potential profitability of new or existing relationships.
- Recognising and mitigating the risk arising from RMs becoming too close to customers and conflicts of interest arising from RMs' remuneration structures.

Poor practice:

- Failing to give due consideration to certain political connections which fall outside the Money Laundering Regulations definition of a PEP (eg wider family) which might mean that certain customers still need to be treated as high risk and subject to enhanced due diligence.
- Poor quality, incomplete or inconsistent CDD.
- Relying on Group introductions where overseas standards are not UK-equivalent or where CDD is inaccessible due to legal constraints.
- Inadequate analysis and challenge of information found in documents gathered for CDD purposes.
- Lacking evidence of formal sign-off and approval by senior management of high-risk and PEP customers and failure to document appropriately why the customer was within AML risk appetite.
- Failing to record adequately face-to-face meetings that form part of CDD.
- Failing to carry out EDD for high risk/ PEP customers.
- Failing to conduct adequate CDD before customer relationships are approved.
- Over-reliance on undocumented 'staff knowledge' during the CDD process.
- Granting waivers from establishing a customer's source of funds, source of wealth and other CDD without good reason.
- Discouraging business units from carrying out adequate CDD, for example by charging them for intelligence reports.
- Failing to carry out CDD on customers because they were referred by senior managers.
- Failing to ensure CDD for high-risk and PEP customers is kept up-to-date in line with current standards.
- Allowing 'cultural difficulties' to get in the way of proper questioning to establish required CDD records.
- Holding information about customers of their UK operations in foreign countries with banking secrecy laws.
- 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.

Box 12.3: High risk customers and PEPs – Customer take-on	
Good practice:	Poor practice: • 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.

Box 12.4: High risk customers and PEPs – Enhanced monitoring of high risk relationships	
Good practice: • Transaction monitoring which takes account of up-to-date CDD information including expected activity, source of wealth and source of funds. • Regularly reviewing PEP relationships at a senior level based on a full and balanced assessment of the source of wealth of the PEP. • Monitoring new clients more closely to confirm or amend the expected account activity. • A risk-based framework for assessing the necessary frequency of relationship reviews and the degree of scrutiny required for transaction monitoring. • Proactively following up gaps in, and updating, CDD during the course of a relationship. • Ensuring transaction monitoring systems are properly calibrated to identify higher risk transactions and reduce false positives.	Poor practice: • Failing to carry out regular reviews of high-risk and PEP customers in order to update CDD. • Reviews carried out by RMs with no independent assessment by money laundering or compliance professionals of the quality or validity of the review. • Failing to disclose suspicious transactions to SOCA. • Failing to seek consent from SOCA on suspicious transactions before processing them. • Unwarranted delay between identifying suspicious transactions and disclosure to SOCA. • Treating annual reviews as a tick-box exercise and copying information from the previous review. • Annual reviews which fail to assess AML risk and instead focus on business issues such as sales or debt repayment.

Box 12.4: High risk customers and PEPs – Enhanced monitoring of high risk relationships

Good practice:

- Keeping good records and a clear audit trail of internal suspicion reports sent to the MLRO, whether or not they are finally disclosed to SOCA.
- A good knowledge among key AML staff of a bank's highest risk/PEP customers.
- More senior involvement in resolving alerts raised for transactions on higher risk or PEP customer accounts, including ensuring adequate explanation and, where necessary, corroboration of unusual transactions from RMs and/or customers.
- Global consistency when deciding whether to keep or exit relationships with high-risk customers and PEPs.
- Assessing RMs' performance on ongoing monitoring and feed this into their annual performance assessment and pay review.
- Lower transaction monitoring alert thresholds for higher risk customers.

Poor practice:

- Failing to apply enhanced ongoing monitoring techniques to high-risk clients and PEPs.
- Failing to update CDD based on actual transactional experience.
- Allowing junior or inexperienced staff to play a key role in ongoing monitoring of high-risk and PEP customers.
- Failing to apply sufficient challenge to explanations from RMs and customers about unusual transactions.
- RMs failing to provide timely responses to alerts raised on transaction monitoring systems.

Box 12.5: Correspondent banking – Risk assessment of respondent banks

Good practice:

- Regularly 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.
- More robust monitoring respondents identified as presenting a higher risk.
- Risk scores that drive the frequency of relationship reviews.
- Taking into consideration publicly available information from national government bodies and non-governmental organisations and other credible sources.

Poor practice:

- Failing to consider the money-laundering risks of correspondent relationships.
- Inadequate or no documented policies and procedures setting out how to deal with respondents.
- Applying a 'one size fits all' approach to due diligence with no assessment of the risks of doing business with respondents located in higher risk countries.
- Failing to prioritise higher risk customers and transactions for review.
- Failing to take into account high-risk business types such as money service businesses and offshore banks.

Box 12.6: Correspondent banking – Customer take-on

Good practice:

- Assigning clear responsibility for the CDD process and the gathering of relevant documentation.
- EDD for respondents that present greater risks or where there is less publicly available information about the respondent.
- Gathering enough information to understand client details; ownership and management; products and offerings; transaction volumes and values; client market segments; client reputation; as well as the AML control environment.
- Screening the names of senior managers, owners and controllers of respondent banks to identify PEPs and assessing the risk that identified PEPs pose.
- Independent quality assurance work to ensure that CDD standards are up to required standards consistently across the bank.
- Discussing with overseas regulators and other relevant bodies about the AML regime in a respondent's home country.
- Identifying risk in particular business areas (eg informal value transfer such as 'hawala', tax evasion, corruption) through discussions with overseas regulators.
- Visiting, or discuss with, respondent banks to discuss AML issues and gather CDD information.
- Gathering information about procedures at respondent firms for sanctions screening and identifying/managing PEPs.
- Understanding respondents' processes for monitoring account activity and reporting suspicious activity.
- Requesting details of how respondents manage their own correspondent banking relationships.
- Senior management/senior committee sign-off for new correspondent banking relationships and reviews of existing ones.

Poor practice:

- Inadequate CDD on parent banks and/or group affiliates, particularly if the respondent is based in a high-risk jurisdiction.
- Collecting CDD information but failing to assess the risks.
- Over-relying on the Wolfsberg Group AML questionnaire.
- Failing to follow up on outstanding information that has been requested during the CDD process.
- Fail to follow up on issues identified during the CDD process.
- Relying on parent banks to conduct CDD for a correspondent account and taking no steps to ensure this has been done.
- Collecting AML policies etc but making no effort to assess them.
- Having no information on file for expected activity volumes and values.
- Failing to consider adverse information about the respondent or individuals connected with it.
- No senior management involvement in the approval process for new correspondent bank relationships or existing relationships being reviewed.

Box 12.7: Correspondent banking – Ongoing monitoring of respondent accounts

Good practice:

- Review periods driven by the risk rating of a particular relationship; with high risk relationships reviewed more frequently.
- Obtaining an updated picture for the purpose of the account and expected activity.
- Updating screening of respondents and connected individuals to identify individuals/ entities with PEP connections or on relevant sanctions lists.
- Involving senior management and AML staff in reviews of respondent relationships and consideration of whether to maintain or exit high risk relationships.
- Where appropriate, using intelligence reports to help decide whether to maintain or exit a relationship.
- Carrying out ad-hoc reviews in light of material changes to the risk profile of a customer.

Poor practice:

- Copying periodic review forms year after year without challenge from senior management.
- Failing to take account of any changes to key staff at respondent banks.
- Carrying out annual reviews of respondent relationships but fail to consider money-laundering risk adequately.
- Failing to assess new information gathered during ongoing monitoring of a relationship.
- Failing to consider money laundering alerts generated since the last review.
- Relying on parent banks to carry out monitoring of respondents without understanding what monitoring has been done or what the monitoring found.
- Failing to take action when respondents do not provide satisfactory answers to reasonable questions regarding activity on their account.
- Focusing too much on reputational or business issues when deciding whether to exit relationships with respondents which give rise to high money-laundering risk.

Box 12.8: Wire transfers – Paying banks

Good practice:

- Banks' core banking systems ensure that all static data (name, address, account number) held on the ordering customer are automatically inserted in the correct lines of the outgoing MT103 payment instruction and any matching MT202COV.

Poor practice:

- Paying banks take insufficient steps to ensure that all outgoing MT103s contain sufficient beneficiary information to mitigate the risk of customer funds being incorrectly blocked, delayed or rejected.

Box 12.9: Wire transfers – Intermediary banks	
Good practice: • Where practical, intermediary and beneficiary banks delay processing payments until they receive complete and meaningful information on the ordering customer. • Intermediary and beneficiary banks have systems that generate an automatic investigation every time a MT103 appears to contain inadequate payer information. • Following processing, risk-based sampling for inward payments identify 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.	Poor practice: • 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.

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

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

PUB REF: 002558

The Financial Services Authority
25 The North Colonnade Canary Wharf London E14 5HS
Telephone: +44 (0)20 7066 1000 Fax: +44 (0)20 7066 1099
Website: www.fsa.gov.uk

Registered as a Limited Company in England and Wales No. 1920623. Registered Office as above.