Financial Services Authority
Enforcement and Financial Crime Division

The Small Firms Financial Crime Review

A review of the small firms sector implementation of anti-financial crime systems and controls

May 2010

Contents

1. Executive summary

1.1 Introduction

1. The Small Firms Financial Crime Review ('the review') was conducted in response to the findings of the Financial Action Task Force (FATF) in its Mutual Evaluation of the UK (2007), and National Audit Office (NAO) recommendations (2007). Their conclusions were that the targeting and effectiveness of our thematic work did not ensure adequate knowledge of compliance standards by the small firms sector concerning financial crime.

2. To address the findings of the FATF and NAO, the FSA launched a major thematic project in April 2008, aimed at establishing the extent to which small firms across the financial services industry addressed financial crime risks in their businesses. This approach allowed for a manageable sample size of firms (the FSA supervises around 16,500 small firms) to be included in the visit population, and for robust conclusions for the sector as a whole to be drawn from the findings. The project was re-phased due to the secondment of project team members in 2009 to bolster the supervision of high impact firms.

3. The review undertook visits to 159 firms, across the wholesale and retail sectors. It was the FSA's first in-depth assessment of financial crime systems and controls in the small firm sector, and thus a part of the FSA's more intensive scrutiny of the sector as a whole.

4. The review covered three main areas – anti-money laundering/financial sanctions, data security and fraud controls. Given the wide range of legislation and regulations applicable to the sector – with variations of applicability according to firm type – one element of our review was whether firms clearly understood the requirements on them. These requirements are set out in Chapter 2.[1]

5. To assist readers and users of this report the findings in Chapter 3 are set out in the format illustrated below:

This box indicates the **types of firm** for which the findings are most relevant, eg: **all firms**.

1 Market abuse is a type of financial crime; but it did not form part of this review. This was because we decided to focus our attention on aspects of financial crime risk were most relevant to the small firm sector: anti-money laundering, data security and fraud.

6. An opening passage then summarises the aims of the review for a particular issue and outlines the areas addressed by the project team, as illustrated below:

Aim of review

The **opening passage** sets out the key issues which were addressed, eg:

To assess small firms' awareness of their requirements under relevant legislation, |eg: Proceeds of Crime Act 2002 (POCA), Terrorism Act, Money Laundering Regulations 2007 and, where applicable, the role of the Money Laundering Reporting Officer (MLRO).

The review focused on:

- anti-money laundering (AML) policies and procedure;
- firms' consideration of the Joint Money Laundering Steering Group (JMLSG)guidance;
- role of the MLRO and Compliance Officers; and
- suspicious activity reports (SARs) to the Serious Organised Crime Agency (SOCA).

7. Finally, in each section of the Findings we have outlined a non-exhaustive range of questions that firms should ask themselves to help ensure they are meeting the standards required, as illustrated below:

Questions to ask yourself

- Do your policies and procedures take account of your legal obligations including; Proceeds of Crime Act 2002, Money Laundering Regulations 2007, Terrorism Act 2000?
- Do your policies and procedures consider the guidance issued by the JMLSG?
- Is there a designated Compliance Officer and/or MLRO?

8. This report does not constitute nor should it be treated as formal FSA guidance. However, we expect firms to make use of our findings, to translate them into a more effective assessment of the risks in their business, and to implement and maintain more effective and appropriate controls where necessary. As in any other area of their business, firms should take an appropriate, risk-based approach to financial crime considering relevant factors including their customer base, business and risk profile. Failure to do so may result in the FSA taking action.

9. We would like to thank the firms which participated in the review, for the information they supplied before and during our visits, and for meeting us. We would also like to thank the stakeholders for their advice and assistance.

1.2 Findings

10. There were several weaknesses across the sector in implementing systems and controls to reduce the risks from financial crime. While firms generally demonstrated a reasonable awareness of their regulatory and legal obligations, particularly regarding AML systems and controls, there were shortfalls in the implementation of those systems and controls to reduce the risks from financial crime.

11. While most firms with obligations under the Money Laundering Regulations 2007 had adequate customer due diligence systems (also referred to as Know Your Customer or 'KYC'), very few firms had appropriate enhanced due diligence systems in place to identify or deal with higher risk customers or situations such as non face-to-face sales, e.g. where customers can purchase products online.[2]

12. Firms' knowledge, and implementation, of the UK's financial sanctions regime was weak across the sector. Most firms were unclear as to their responsibilities if they identified a 'hit' on the Sanctions list and were generally unaware of the requirements on them under the relevant legislation.

13. Most firms visited relied on policies and procedures that had been prepared by consultants. However, a significant proportion of these firms were unable to, or unaware of the need to, tailor these to their business. In particular, we noted a lack of financial crime risk assessments for different products.

14. Formal vetting and appropriate referencing of staff was weak in several firms. Many small firms employed staff through close links such as long standing relationships, previous colleagues or family members. As a result the formal consideration of a person's integrity and honesty was often overlooked.

15. Where vetting or referencing was more formally undertaken at the initial recruitment stage, it was rarely revisited or reassessed during a person's employment. So, for example, changes in a staff member's financial or personal circumstances which might indicate a more heightened susceptibility to financial crime were rarely explored.

16. Many small firms had written policies and authorisations for granting staff appropriate access to customer data systems; however these tended to vary in formality from those requiring senior management acknowledgments and sign off, to a far less rigid approach and general acceptance by senior management of a less formal approach.

17. The majority of small firms had appropriate physical security for their business although firms tended to regard security more as protecting fixed assets or property, rather than defending against customer data compromise or data theft.

2 See Box 6 at pg 18.

18. Across the sector there was a good awareness and understanding of the need to securely dispose of confidential paper, either by shredding on-site or by employing reputable third party disposal companies to perform the task. However, there was a limited understanding, or consideration, of how to securely dispose of electronic data and computer equipment.

19. Few small firms were aware of their obligations in respect of managing and mitigating fraud risk. Most small firms had some awareness of their fraud risks but the extent to which this was formalised and communicated within firms in the form of specific fraud policies and procedures varied significantly.

20. Firms' awareness tended to focus on the risk that their firm might incur fraud losses as opposed to the risk that their business might be used to facilitate fraud. For most, controls therefore focused on mitigating this risk – for example, developing and maintaining robust internal financial controls.

21. Reported fraud incidents and losses were low. Where fraud had occurred, firms were generally quick to develop a more robust framework to ensure these incidents were not replicated.

1.3 Conclusions

22. Although individually they are 'low impact', small firms can collectively pose significant risks to the FSA's statutory objective to reduce financial crime. In particular the review noted 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. Having effective customer take-on procedures is therefore essential in ensuring that criminals do not gain access to the UK financial sector. While firms generally had adequate customer due diligence arrangements, we were concerned by the weaknesses we identified in firms' enhanced due diligence procedures for dealing with high risk customers or situations. These should be addressed.

23. The importance of robust customer due diligence to prevent firms undertaking business with individuals or entities subject to financial sanctions is clear. However, small firms remain weak in their knowledge and implementation of the UK financial sanctions regime. The FSA has made a substantial effort to raise the industry's standards in this area and a small firms factsheet was published to assist small firms following our thematic work in this area in 2009.[3] We expect firms to use these materials as they have done with our data security publications.

3 The link to the Sanctions spreadsheet is here: http://www.fsa.gov.uk/smallfirms/resources/pdfs/Sanctions.pdf

24. Generally, firms had greater awareness of the need for anti-money laundering and data security systems and controls than of those for preventing fraud. However with robust anti-money laundering and data security systems and controls small firms can go some way to prevent themselves being used for, or becoming the victims of, fraud. While few firms had developed specific fraud controls to reduce the risk that their firm might be used to ease fraud, recorded fraud incidents and losses by firms visited were low. Where fraud had occurred, firms were quick to develop a more robust framework to ensure these incidents were not repeated.

25. During the review we observed that the small firms sector had paid more attention to financial crime issues. We noted that a significant proportion of the firms visited had been using the information and materials provided by the FSA on data security to mitigate risks in this area. Notwithstanding this encouraging observation, we considered the sector to be generally weak in its assessment and mitigation of financial crime risks.

Contact

This report is published for information but your comments are welcomed.

Please contact:

Financial Crime Operations Team
Financial Services Authority
25 The North Colonnade
London
E14 5HS

Email: mark.persad@fsa.gov.uk

2. Introduction

2.1 Background

26. The review was undertaken in response to the findings of the FATF in its Mutual Evaluation of the UK 2007, and the recommendations of the NAO in 2007. They concluded that the targeting and effectiveness of our thematic work did not ensure adequate knowledge of the compliance standards by the small firms sector concerning financial crime.

27. The review conducted visits to 159 small firms from the retail and wholesale sectors. It was the first systematic review of financial crime systems and controls in small firms conducted by the FSA.

28. The main purpose of the review was to gather information on current anti-financial crime practices in small firms, identify good practice to share with the industry, and highlight areas where improvement is required. We have incorporated several examples of good and poor practice observed during our fieldwork; these are set out in Appendix 2.

2.2 Methodology

29. We obtained pre-visit information from each firm including relevant financial crime policies and procedures, details of fraud events and any other relevant financial crime documentation.

30. We interviewed staff with key roles in each firm to get a balanced view of how financial crime risks were managed and identify at what level in the management structure it was dealt with. Where dedicated roles existed, we met the staff responsible for financial crime; although in some cases the small firms were sole traders or partnerships where individuals had more than one role.

2.3 What is financial crime?

31. The Financial Services and Markets Act (FSMA) defines financial crime as including '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'. So this is not an exhaustive list and includes, for example, corruption or funding terrorism. During the course of the review the visit teams spent time with firms explaining how their firms or business could be exploited for the purposes of financial crime. Examples of how small firms may be affected are listed in Box 1.

Box 1

A firm **directly suffers from a financial crime** if, for example:

- the firm is defrauded by an employee (e.g. a company director embezzles corporate funds);
- the firm is defrauded by a customer (e.g. a borrower gives false details and disappears); or
- the firm is defrauded by organised criminals (e.g. a gang stage a motor accident and claim against an insurance policy).

A firm **is exploited as a vehicle for financial crime** if, for example:

- criminals use the firm's services to launder the proceeds of crime;
- a firm's customer makes payments to terrorists (eg: in December 2007, three men were convicted in Germany on charges of attempting to raise US$6.3 million for Al Qaeda by faking a death to collect on nine life insurance policies); and
- customer data held by the firm is stolen and used to commit identify theft.

A firm, or a representative of the firm, **carries out a financial crime**, perhaps in collusion with another party if, for example:

- an advisor knowingly overstates the income of a customer to obtain a mortgage for which the customer was not otherwise eligible.

2.4 What we require of small firms

32. Reducing the extent to which it is possible for a business to be used for a purpose connected with financial crime is one of the FSA's five statutory objectives. Consequently, all firms are subject to a high-level **regulatory** requirement. This sits in the Systems and Controls chapter of the FSA's Handbook (Senior Management Arrangements, Systems and Controls (SYSC 6.1.1R[4]) and states:

'A firm must establish, implement and maintain adequate policies and procedures sufficient to ensure compliance of the firm including its managers, employees and appointed representatives (or where applicable, tied agents) with its obligations under the regulatory system and for countering the risk that the firm might be used to further financial crime.'

4 From 1 April 2009, SYSC 6.1.1.R has applied to firms that are subject to the Markets in Financial Instruments Directive and the Capital Requirements Directive. Insurers, managing agents and the Society of Lloyd's continue to fall under SYSC 3.2.6, although the effect is the same.

33. Financial crime is also relevant to other parts of the Handbook. For example, **all** firms are obliged to report fraud, irregularities and other errors which are significant to the FSA. Financial crime is also relevant to the **Principles for Businesses** which, among other things, require a firm to take reasonable care to organise and control its affairs responsibly and effectively (Principle 3). **Approved Persons** are under similar obligations under the Statements of Principle for Approved Persons. Financial crime considerations could affect the **threshold conditions**, particularly assessments of suitability.

34. All authorised firms (apart from mortgage brokers, general insurance intermediaries, and general insurers, including Lloyd's and managing agents) are subject to the **Money Laundering Regulations 2007**. There are also specific money laundering systems and controls requirements in the FSA Handbook (SYSC 6.3); these apply to all firms (apart from mortgage brokers, general insurers and general insurance intermediaries).

2.5 What the law requires of small firms

35. The small firms sector has many legal obligations related to financial crime. Some of the key pieces of UK legislation that small firms are subject to are summarised in Box 2.

4 The Organisation for Economic Cooperation and Development (OECD) defines facilitation payments as those made to government employees to speed up an administrative process where the outcome is already pre-determined. They are illegal under UK anti-bribery legislation.

Box 2: Some key legislation

Proceeds of Crime Act 2002

Criminalises all forms of money laundering and creates other offences such as failing to report a suspicion of money laundering and "tipping off" (see Appendix 1 Glossary).

Data Protection Act 1998

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.

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.

Counter Terrorism Act 2008

Enables HM Treasury to direct financial firms to restrict their business with specific jurisdictions of concern to the UK government. The FSA has a duty to secure firms' compliance with any direction that is made.

Criminal Justice Act 1993

Captures the offence of insider dealing. This includes the offence of tipping off, where inside information is disseminated to a third party. Tipping off is punishable regardless of whether the information received is actually traded on or not.

2.6 The Money Laundering Regulations 2007

36. All small firms (apart from mortgage brokers, general insurance intermediaries, and general insurers, including Lloyd's and managing agents) are subject to the Money Laundering Regulations 2007. The regulations require that firms take specified steps to detect and prevent both money laundering and terrorist financing: more detail is in Box 3.

Box 3: Key requirements of the Money Laundering Regulations 2007

The Regulations require that firms establish **appropriate** and **risk-sensitive** policies and procedures relating to:

- **customer due diligence** checks;
- **ongoing monitoring** of business relationships
- **reporting of suspicions**, both within the firm, and to SOCA;
- assessment of money laundering risks and the application of enhanced due diligence measures in **higher risk situations** (e.g. politically exposed persons; see Box 6);
- **record keeping;**
- **monitoring compliance** with procedures;
- **internal communication** of policies and procedures; and
- **staff awareness** and **training** on money laundering matters.

The FSA has a legal duty to take measures to secure firms' compliance with the requirements of the Regulations.

37. There are also specific money laundering systems and controls requirements in the FSA Handbook (SYSC 6.3). These apply to all small firms (**apart from mortgage brokers, general insurers and general insurance intermediaries**) and are summarised in Box 4.

Box 4: Money laundering systems and controls requirements

A firm should ensure that its systems and controls:

- enable it to **identify, assess, monitor and manage** money laundering risk;
- are **comprehensive;**
- are **proportionate;** and
- are **regularly assessed** to ensure they are adequate.

A firm must also allocate overall responsibility for anti-money laundering systems and controls to a director or senior manager. The firm must also appoint an MLRO, who will usually be located in the United Kingdom. (See SYSC 6.3 for the full requirements).

2.7 Industry guidance

38. Detailed practical guidance on the steps that small firms can take to meet their legal and regulatory anti-money laundering obligations is available from the JMLSG, a body made up of trade associations from across the industry.

    Their guidance is formally approved by the UK government, which means a court must take into account whether a firm has followed the guidance when considering if an offence has been committed. The FSA is also required to take account of whether the firm has followed the JMLSG guidance when making decisions related to a firm's money laundering defences. Where a firm departs from the Guidance, they should be prepared to justify their reasons for doing so to the FSA. The guidance can be found at http://www.jmlsg.org.uk.

2.8 Mortgage brokers, general insurers and general insurance intermediaries

39. As noted above, 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 SYSC provisions** that specifically relate to money laundering.

40. Notwithstanding the above, during the review we noted that some small firms had, as a matter of good practice, voluntarily adopted a number of the requirements of the Money Laundering Regulations or the SYSC provisions. In particular, several small firms had appointed an MLRO even though they were not required to do so. Firms said this allowed for a more efficient delineation of responsibilities and mitigation of financial crime risks in their businesses and gave staff a clear point of contact for financial crime enquiries.

41. However, we noted that some small firms in this group, particularly the sole traders, had difficulty in aligning their financial crime systems and controls to the legislative and regulatory requirements. Box 5 below answers some of the regular questions firms in this category posed to the review teams.

Box 5: Mortgage brokers, general insurers and general insurance intermediaries

Q. I am a firm that is not subject to the Money Laundering Regulations 2007. Does this mean that I have no obligations related to money laundering?

A. Mortgage brokers, general insurers 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, and, as such, there is no legal requirement to, for example, identify their customers and verify their identity (although, they may decide to do so for other reasons, such as fraud control). IT is nonetheless still possible for these firms to violate the Proceeds of Crime Act; they may, for example, become directly involved in money laundering, or tip off a criminal about a police investigation.

Q. Are mortgage brokers, general insurers and general insurance intermediaries firms required to appoint an MLRO?

A. No, however, they may choose to appoint someone to an equivalent role in case it proves necessary for the firm to report suspicions to SOCA. Where they do so, this person will be subject to the reporting obligations in the Proceeds of Crime Act and the Terrorism Act.

Q. Does the mortgage lender or the mortgage broker have responsibility for ID checks?

A. The Money Laundering Regulations require lenders to identify their customers and verify their identity, although this can be undertaken by an agent, which is often a mortgage broker. The lender nonetheless remains liable under the Regulations for any failure to apply measures.

Q. What customer due diligence checks should a mortgage broker carry out on a new client?

A. A mortgage broker needs to demonstrate that it has sufficient systems and controls to counter the risk that it can be used to further financial crime. If it carries out ID checks on behalf of a lender it should ensure they are in accordance with the lender's requirements.

5 See: http://www.transparency.org/policy_research/surveys_indices/cpi/2009

3. Findings

3.1 Anti-money laundering

The findings in this section are relevant to **all authorised firms** although **general insurance** firms and **mortgage brokers** have more limited responsibilities: see chapter 2.

3.1.1 Firms knowledge of their regulatory and legal obligations

Aim of review

To assess small firms' awareness of their requirements under relevant legislation eg: Proceeds of Crime Act (POCA), Terrorism Act, Money Laundering Regulations 2007 and, where applicable, the role of the Money Laundering Reporting Officer (MLRO).

The review focused on:

- AML policies and procedure;
- firms' consideration of the JMLSG guidance; and
- role of the MLRO and Compliance Officers.

42. There was a good general awareness of the AML systems and controls small firms are required to have in place.

43. The majority of small firms had policies and procedures in place which included requirements under POCA and the Terrorism Act.

44. The use of external consultants to produce policies and procedures was widespread throughout the sector. However, where consultants had produced policies and procedures on behalf of the firm, these had generally not been tailored by the firms to suit their business. In particular, we noted a lack of financial crime risk assessments of different products.

> *The use of consultants to produce policies and procedures was most popular with independent financial advisers (IFAs); 52% (22 out of 42) of our sample chose to do this. However, where consultants had produced policies and procedures on behalf of the firm, these had generally not been tailored by the senior management of the firms.*

45. The majority of our visit population had appointed an MLRO and this role was, in most cases combined with that of the Compliance Officer.

Questions to ask yourself

- Do your policies and procedures take account of your legal obligations under the following legislation: Proceeds of Crime Act, Money Laundering Regulations 2007, Terrorism Act?
- Do your policies and procedures consider the guidance issued by (JMLSG)?
- Is there a designated Compliance Officer and/or MLRO?

3.1.2 Account opening procedures

Aim of review

To test how effectively small firms verified the identity of new customers and identified potentially high risk individuals including identifying beneficial owners, (where relevant), and obtained information on the purpose and intended nature of the business relationship.

The review focused on:

- customer take-on procedures;
- enhanced due diligence procedures; and
- procedures to comply with UK financial sanctions.

46. Nearly all firms visited had policies and procedures in place which included verification of personal/business customers and beneficial owners (where appropriate).

47. The majority of firms were proficient at adopting customer take-on procedures, namely collecting appropriate identification verification documents and keeping suitable records of this information, for routine customers.

48. Only a minority of firms had enhanced due diligence procedures in place to deal with high risk customers or situations. The most common reason given for not having such procedures was that the firm believed their customers were low risk. However, most firms could not demonstrate how they had made this assessment. Even firms with procedures in place were, on occasions, confused as to their responsibilities in this area. We have set out in Box 6 below some of the key issues that firms should address when dealing with high risk customers or situations.

Box 6: Higher risk customers/situations

The law requires that firms' anti-money laundering policies and procedures are sensitive to risks. It also identifies some higher-risk situations that deserve greater scrutiny ('enhanced due diligence'):

- **Non-face-to-face transactions**: this is where the firm does not meet the customer in person, perhaps because business is conducted by telephone or the internet. Extra measures are necessary.
- **Politically exposed person (PEP)**: a customer may be a PEP if he/she holds certain prominent public offices abroad. In these circumstances a firm should apply extra measures to ensure it does not handle the proceeds of corruption. These extra measures must also be applied to customers who are close associates or family of a PEP. A firm's senior management must approve the initiation of a business relationship with a PEP (or the continuation, where an existing customer becomes a PEP).
- **Other situations that present a higher risk**: this might include dealing with high-net-worth individuals or certain higher-risk countries as well as transactions which are unusual, lack an obvious economic or lawful purpose, are complex or large or might lend themselves to anonymity.

49. A minority of firms visited had procedures in place to meet their responsibilities under the UK financial sanctions regime. Of these firms none had identified a 'hit' on the UK Sanctions List.

> *Only 26% of all firms visited (41 firms) had any sanctions procedures in place. Of those firms that did have procedures in place, none had identified a 'hit' on the UK Sanctions List.*

50. There was some confusion amongst firms as to what should do in terms of identifying and reporting a 'hit' on the UK Sanctions List. A very small proportion of firms recognised the requirement to refer a relevant 'hit' to the Asset Freezing Unit of Her Majesty's Treasury (HMT).

Questions to ask yourself

- What do you require to identify and verify the identity of new customers (using electronic or paper documents)? Are these procedures always applied?
- What measures do you take to identify customers who are higher risk?
- Do you screen your customer list against the HMT Sanctions list?
- Do you have a procedure in place for dealing with 'hits' identified on the HMT Sanctions list?

3.1.3 Monitoring activity

Aim of review

To measure the extent and effectiveness of customer monitoring systems within small firms. The review focused on:

- monitoring customer activity;
- suspicious activity monitoring; and
- managing 'hits' on monitoring systems.

51. Firms showed a limited understanding of customer monitoring procedures, with most thinking that customer monitoring did not apply to their businesses as they did not deal with regular transactions. This confusion between transaction monitoring and general monitoring of customer activity resulted in some firms dismissing the need to identify where a customer's activity was inconsistent with the firm's knowledge of their financial circumstances or source of funds.

52. Some firms had effective monitoring systems in place, capable of identifying suspicious activity. Monitoring ranged from electronic systems producing exception reports relating to account activity through to regular face-to-face customer meetings. However, only a very small proportion of these firms had effective procedures in place for managing 'hits' on these systems.

17 out of 42 (40%) IFAs visited had monitoring systems in place capable of identifying suspicious activity. However, only nine of these had effective procedures for managing 'hits' on these systems.

Questions to ask yourself

- Do you have an effective system in place for monitoring the activity of your customers?
- Is this monitoring system capable of identifying suspicious activity?
- Do you have effective procedures in place for dealing with 'hits' on your monitoring system?
- How do you adjust your monitoring system for higher risk customers?

3.1.4 Suspicious Activity Reporting (SARs)

Aim of review

To test whether firms were aware of their responsibility to report suspicious activity to (SOCA) at the earliest opportunity.

The review focused on:

- identifying and investigating suspicious activity; and
- when and how small firms report suspicious activity to SOCA.

53. Three firms out of 159 reviewed had submitted a Suspicious Activity Reporting (SAR) to SOCA.

54. The majority of firms visited were aware of their responsibilities to report suspicious activity. However, a small number of these firms did not know where to send these reports, either believing that SARs should be reported to the FSA or mistakenly believing that they should be sent to the National Criminal Intelligence Service (NCIS), which also reflected a worrying lack of knowledge or updating of procedures as SOCA superseded NCIS in April 2006.

55. The majority of MLROs were able to exercise their personal judgement when investigating an internal suspicious activity report and when deciding whether to report to SOCA.

Examples offered by firms of incidents that would raise raising suspicion included: quick cancellation of policies; size of transaction; out-of-the-ordinary customer behaviour; no advance notice of a significant transaction; going against advice; hits on PEP or Sanctions list; large or multiple claims; customers attempting to pay with cash; no source of funds; false or inaccurate information presented at 'KYC' stage; and customers being evasive or unwilling to provide information.

56. Half of the firms reviewed had a pro-forma to submit SARs to SOCA. However, in the majority of cases no suspicious activity had been identified.

Questions to ask yourself

- Do you have a process in place for investigating suspicious activity and reporting to SOCA?
- Are you and your staff (where applicable) aware of your responsibility to identify suspicious activity and escalate to the MLRO/designated person?

3.1.5 Record keeping

Aim of review

To identify whether small firms were ensuring that their customer data or information was; up to date, could be accessed easily and was kept for the required amount of time (five years after the relationship with the customer had ended).

The review focused on:

- How small firms store and maintain customer data.

57. The majority of files and KYC records reviewed were in good order and were easy to navigate.

> *112 out of 159 (70%) firms kept their records in electronic and hard copy formats. 26 firms kept just paper records and three firms kept just electronic records.*

58. Most firms kept their records in both electronic and hard copy formats. Of those firms that used a single method of record keeping, paper records were by far the most popular option.

Questions to ask yourself

- Are your customer records kept for at least 5 years after the relationship with the customer has ended?
- Can your records be retrieved promptly in response to a Production Order?
- Are your records readily available for audit or investigation?

3.1.6 Staff training

Aim of review

To test whether firms ensured that relevant members of staff were trained on how its products and services could be used as a vehicle for money laundering or terrorist financing and that firms' procedures managed this risk.

The review focused on:

- the methods adopted for staff training in financial crime related topics;
- the frequency of such training;
- how knowledge was tested; and
- how training records were maintained.

59. The majority of firms visited trained their staff regularly in financial crime related topics and many of those firms kept records of their training.

60. While a small number of firms used computer based training, other firms preferred to have face-to-face training, most commonly conducted by external consultants.

- *98 out of 159 (62%) firms visited trained their staff regularly in financial crime related topics and 79 firms (50%) kept records of this training; and*
- *17 firms (11%) used computer based training which included a test at the conclusion of the training.*

61. Most firms which had no formalised training programmes were sole traders who kept themselves informed by reading information produced by Trade Associations, the FSA and compliance consultants.

Questions to ask yourself

- Is financial crime training provided to all members of staff, and has it been tailored to the requirements of their job? Does this training include a test?
- Is financial crime training repeated at regular intervals (at least every two years)?
- Is the financial crime knowledge of key members of staff (e.g. MLRO) regularly updated?

3.2 Data security

The findings in this section are relevant to **all authorised firms**.

3.2.1 Responsibilities and risk assessment

Aim of review

To understand the approach that senior management of small firms took in identifying their responsibilities for customer data and the methods that firms used to identify the risks associated with their businesses.

The review focused on:

- risk assessment process;
- firms' awareness of data security risks; and
- loss or theft of customer data.

62. Over half of the firms visited had carried out some form of data security risk assessment within their business.

63. Just under half of firms visited were aware of the FSA's small firms factsheet published in April 2008, 'Your responsibilities for customer data security', We were encouraged to see that this had been useful in providing areas of focus for carrying out specific data security risk assessments in most of these firms.

> *69 out of 159 firms (43%) had used the FSA's factsheet for small firms on data security, and in most cases had used the document as part of their risk assessment process.*
> *http://www.fsa.gov.uk/smallfirms/resources/factsheets/pdfs/data_security.pdf*

64. The majority of firms had a specific person(s) in a senior position that had overall responsibility for data security.

65. Most firms had experienced no instances of lost customer data, nor been the victims of a theft of customer data. As a consequence the majority had no record or log of such incidents, although if such an incident took place they would institute such a register.

Questions to ask yourself

- Is there a specific focus on data security in your firm?
- Is there a specific individual with responsibility for data security?
- Do you have any written policies or procedures covering data security which are proportionate to your business?
- Does the culture of the firm encourage staff to report data security concerns?

3.2.2 Access to systems

Aim of review

To test the controls that existed around the recruitment of staff and the granting of appropriate access to data systems relevant to an individual's role.

The review focused on:

- staff vetting processes;
- how vetting relates to data access; and
- whether data access is job or role specific.

66. While over half of small firms had a formal process for granting staff access to their systems and databases, we found the formality of approach varied greatly between firms. While some firms had specific written procedures which staff were required to sign and acknowledge their understanding of their requirements, others were less formalised with processes and data system access rights loosely defined. In many cases this was because firms were operating in a small office environment and the close proximity of staff in their day to day activities meant that monitoring, though informal, was regular.

67. In the majority of small firms (given their size) there was no specific HR function responsible for recruitment and vetting, with recruitment issues generally handled and managed by senior management close to the business. Where such functions did exist, the link with the recruitment and vetting of staff was generally satisfactory.

68. Nearly half of the firms carried out some form of staff vetting before granting them access to data systems. However, the standards and extent of vetting varied between firms and very few carried out any form of repeat vetting once staff had been employed.

> *47% of firms (75 firms) vetted their staff before granting access to systems. However, the standards and extent of vetting varied between firms and only 8% of firms (13 firms) said they repeated vetting of any kind once staff had been employed.*

69. In almost half of firms, staff access to systems was limited and relevant to the roles or job being performed, and in just over a third of firms there was some form of controls to monitor staff changing roles or jobs which could have an effect on their requirements to view certain data.

Questions to ask yourself

- Are recruitment processes robust enough to identify potential staffing issues or concerns?
- Do staff have appropriate access to customer data in their day to day role?
- When staff change roles are unnecessary access rights removed in good time?
- Could you perform random checking to ensure that staff are accessing customer data for legitimate business reasons?

3.2.3 Outsourcing

Aim of review

To assess whether firms outsourced any customer data responsibilities to third parties or whether they allowed third parties access to their customer data, either by design or error.

The review focused on:

- how customer data is shared and with whom;
- firms' understanding of third party security; and
- unsupervised access of third parties.

70. Over half the firms visited shared customer data with third parties, in a variety of ways. These included providing 'know your customer' details to product providers when required, using IT companies to administer or trouble shoot data systems, and using offsite providers for data storage and destruction.

71. Of these firms less than a quarter had confidence that the third parties they dealt with had robust procedures for dealing with data security issues. A number of the firms sharing data relied on the fact that the third party was a regulated entity rather than having a separate service level agreement to ensure robust procedures.

72. We observed a number of firms who allowed third parties unaccompanied or unsupervised access to their premises. Very few of these firms verified with their suppliers how their staff were vetted. This is a potential risk as a number of firms did not have adequate data storage procedures or had lax 'clear desk' controls.

Only 21% of firms (33 firms) felt confident that the third parties they dealt with had any real understanding of data security issues.

73. A third of firms visited had outsourced all or some aspects of their IT administration function to a third party, including the granting and review of access rights. It is important that firms understand that, if they use third parties, they are still responsible for the security of that data and for ensuring that it is kept securely.

Questions to ask yourself

- How well do you know your third party suppliers or service providers?
- Have you carried out any due diligence on third parties, including their security arrangements and staff recruitment policies?
- Do you allow third parties unsupervised access to your office or records?
- Do you maintain a clear desk policy to reduce the risk of customer data being lost, stolen or becoming accessible to unauthorised persons?

3.2.4 Physical controls

Aim of review

To assess the general physical security of firms' business premises and the controls that firms had around the appropriate use of laptops, desktop PCs, portable media devices, and the backup of customer data.

The review focused on:

- encryption of laptops and portable media devices;
- copying or downloading of customer data;
- physical security of premises; and
- backup of customer data.

74. A quarter of firms that used laptops and or portable devices had some level of encryption, although in many firms laptops were not regularly used to hold customer data.

75. Nearly half of the firms visited had no formalised system for restricting staff from copying customer data to portable devices. Most firms did not block or restrict the ability to plug in portable devices to computers which increased the risk that confidential data could be lost.

Of the 159 firms visited 34 (21%) had encrypted laptops and or portable devices; although in many firms laptops were not regularly used to hold customer data.

76. Around a fifth of firms had processes for internally monitoring unauthorised access to customer data. In several cases where there were no such processes, this was because the business was small enough for management to be able to physically 'oversee' the business.

77. Most firms regularly backed up customer data. However, in a number of firms 'secure backup' was viewed primarily as physically securing the backup tapes, discs, or portable hard drives in either on- or off-site storage rather than by encrypting the tapes or discs themselves.

78. The majority of firms visited had adequate physical security. However, firms often looked on physical security as a means of protecting physical assets (e.g. laptops, phones), rather than by securing customer data.

Questions to ask yourself

- Do you allow staff to work remotely or take customer data outside the office on laptops, or other portable devices? If so, are the data files or the devices themselves encrypted?
- Do you monitor the content of laptops or portable devices?
- Would you know if laptops or portable devices were to go missing?
- Are you satisfied with the consistency and security of the backup of your data?
- Have you identified any vulnerability in the security of or access to your premises?

3.2.5 Disposal of data

Aim of review

To assess whether firms were considering and utilising secure methods of disposal for customer data held in both paper and electronic format.

The review focused on:

- processes around disposal of paper data; and
- processes around disposal of electronic data.

79. Over three quarters of firms visited had specific procedures or internal requirements to securely dispose of confidential paper.

136 firms (85%) had shredding facilities on-site to handle the destruction of paper customer data, and a small number also used a reputable company to remove the shredded data at regular intervals, or to carry out bulk shredding, either on-site or at third party premises.

80. Most firms had in-house shredding facilities to destroy paper customer data. A number of firms with large amounts of confidential data also used accredited data disposal firms to remove the shredded data at regular intervals, or to carry out bulk shredding, either on-site or at third party premises.

81. Nearly half of firms visited had adequate arrangements for disposing of electronic equipment containing customer data. However many of the remaining firms had not addressed this issue or formalised an approach as they had not yet had cause to destroy computer records or the hardware used to facilitate storage.

Questions to ask yourself

- Do you shred your customer data in house and if so, are staff aware of the requirements?
- If you use a third party for disposal of data, are you satisfied with their security and staff vetting arrangements?
- If you have ever disposed of a computer, did you wipe the hard drive with specialist software or remove and destroy the hard drive?

3.2.6 Data compromise incidents

Aim of review

To assess whether firms had experienced any data compromise incidents within their business, the level of seniority or experience of staff handling data incidents and whether they had handled, reported and resolved these in an appropriate fashion.

The review focused on:

- processes for data compromise incident handling; and
- compliance role in data security.

82. One third of firms had procedures for handling a data security incident and nearly three quarters of all firms visited had designated an individual within the firm to handle data security incidents if they arose. Given the size of a number of the firms this was often someone in a senior or management position.

113 firms (71%) had designated an individual within the firm (invariably someone in a senior position) to handle data security incidents if they arose. However, given that only 49 of these firms (43%) had a procedure for handling data security incidents, it is unclear as to how staff would be aware of how to report an incident and indeed to whom to report it.

83. Very few firms had experienced or recorded a data security incident. However, given that two thirds of firms visited had no formal procedures in place to deal with such incidents it was unclear how staff would be aware of and recognise an incident, and indeed to whom they should report such incidents.

84. In over half of the firms visited the Compliance Officer played a role in controlling data security. In many small firms the Compliance Officer often had a number of responsibilities, including being responsible for their firm's data security controls.

Questions to ask yourself

- Do you have a designated individual responsible for data security incidents?
- Would your staff recognise a data security incident and how to report it?

3.3 Fraud

The findings in this section apply to **all firms**.

3.3.1 General fraud

Aim of review

To assess the extent of firms' fraud risk awareness and understand what processes are in place to mitigate fraud risk.

The review focused on:

- fraud assessment and identification;
- escalation and investigation; and
- training and prevention.

85. Most firms had appointed a senior manager(s) to take responsibility for fraud investigations.

86. A minority of firms had a defined escalation process in place should fraudulent activity be identified in the business. The majority of those firms which did not have a formalised process felt staff would be aware of who to contact should the need arise.

28 firms had a formalised escalation process in place for staff that had identified fraudulent activity.

87. Few firms provided specific fraud training to staff. Often fraud issues were included in broader financial crime or induction training that staff received. Where fraud updates were provided, these were done primarily through reading FSA publications, press articles or via compliance consultants' updates.

Questions to ask yourself

- What are the main fraud risks in your business?
- Have you considered fraud risks arising from products, distribution channels, staff and services to customers?
- How do you measure fraud loss?
- Is fraud loss measured consistently across the business and not hidden within other costs such as bad debts and insurance claims?

3.3.2 Insurance fraud

Aim of review

To assess the extent to which firms carrying out insurance activities had assessed fraud risks in their businesses and implemented mitigating processes.

The review focused on:

- risk identification; and
- relationships with loss adjustors.

88. Over half of the firms visited had informally assessed how their business could be used to commit insurance fraud. Those that had conducted a risk assessment were aware of insurance fraud risk indicators specific to their business.

One firm had reported two instances of fraudulent claims to the police, one of which led to a successful prosecution. Seven other firms had experienced fraudulent activity which had been dealt with internally and not reported to the police.

89. Where loss adjusters were used, fewer than half the relevant firms visited had verified their work in order to guard against collusion in a fraudulent claim.

Questions to ask yourself

- Which insurance products pose the greatest risk to your business?
- How do you monitor early surrenders?

3.3.3 Investment fraud

Aim of review

To assess the extent to which firms carrying out investment activities had assessed fraud risks in their businesses and implemented mitigating processes

The review focused on:

- new product risk assessment; and
- complaints handling.

90. A minority of firms visited conducted a risk assessment on new investment products offered through their business.

> *Of the 87 firms who conducted investment business, 35 firms (40%) had identified or defined higher risk customers or countries. However, most of these firms did not then apply any enhanced due diligence in respect of these customers.*

91. All firms visited had a formalised complaints policy in place. One boiler room fraud incident had been reported. This related to a cold call received by a firm's customer rather than the activities of one of the firms visited.

Questions to ask yourself

- Which investment products pose the greatest risk to your business?
- How do you monitor your high risk products and customers and are there robust processes in place to approve undertaking higher risk business?

3.3.4 Mortgage fraud

Aim of review

To identify how firms conducting mortgage business assess the risk that their business could be used to facilitate mortgage fraud.

The review focused on:

- how firms assessed suspicious applications;
- KYC and Customer Due Diligence(CDD) documentation (use of introducer, documentation obtained);
- dealing with higher risk customers and products; and
- broker/lender responsibilities.

92. The level of customer due diligence (KYC) checks undertaken during the customer take-on process varied across the sector. The majority of firms obtained two forms of identification – normally a passport/driving licence and utility bill.

93. Most firms were aware of potential suspicious indicators when conducting mortgage business. Indicators included:

    a. difficulties verifying identity;

    b. self certification mortgages when the individual holds a PAYE job;

    c. fast track mortgages with a high loan to value ratio;

    d. multiple applications; and

    e. difficulties in obtaining source of funds/source of wealth/income verification information.

94. Most small firms that conducted mortgage business obtained proof of income and a number also obtained source of wealth information (mainly through bank statements). This was predominantly obtained via the fact find process rather than as part of an integrated AML/fraud process.

95. The majority of firms conducted home visits during customer take-on. Where introducers were used, most firms verified the customer checks undertaken by the introducer or conducted their own customer due diligence.

Levels of KYC checks undertaken at customer take-on varied considerably.

- Of the 46 firms who conducted mortgage business:
  - 19 firms (or 41%) obtained 2 forms of evidence;
  - 19 firms (or 41%) also obtained income verification;
  - 5 firms (or 11%) also obtained source of funds/source of wealth evidence; and
  - 3 firms (or 7%) indicated they only obtained KYC when specifically requested by the lender.

96. Most firms indicated that when requested they would make KYC information available to lenders. However, firms also commented that lenders rarely, if ever, asked for such documentation.

97. Less than half the firms visited said that they would find out why a mortgage application had been declined. Firms also stated that lenders were reluctant to disclose or share such information.

Questions to ask yourself

- Do you have policies and procedures covering the whole of the mortgage application process?
- What formal relationships do you and the mortgage lender(s) have with valuers and solicitors?
- What oversight monitoring do you do?
- Do you collect enough information on your customers?

3.3.5 Staff/Internal fraud

Aim of review

To identify how firms assess the fraud risk posed by their employees and the mitigating controls in place.

The review focused on:

- pre-recruitment vetting;
- segregation of duties;
- termination of employment; and
- internal accounting controls (including controls over external payments, company cheques).

98. Less than half the firms visited carried out full background checks or referencing before appointing staff. The majority of these firms indicated that their employees were family or close friends or had been referred by a known and trusted associate.

99. There were varying levels of pre-vetting checks; from those firms which undertook little or no staff vetting through to personal references, obtaining full employment history, credit checks, Companies House and Criminal Records Bureau (CRB) checks. Where background checks were undertaken, qualifications and references were generally authenticated.

100. Few firms segregated staff duties with many highlighting that they employed too few staff who have broad responsibilities for this to be practical. Where segregation had been implemented, solutions to reduce the risk of financial crime included role specific IT access, dual signatories and separation of front and back office functions.

Of the 144 firms with more than one employee:

> *72 (or 50%) firms felt there were too few staff (or were sole traders) with a range of responsibilities to segregate access to systems. Where this wasn't the case, 50 (or 32%) firms had implemented system segregation.*

101. Most firms had implemented internal accounting controls. Examples of these controls included quarterly accounts audits/reconciliations, dual signatories to authorise external payments, assigning authorisation limits to individuals, compliance consultant reviews and external audit reviews. The majority of those firms that did not implement internal controls were sole traders where the risks of fraud could be assessed as low.

102. Most firms visited had controls over the use of petty cash and company cheque books. However, few firms had extended controls to monitor or reconcile company credit card usage.

Questions to ask yourself

- Do you have tailored fraud awareness training in place for your staff?
- Are your employees monitored for their performance against fraud management indicators and is it monitored and action taken where it falls below accepted standards?
- Are you producing newsletters or other alerts to inform staff about fraud risks and trends?
- Are new recruits in high-risk positions (e.g. finance department) subject to enhanced vetting (e.g. criminal records checks)?

Annexes

Annex 1: Glossary

Term	Meaning
Asset freezing	See 'financial sanctions regime'.
Beneficial owner	The person who ultimately owns or controls the customer. The Money Laundering Regulations 2007 provides a definition of a beneficial owner for each of the following types of customer: bodies corporate; partnerships; trusts; entities or arrangements that administer and distribute funds; and estates of deceased persons. An entity may have more than one beneficial owner. More information can be found at: http://www.opsi.gov.uk/si/si2007/uksi_20072157_en_3#pt2-l1g6
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. http://www.moneymadeclear.fsa.gov.uk/news/scams/share_scams.html
Consent	If a firm is concerned that it may be assisting in the laundering of funds it can file a Suspicious Activity Report and apply to the Serious Organised Crime Agency (SOCA) for consent to continue the transaction. The Proceeds of Crime Act gives SOCA seven working days to respond, although it often responds more quickly. 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. For more, see: http://www.soca.gov.uk/financialIntel/disclosure.html
Corruption	A situation where private persons or public officials abuse their position by, for example, paying or accepting bribes from a firm or by embezzling funds, to make personal gain. Corruption is an offence under UK law.
Customer due diligence	Customer due diligence measures are taken by firms to a) identify their customers and b) verify the customer's identity by using documents (e.g. photo ID such as a passport or driving licence) or reliable independent sources (such as the electoral roll). It also includes obtaining information about why the customer is making use of the firm's services. See Regulation 7 of the Money Laundering Regulations.
Enhanced due diligence	The Money Laundering Regulations 2007 require firms to undertake enhanced customer due diligence and ongoing monitoring in higher risk situations (see Box 7).
EU Money Laundering Directive	The Third EU Money Laundering Directive, adopted in 2005 (2005/60/EC), updated European Community legislation in line with the revised international standards set by FATF Recommendations. The UK has implemented this Directive through the Money Laundering Regulations 2007.

Term	Meaning
FATF	See 'Financial Action Task Force'.
Financial Action Task Force	An intergovernmental body that develops and promotes anti-money laundering and counter terrorist financing standards. There are 34 member jurisdictions including the UK, some other EU countries and the USA. Further information is available at http://www.fatf-gafi.org.
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 HMT. The Asset Freezing Unit is responsible for ensuring compliance with the UK's financial sanctions regime; the FSA's role is to ensure firms have appropriate systems and controls to enable compliance.
Fraud	Fraud is the deliberate act of prejudicing the rights of another party knowing you have no right to do so. This general definition has been supplemented by the Fraud Act 2006 which created three basic offences of fraud: 1) by false representation, 2) by failing to disclose information and 3) by abuse of position. An offence may be committed even if an individual does not gain personally but compromises the interests of another person.
Identification	The JMLSG's definition is: 'ascertaining the name of, and other relevant information about, a customer or beneficial owner'.
Know your customer (KYC)	This term is often used as a synonym for 'customer due diligence' checks. We would caution against its use in an AML context because the term can also refer to suitability checks related to the regulated sales of financial products. The Money Laundering Regulations explicitly refer to customer due diligence and not to KYC.
Market abuse	Umbrella term which covers the offences of insider dealing and market manipulation. Both offences can be prosecuted under criminal or civil legislation.

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. The JMLSG guidance states: 'Money laundering takes many forms, including: • trying to turn money raised through criminal activity into 'clean' money (that is, classic money laundering); • handling the benefit of acquisitive crimes such as theft, fraud and tax evasion; • handling stolen goods; • being directly involved with any criminal or terrorist property, or entering into arrangements to facilitate the laundering of criminal or terrorist property; and • criminals investing the proceeds of their crimes in the whole range of financial products.'
Money Laundering Regulations	The Money Laundering Regulations 2007 implements the requirements of the EU's Third Money Laundering Directive into UK law.
Money Laundering Reporting Officer (MLRO)	The MLRO is appointed by a firm and charged with receiving internal reports of suspicious activity and making SARs to the authorities. They have wider responsibilities to ensure that measures to combat money laundering within the firm are effective. The MLRO is a controlled function under the Approved Persons Regime. The MLRO will usually be the 'nominated officer' (see definition below). Note that not all firms authorised by the FSA need to maintain an MLRO: mortgage brokers, general insurers and general insurance intermediaries are not required to appoint an MLRO, but may choose to appoint a nominated officer (see below) for administrative convenience.
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.
Ongoing monitoring	The Money Laundering Regulations require ongoing monitoring of business relationships. This means that the transactions performed by a customer, and other aspects of their behaviour, are scrutinised throughout the course of their relationship with the firm. The intention is to spot where a customer's actions are inconsistent with what might be expected of a customer of that type, given what is known about their business, risk profile, etc. Firms should also seek to update the information they hold on customers for anti-money laundering purposes.

Term	Meaning
PEP	See Politically Exposed Person
Politically exposed person	A person entrusted with a prominent public function and who is potentially able to abuse that position for personal gain. This may include senior government officials such as MPs and heads of state, senior military officers and other equivalent officials like central bank governors. It also includes their immediate family members and known close associates. A formal definition is set out in Regulation 14 (5) the Money Laundering Regulations. It is entirely acceptable for a financial firm to have a PEP as a customer, but this relationship must be subject to greater scrutiny. (See also Regulation 14 (4) of the Money Laundering Regulations).
Reliance	The Money Laundering Regulations allow a firm to rely on customer due diligence checks performed by others. However, there are many limitations on how this can be done. First, the relying firm nonetheless remains liable for any failure to apply these checks. Second, the firm being relied upon must give their 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. In practice, common situations where reliance is applied include investment funds relying on checks performed by the financial advisor or banks that take part in a syndicated loan relying on checks performed by one of the institutions.
Sanctions	See 'financial sanctions regime'.
SOCA	The Serious Organised Crime Agency, the UK's financial intelligence unit (FIU).
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	1. In the UK, the term 'Suspicious Transaction Report' (STR) refers to market abuse reporting. An STR must be submitted to the FSA where a firm has reasonable grounds to believe that a transaction constitutes market abuse. For further information on when a firm should submit and STR, please see this document: http://connectplus/tools/ARROW/documents/MarketAbuseGuidanceUpdate20090209.pdf 2. 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.

Term	Meaning
Terrorism Act	The Terrorism Act 2000 as amended.
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.
Tipping off	1. See POCA, section 333A. The offence of tipping off is committed where a person discloses that: (i) a 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 (ii) an investigation into allegations that an offence of money laundering has been committed is being contemplated or carried out. A similar offence exists in relation to terrorism (including terrorism financing) by virtue of section 21D of the Terrorism Act 2000. Note that the tipping off offence above applies slightly differently in relation to FSA personnel acting in the course of their duties. For further information please contact your usual GCD Legal Adviser. 2. As well as prohibiting market abuse, the Criminal Justice Act outlaws tipping off, where inside information is disseminated to a third party. Tipping off is punishable regardless of whether the information received is actually traded on or not.
Verification	Making sure the customer is who they say they are. The JMLSG defines this as: 'verifying the identity of a customer, by reference to reliable, independent source documents, data or information, or of a beneficial owner through carrying out risk-based and adequate measures'.

Annex 2: Good and poor practices

AML	
Examples of good practice	**Examples of poor practice**
Regulatory/Legal obligations	
• 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.	• 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.

AML	
Examples of good practice	**Examples of poor practice**
Account opening procedures	
• 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 advisor at home and in these cases the advisors would usually ask for identity verification documents on the second meeting with the customer. Where business was conducted remotely, more (three or four) identity verification documents were required and the source of funds exemption was not used.	• An IFA commented that they only dealt with investment customers that were well known to the firm or regulated entities. However, the firm had some high risk customers who were subject to very basic due diligence (eg: 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 sanctions requirements both HMT 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.

AML	
Examples of good practice	**Examples of poor practice**
Monitoring activity	
• 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.	

AML	
Examples of good practice	**Examples of poor practice**
Suspicious activity reporting	
	• 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 proforma 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.
Records	
• An advising only intermediary firm used a web-based system as its database of leads, contact names and addresses. It also stored telephone and meeting notes there which were accessed by staff using individual passwords.	• A file review at an IFA revealed disorganised files and missing KYC documentation in 3 of 5 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.

AML	
Examples of good practice	**Examples of poor practice**
Records (continued)	
• 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.	
Training	
• A GI Intermediary used an on-line training website (costing around £100 per employee per year). The firm believed that the training was good quality and included separate modules on financial crime which were compulsory for staff to complete. Staff were also required to complete refresher training. An audit of all training completed was stored on-line. • An IFA (sole trader) carried out on-line training on various financial crime topics. He also participated in conference call training where a trainer talked trainees through various topics while on-line, this was both time and travel efficient.	• 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.

Data security	
Examples of good practice	**Examples of poor practice**
Responsibilities and risk assessments	
• 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 the use of portable media devices, the secure disposal of data, and the logging of customer files removed and returned to the office. • An IFA had produced a written data security review of its business which had been prompted by their external consultants and largely followed the small firms' factsheet material on data security, provided by the FSA in April 2008. • In a personal pension operator, there was a full and comprehensive anti-fraud strategy in place and a full risk assessment had been carried 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.	• 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 firms 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.

Data security	
Examples of good practice	**Examples of poor practice**
Access to systems	
• AIn 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.	• 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.
Outsourcing	
• A discretionary investment manager used an external firm for IT support and had conducted its own on-site review of the IT firm's security arrangements. The same firm also insisted on CRB checks for cleaners.	• An authorised professional firm employed the services of third party cleaners, security staff, and an offsite confidential waste company, but had carried out no due diligence on any of these parties.

Data security	
Examples of good practice	**Examples of poor practice**
Outsourcing (continued)	
• An IFA had received a request from an introducer to provide names of customers who had bought a certain financial product. The firm refused to provide the data as it considered the request unnecessary and wanted to protect its customer data. It also referred the matter to the Information Commissioner who supported the firm's actions. • A general insurance intermediary employed office cleaners supplied by an agency that conducts due diligence including CRB checks. Office door codes were regularly changed and always if there was a change in staff.	• IAn IFA allowed a third party IT consultant full access rights to its customer data bank. Although the firm had a service agreement in place which 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.
Physical controls	
• 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.	• 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.

Data security	
Examples of good practice	**Examples of poor practice**
Outsourcing (continued)	
• 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.	• 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.
Data disposal	
• 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.	• IIn an IFA there was a clear desk policy that was not enforced and customer data was stored in cabinets which are unlocked and which were situated in a part of the office accessible to all visitors to the firm.

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

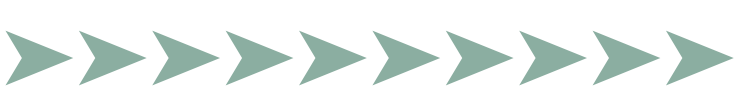
Fraud	
Examples of good practice	**Examples of poor practice**
General fraud	
• A small product provider had assessed the fraud risk presented by each product and developed appropriate controls to mitigate this risk based on the assessment. This assessment was then set out in the firm's Compliance Manual 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. • 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 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.

Fraud	
Examples of good practice	**Examples of poor practice**
General fraud	
• 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.	
Insurance fraud	
• 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.	• 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.

Fraud	
Examples of good practice	**Examples of poor practice**
Investment fraud	
• An IFA had undertaken a risk assessment for all high net worth customers. • A discretionary investment manager referred higher risk decisions (in respect of a high risk customer/value of funds involved) to a specific senior manager. • A personal pension operator carried out a financial crime risk assessment for newly introduced investment products.	• An IFA had a 'one size fits all' approach to identifying the risks associated with customers and investments.
Mortgage fraud	
• The majority of firms conducted customer fact finds. This allowed them to know their customers sufficiently to identify any suspicious behaviour. CDD (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 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.

Fraud	
Examples of good practice	**Examples of poor practice**
Mortgage fraud (continued)	
• An IFA had informally assessed the mortgage fraud risks the business faced and was aware of potentially suspicious indicators. The IFA also looked at how 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 long standing customers.	
Staff/Internal fraud	
• 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.	• 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

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: http://www.fsa.gov.uk



FSA®
Financial Services Authority