JMLSG

The Joint Money Laundering Steering Group

Prevention of money laundering/ combating the financing of terrorism

GUIDANCE FOR THE UK FINANCIAL SECTOR

PART I

January 2006

Contents

Chapter 5 Customer due diligence

PREFACE

1. In the UK, there has been a long-standing obligation to have effective procedures in place to detect and prevent money laundering. The UK Money Laundering Regulations, applying to financial institutions, date from 1993. The offence of money laundering was contained in various acts of parliament (such as the Criminal Justice Act 1988 and the Drug Trafficking Offences Act 1986). The Proceeds of Crime Act 2002 (POCA) consolidated, updated and reformed the law relating to money laundering to include any dealing in criminal property. Specific obligations to combat terrorist financing were set out in the Terrorism Act 2000. Many of the procedures which will be appropriate to address these obligations are similar, and firms can often employ the same systems and controls to meet them.

Purpose of the guidance

2. The purpose of this guidance is to:

    - outline the legal and regulatory framework for AML/CFT requirements and systems across the financial services sector;
    - interpret the requirements of the relevant law and regulations, and how they may be implemented in practice;
    - indicate good industry practice in AML/CFT procedures through a proportionate, risk-based approach; and
    - assist firms to design and implement the systems and controls necessary to mitigate the risks of the firm being used in connection with money laundering and the financing of terrorism.

Scope of the guidance

3. This guidance sets out what is expected of firms and their staff in relation to the prevention of money laundering and terrorist financing, but allows them some discretion as to how they apply the requirements of the UK AML/CFT regime in the particular circumstances of the firm, and its products, services, transactions and customers.

4. This guidance relates solely to how firms should fulfil their obligations under the AML/CFT law and regulations. It is important that customers understand that production of the required evidence of identity does not automatically qualify them for access to the product or service they may be seeking; firms bring to bear other, commercial considerations in deciding whether particular customers should be taken on.

What is the offence of money laundering?

5. 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.

6. The techniques used by money launderers constantly evolve to match the source and amount of funds to be laundered, and the legislative/regulatory/law enforcement environment of the market in which the money launderer wishes to operate. For more information on the ways in which particular financial services businesses, products, relationships and technologies may be used by money launderers and terrorist financiers, along with some case study examples, see the JMLSG website www.jmlsg.org.uk.

7. There are three broad groups of offences related to money laundering that firms need to avoid committing. These are:

    - knowingly assisting (in a number of specified ways) in concealing, or entering into arrangements for the acquisition, use, and/or possession of, criminal property;
    - failing to report knowledge, suspicion, or where there are reasonable grounds for knowing or suspecting, that another person is engaged in money laundering; and
    - tipping off, or prejudicing an investigation.

8. It is also a separate offence under the ML Regulations not to have systems and procedures in place to combat money laundering (regardless of whether or not money laundering actually takes place).

The guidance also covers terrorist financing

9. There can be considerable similarities between the movement of terrorist property and the laundering of criminal property: some terrorist groups are known to have well established links with organised criminal activity. However, there are two major differences between terrorist property and criminal property more generally:

    - often only small amounts are required to commit individual terrorist acts, thus increasing the difficulty of tracking the terrorist property;
    - terrorists can be funded from legitimately obtained income, including charitable donations, and it is extremely difficult to identify the stage at which legitimate funds become terrorist property.

10. Terrorist organisations can, however, require quite significant funding and property to resource their infrastructure. They often control property and funds from a variety of sources and employ modern techniques to manage these funds, and to move them between jurisdictions.

11. In combating terrorist financing, the obligation on firms is to report any suspicious activity to the authorities. This supports the aims of the law enforcement agencies in relation to the financing of terrorism, by allowing the freezing of property where there are reasonable grounds for suspecting that such property could be used to finance terrorist activity, and depriving terrorists of this property as and when links are established between the property and terrorists or terrorist activity.

What about other financial crime?

12. Money laundering and terrorist financing risks are closely related to the risks of other financial crime, such as fraud. Fraud and market abuse, as separate offences, are not dealt with in this guidance. The guidance does, however, apply to dealing with any proceeds of crime that arise from these activities. Guidance on fraud-related matters can be found in the Fraud Manager's Reference Guide, published by the British Bankers' Association (copies available at www.bba.org.uk), and Identity Fraud – The UK Manual, published jointly by the Association of Payment and Clearing Services, CIFAS – the UK's Fraud Prevention Service, and the Finance & Leasing Association (copies available at any of www.apacs.org.uk, www.cifas.org.uk, or www.fla.org.uk). An online version of this manual is available at www.idpreventiontraining.com.

13. Firms increasingly look at fraud and money laundering as part of an overall strategy to tackle financial crime, and there are many similarities – as well as differences - between procedures to tackle the two. When considering money laundering and terrorist financing issues, firms should consider their procedures against fraud and market abuse and how these might reinforce each other. Where responsibilities are given to different departments, there will need to be strong links between those in the firm responsible for managing and reporting on these various areas of risk. When measures involving the public are taken specifically as an anti-fraud measure, the distinction should be made clear.

Who is the guidance addressed to?

14. The guidance, prepared by JMLSG, is addressed to firms in the industry sectors represented by its member bodies (listed at paragraph 31 below), and to those firms regulated by the FSA. All such firms – which, for the avoidance of doubt, include those which are members of JMLSG trade associations but not regulated by the FSA, and those regulated by the FSA which are not members of JMLSG trade associations - should have regard to the contents of the guidance.

15. Financial services firms which are neither members of JMLSG trade associations nor regulated by the FSA are encouraged to have regard to this guidance as industry good practice. Firms which are outside the financial sector, but subject to the ML Regulations, particularly where no specific guidance is issued to them by a body representing their industry, may also find this guidance helpful.

16. The guidance will be of direct relevance to senior management, nominated officers and MLROs in the financial services industry. The purpose is to give guidance to those who set the firm's risk management policies and its procedures for preventing money laundering and terrorist financing. Although the guidance will be relevant to operational areas, it is expected that these areas will be guided by the firm's own, often more detailed and more specific, internal arrangements, tailored by senior management, nominated officers and MLROs to reflect the risk profile of the firm.

How should the guidance be used?

17. The guidance gives firms a degree of discretion in how they comply with AML/CFT legislation and regulation, and on the procedures that they put in place for this purpose.

18. It is not intended that the guidance be applied unthinkingly, as a checklist of steps to take. Firms should encourage their staff to 'think risk' as they carry out their duties within the legal and regulatory framework governing AML/CFT. The FSA has made clear its expectation that FSA-regulated firms address their management of risk in a thoughtful and considered way, and establish and maintain systems and procedures that are appropriate, and proportionate to the risks identified. This guidance assists firms to do this.

19. When provisions of the statutory requirements and of FSA's regulatory requirements are directly described in the text of the guidance, it uses the term **must**, indicating that these provisions are mandatory. In other cases, the guidance uses the term **should** to indicate ways in which the statutory and regulatory requirements may be satisfied, but allowing for alternative means of meeting the requirements. References to 'must' and 'should' in the text should therefore be construed accordingly.

20. Many defined terms and abbreviations are used in the guidance; these are highlighted, and their meanings are explained in the Glossary.

What's new in this guidance?

21. This guidance departs radically from that which JMLSG has issued in the past. It emphasises the responsibility of senior management to manage the firm's money laundering and terrorist financing risks, and how this should be carried out on a risk-based approach. It introduces a standard approach to the identification and verification of customers, separating out basic identity from other aspects of knowing the customer, as well as giving guidance on the need to monitor customer activity.

22. The guidance deals separately with different sectors in the financial services industry, and gives more detailed guidance on how the risks in these sectors should be addressed.

23. For the first time, the guidance incorporates a range of reference material which it is hoped that senior management, nominated officers and MLROs will find helpful in appreciating the overall context of, and obligations within, the UK AML/CFT framework.

The content of the guidance

24. The guidance provided by the JMLSG is in two parts. The main text in Part I contains generic guidance that applies across the UK financial sector. Part II provides guidance for a number of specific industry sectors, supplementing the generic guidance contained in Part I.

25. Part I comprises nine separate chapters, followed by a Glossary of terms and abbreviations, and a number of appendices setting out other generally applicable material. Some of the individual chapters are followed by annexes specific to the material covered in that chapter.

26. Part I sets out industry guidance on:

- the importance of senior management taking responsibility for effectively managing the money laundering and terrorist financing risks faced by the firm's businesses (Chapter 1);
- appropriate controls in the context of financial crime (Chapter 2);
- the role and responsibilities of the nominated officer and the MLRO (Chapter 3);
- adopting a risk-based approach to identifying customers, collecting sufficient 'know your customer' information, and monitoring (Chapter 4);
- helping a firm have confidence that it knows its customers (Chapter 5);
- monitoring customer transactions and activity (Chapter 6);
- the identification and reporting of suspicious activity (Chapter 7);
- staff awareness, training and alertness (Chapter 8);
- record keeping (Chapter 9).

27. Part II of the guidance comprises the sector specific additional material, which has been principally prepared by practitioners in the relevant sectors. The sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the guidance.

Status of the guidance

28. POCA requires a court to take account of industry guidance that has been approved by a Treasury minister when considering whether a person within the regulated sector has committed the offence of failing to report where that person knows, suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering. Similarly, the Terrorism Act requires a court to take account of such approved industry guidance when considering whether a person within the financial sector has failed to report under that Act. The ML Regulations also provide that a court must take account of similar industry guidance in determining whether a

person or institution within the regulated sector has complied with any of the requirements of the ML Regulations.

29. When considering whether to take disciplinary action against an FSA-regulated firm in respect of a breach of the relevant provisions of SYSC, the FSA will have regard to whether a firm has followed relevant provisions in this guidance. When considering whether to bring a criminal prosecution in relation to a breach of the ML Regulations, the FSA may also have regard to whether the person concerned has followed this guidance. The guidance will therefore be significant for individuals being prosecuted, or subject to regulatory action, in relation to their responsibility for firms' systems and controls and/or in relation to their personal actions: for example, why did they fail to disclose?

30. The guidance provides a sound basis for firms to meet their legislative and regulatory obligations when tailored by firms to their particular business risk profile. Departures from good industry practice, and the rationale for so doing, should be documented, and may have to be justified, for example to the FSA.

Who are the members of JMLSG?

31. The members of JMLSG are:

Association of British Insurers (ABI)

Association of Foreign Banks (AFB)

Association of Friendly Societies (AFS)

Association of Independent Financial Advisers (AIFA)

Association of Private Client Investment Managers and Stockbrokers (APCIMS)

British Bankers' Association (BBA)

British Venture Capital Association (BVCA)

Building Societies Association (BSA)

Council of Mortgage Lenders (CML)

Electronic Money Association (EMA)

Finance & Leasing Association (FLA)

Futures and Options Association (FOA)

Investment Management Association (IMA)

London Investment Banking Association (LIBA)

PEP & ISA Managers' Association (PIMA)

Wholesale Market Brokers' Association (WMBA)

CHAPTER 1

SENIOR MANAGEMENT RESPONSIBILITY

Key points in this chapter

- **International recommendations and authorities**
  - FATF
    - Forty Recommendations (June 2003, as amended October 2004)
    - Nine Special Recommendations on Terrorist Financing (revised October 2004)
  - UN Security Council Resolutions 1267 (1999), 1373 (2001) and 1390 (2002)
- **International regulatory pronouncements**
  - Basel CDD paper
  - IAIS Guidance Paper 5
  - IOSCO Principles paper
  - Basel Consolidated KYC Risk Management
- **EU Directives**
  - First Money Laundering Directive 91/308/EEC
  - Second Money Laundering Directive 2001/97/EC
- **EU Regulations**
  - EC Regulation 2580/2001
- **UK framework**
  - Legislation
    - FSMA 2000
    - Proceeds of Crime Act 2002 (as amended)
    - Terrorism Act 2000 (as amended by the Anti-terrorism, Crime and Security Act 2001)
    - Money Laundering Regulations 2003
  - Financial Sanctions
    - Bank of England Sanctions Notices and News Releases
  - Regulatory regime
    - FSA Handbook –APER, COND, ENF, PRIN, and SYSC
  - Industry guidance
- **Other matters**
  - USA PATRIOT Act – extra-territoriality
  - Wolfsberg Principles
    - Private Banking
    - Suppression of the Financing of Terrorism
    - Correspondent Banking
    - Monitoring, Screening and Searching (appropriate monitoring of transactions and customers)
- **Core obligations**
  - Senior management in all firms must
    - identify, and manage effectively, the risks in their businesses
    - if in the regulated sector, appoint a nominated officer to process disclosures
  - Senior management in FSA-regulated firms must appoint an MLRO with certain responsibilities
  - Adequate resources must be devoted to AML/CFT
  - Potential personal liability if legal obligations not met
- **Actions required, to be kept under regular review**
  - Prepare a formal policy statement in relation to money laundering/terrorist financing prevention
  - Ensure adequate resources devoted to AML/CFT
  - Commission annual report from the MLRO and take any necessary action to remedy deficiencies identified by the report in a timely manner

Introduction

SYSC 3.1.1 R, 3.2.6 R 3.2.6A R

1.1 Being used for money laundering or terrorist financing involves firms in reputational, legal and regulatory risks. Senior management has a responsibility to ensure that the firm's control processes and procedures are appropriately designed and implemented, and are effectively operated to reduce the risk of the firm being used in connection with money laundering or terrorist financing.

1.2 Senior management in financial firms is accustomed to applying proportionate, risk-based policies across different aspects of its business. A firm should therefore be able to take such an approach to the risk of being used for the purposes of money laundering or terrorist financing. Such an approach would change the emphasis and mindset towards money laundering and terrorist financing without reducing the effectiveness with which the risks are managed.

1.3 Under a risk-based approach, firms start from the premise that most customers are not money launderers or terrorist financiers. However, firms should have systems in place to highlight those customers who, on criteria established by the firm, may indicate that they present a higher risk of this. The systems and procedures should be proportionate to the risks involved, and should be cost effective.

1.4 Senior management must be fully engaged in the decision making processes, and must take ownership of the risk-based approach, since they will be held accountable if the approach is inadequate. That said, provided the assessment of the risks and the selection of mitigation procedures have been approached in a considered way, all the relevant decisions are properly recorded, and the firm's procedures are followed, the risk of censure should be very small.

International pressure to have risk-based AML/CFT procedures

1.5 Governments in many countries have enacted legislation to make money laundering and terrorist financing criminal offences, and have legal and regulatory processes in place to enable those engaged in these activities to be identified and prosecuted.

1.6 FATF have issued Forty Recommendations aimed at setting minimum standards for action in different countries, to ensure that AML efforts are consistent internationally. FATF have also issued Nine Special Recommendations on Terrorist Financing, with the same broad objective as regards CFT. The text of these Recommendations is available at www.fatf-gafi.org.

1.7 Separate from the development of FATF's Recommendations, two EU Directives are targeted at money laundering prevention, and have

been implemented in the UK mainly through the Money Laundering Regulations 2003.

1.8 Internationally, the FATF Forty Recommendations, the Basel CDD paper, IAIS Guidance Paper 5 and the IOSCO Principles paper encourage national supervisors of financial firms to require firms in their jurisdictions to follow specific due diligence procedures in relation to customers. In addition, the Basel Committee has issued a paper on Consolidated KYC Risk Management. These organisations explicitly envisage a risk-based approach to AML/CFT being followed by firms.

1.9 The United Nations and the EU have sanctions in place to deny a range of named individuals and organisations, as well as nationals from certain countries, access to the financial services sector. In the UK, the Bank of England acts on behalf of the Treasury by issuing sanctions notices whenever a new name is added to the list, or when any details are amended.

1.10 The private sector Wolfsberg Group of banks has also published guidance in relation to Private Banking; Correspondent Banking; Suppression of the Financing of Terrorism; and Monitoring, Screening and Searching (collectively referred to as the Wolfsberg Principles).

The UK legal and regulatory framework

1.11 The UK approach to fighting money laundering and terrorist financing is based on a partnership between the public and private sectors. Objectives are specified in legislation and in the FSA Rules, but there is usually no prescription about how these objectives must be met. Often, the objective itself will be a requirement of an EU Directive, incorporated into UK law without any further elaboration, leaving UK financial businesses discretion in interpreting how it should be met.

1.12 Key elements of the UK AML/CFT framework are:

- Proceeds of Crime Act 2002 (as amended);
- Terrorism Act 2000 (as amended by the Anti-terrorism, Crime and Security Act 2001);
- Money Laundering Regulations 2003;
- Bank of England Sanctions Notices and News Releases; and
- FSA Handbook.

1.13 Implementation guidance for the financial services industry is provided by the JMLSG.

1.14 No single UK body has overall responsibility for combating money laundering or terrorist financing. Responsibilities are set out in Appendix I.

1.15 In the UK, the ML Regulations apply to all firms undertaking

relevant business. POCA and the Terrorism Act consolidated, updated and reformed the scope of UK AML/CFT legislation to apply it to any dealings in criminal or terrorist property. Thus, in considering their statutory obligations, firms need to think in terms of involvement with any crime or terrorist activity.

HMT Anti-money laundering strategy, 26 November 2004

1.16 Senior management should be aware of the Treasury's AML strategy document (available on the Treasury website www.hm-treasury.gov.uk/documents/financial_services/fin_index.cfm) which sets out why it is important to combat money laundering. The strategy document notes that if money laundering is not combated:

- there is a greater incentive for crime;
- detection and prosecution of crime is obstructed;
- integrity of the financial sector is at risk; and
- economic and competitive distortions are encouraged.

General legal and regulatory obligations

Regulation 3
POCA ss327-330
Terrorism Act ss18, 21A

1.17 Senior management of any enterprise is responsible for managing its business effectively. Certain obligations are placed on all firms subject to the ML Regulations, POCA and the Terrorism Act - fulfilling these responsibilities falls to senior management as a whole. These obligations are summarised in Annex 1-I.

FSMA s 6
SYSC

1.18 For FSA-regulated firms the specific responsibilities, and the FSA's expectations, of senior management are set out in FSMA and the FSA Handbook. These obligations are summarised in Annex 1-I.

Obligations on all firms

Regulation 3

1.19 The ML Regulations place a general obligation on firms within its scope to have appropriate systems and controls to forestall and prevent money laundering. Failure to comply with this obligation risks a prison term of up to two years and/or a fine.

Regulation 27

1.20 For any firm subject to the ML Regulations, any officer in a body corporate (ie a director, manager, secretary, chief executive, member of the committee of management, or a person purporting to act in such a capacity), or any partner in a partnership, who consents to or connives in the commission of offences under the ML Regulations, or where the commission of any such offence is attributable to any neglect on his part, will be individually liable for the offence.

POCA ss 327-330
Terrorism Act s 21A
Regulation 3(1)(c)

1.21 The offences of money laundering under POCA, and the obligation to report knowledge or suspicion of possible money laundering, affect members of staff of firms. The similar offences and obligations under the Terrorism Act also affect members of staff. However, firms have an obligation under the ML Regulations to take appropriate measures so that employees are made aware of the relevant provisions of the ML Regulations, POCA and the Terrorism Act, and are given training in how to recognise and deal with transactions which may be related to money laundering or terrorist

financing.

Obligations on FSA-regulated firms

FSMA, s 6 (2) (a)
FSMA, s 6 (2) (b)
SYSC 2.1.1 R,
2.1.3 R, 3.2.6 R

1.22 FSMA refers, in the context of setting the FSA's financial crime objective, to the desirability of senior management of FSA-regulated firms being aware of the risk of their businesses being used in connection with the commission of financial crime, and taking appropriate measures to prevent financial crime, facilitate its detection and monitor its incidence. Senior management has operational responsibility for ensuring that the firm has appropriate systems and controls in place to combat financial crime.

SYSC 3.2.6H R

1.23 In FSA-regulated firms (but see paragraph 1.31 for general insurance firms and mortgage intermediaries), a director or senior manager must be allocated overall responsibility for the establishment and maintenance of the firm's anti-money laundering systems and controls.

SYSC 3.2.6I(2) R

1.24 In FSA-regulated firms (but see paragraph 1.31 for general insurance firms and mortgage intermediaries), an individual must be allocated responsibility for oversight of a firm's compliance with the FSA's Rules on systems and controls against money laundering: this is the firm's MLRO. The FSA requires the MLRO to have a sufficient level of seniority within the firm to enable him to carry out his function effectively. In some firms the MLRO will be part of senior management (and may be the person referred to in paragraph 1.23); in firms where he is not, he will be directly responsible to someone who is. The relationship between the MLRO and (other) members of senior management is one of the keys to a successful AML/CFT regime.

SYSC 3.2.5H R
SYSC 3.2.6I R

1.25 Senior management of FSA-regulated firms must:

- appoint an appropriately qualified senior member of the firm's staff as the MLRO (see Chapter 3);
- provide direction to, and oversight of the firm's AML/CFT strategy; and
- allocate to a director or senior manager (who may or may not be the MLRO) overall responsibility for the establishment and maintenance of the firm's AML/CFT systems and controls.

SYSC 3.2.6G(2) G

1.26 At least once in each calendar year, an FSA-regulated firm must commission a report from its MLRO (see Chapter 3) on the operation and effectiveness of the firm's systems and controls to combat money laundering. In practice, senior management should determine the depth and frequency of information they feel is necessary to discharge their responsibilities. The MLRO may also wish to report to senior management more frequently than annually, as circumstances dictate.

1.27 When senior management receives reports from the firm's MLRO it should consider them and take any necessary action to remedy any deficiencies identified in a timely manner.

SYSC 3.2.6I(2) R
FSMA s 6 (2) (c)

1.28 Those FSA-regulated firms required to appoint an MLRO are specifically required to provide the MLRO with adequate resources. All firms, however, whether or not regulated by the FSA, should apply adequate resources to AML/CFT procedures, systems and controls. The level of resource should reflect the size, complexity and geographical spread of the firm's customer and product base.

1.29 The role, standing and competence of the MLRO, and the way the internal processes for reporting suspicions are designed and implemented, impact directly on the effectiveness of a firm's money laundering/terrorist financing prevention arrangements.

1.30 Firms should be aware of the FSA's findings in relation to individual firms, and its actions in response to these; this information is available on the FSA website at www.fsa.gov.uk/Pages/Library/Communication/index.shtml.

Exemptions from legal and regulatory obligations

SYSC 3.2.6 R

1.31 General insurance firms and mortgage intermediaries are regulated by the FSA, but are not covered by the ML Regulations, or the provisions of SYSC specifically relating to money laundering. They are, therefore, under no obligation to appoint an MLRO. They are, however, subject to the general requirements of SYSC, and so have an obligation to have appropriate risk management systems and controls in place, including controls to counter the risk that the firm may be used to further financial crime.

POCA ss 327-329, 335, 338
Terrorism Act s 21

1.32 These firms are also subject to the provisions of POCA and the Terrorism Act which establish the primary offences. These offences are not committed if a person's knowledge or suspicion is reported to NCIS, and appropriate consent for the transaction or activity obtained.

POCA s 332
Terrorism Act ss 19, 21

1.33 For administrative convenience, and to assist their staff fulfil their obligations under POCA or the Terrorism Act, general insurance firms and mortgage intermediaries may choose to appoint a nominated officer. Where they do so, he will be subject to the reporting obligations in s 332 of POCA and s 19 of the Terrorism Act (see Chapter 7).

Relationship between money laundering, terrorist financing and other financial crime

1.34 Although the ML Regulations focus on firms' obligations in relation to the prevention of money laundering, POCA updated and reformed the obligation to report to cover involvement with any criminal property, and the Terrorism Act extended this to cover terrorist property.

1.35 From a practical perspective, therefore, firms should consider how best they should assess and manage their overall exposure to financial crime. This does not mean that fraud, market abuse, money laundering and terrorism financing prevention must be addressed by

a single function within a firm; there will, however, need to be close liaison between those responsible for each activity.

1.36 Money laundering prevention is not simply a matter of taking customer ID, although typically this is the only aspect of which customers are fully aware, and has received considerable regulatory attention over the past few years. Knowing enough about the customer and his business are just as important as confirming his identity.

Senior management should adopt a formal policy in relation to financial crime prevention

SYSC 3.1.1 R, 3.2.6 R 3.2.6A R

1.37 As mentioned in paragraph 1.1 above, senior management in FSA-regulated firms has a responsibility to ensure that the firm's control processes and procedures are appropriately designed and implemented, and are effectively operated to manage the firm's risks. This includes the risk of the firm being used to further financial crime.

SYSC 3.2.6G G

1.38 For FSA-regulated firms (but see paragraph 1.31 for general insurance firms and mortgage intermediaries) SYSC 3.2.6G G says that a firm should produce "adequate documentation of [its] risk management policies and risk profile in relation to money laundering, including documentation of that firm's application of those policies". A statement of the firm's AML/CFT policy and the procedures to implement it will clarify how the firm's senior management intends to discharge its responsibility for the prevention of money laundering and terrorist financing. This will provide a framework of direction to the firm and its staff, and will identify named individuals and functions responsible for implementing particular aspects of the policy. The policy will also set out how senior management undertakes its assessment of the money laundering and terrorist financing risks the firm faces, and how these risks are to be managed. Even in a small firm, a summary of its high-level AML/CFT policy will focus the minds of staff on the need to be constantly aware of such risks, and how they are to be managed.

1.39 A policy statement should be tailored to the circumstances of the firm. Use of a generic document might reflect adversely on the level of consideration given by senior management to the firm's particular risk profile.

1.40 The policy statement might include, but not be limited to, such matters as:

- Guiding principles:
  - an unequivocal statement of the culture and values to be adopted and promulgated throughout the firm towards the prevention of financial crime;
  - a commitment to ensuring that customers' identities will be satisfactorily verified before the firm accepts them;

- a commitment to the firm 'knowing its customers' appropriately - both at acceptance and throughout the business relationship - through taking appropriate steps to verify the customer's identity and business, and his reasons for seeking the particular business relationship with the firm;
- a commitment to ensuring that staff are trained and made aware of the law and their obligations under it, and to establishing procedures to implement these requirements; and
- recognition of the importance of staff promptly reporting their suspicions internally.

- Risk mitigation approach:
  - a summary of the firm's approach to assessing and managing its money laundering and terrorist financing risk;
  - allocation of responsibilities to specific persons and functions;
  - a summary of the firm's procedures for carrying out appropriate identification and monitoring checks on the basis of their risk-based approach; and
  - a summary of the appropriate monitoring arrangements in place to ensure that the firm's policies and procedures are being carried out.

Application of group policies outside the UK

1.41 The UK legal and regulatory regime is primarily concerned with preventing money laundering which is connected with the UK. Where a UK financial institution has overseas branches, subsidiaries or associates, where control can be exercised over business carried on outside the United Kingdom, or where elements of its UK business have been outsourced to offshore locations (see paragraphs 2.6-2.10), the firm should consider putting in place a group AML/CFT strategy. It is, however, for the firm to decide how to address AML/CFT outside the UK, taking into account the various obligations which it has to meet in these countries.

1.42 A group policy may wish to ensure that all overseas branches and subsidiaries undertake identification and record-keeping procedures at least to the standards required under UK law or, if the standards in the host country are more rigorous, to those higher standards. Reporting processes must nevertheless follow local laws and procedures.

1.43 Whilst suspicions of money laundering or terrorist financing may be required to be reported within the jurisdiction where the suspicion arose and where the records of the related transactions are held, there may also be a requirement for a report to be made to NCIS (see paragraph 7.23).

USA PATRIOT Act – extra-territoriality

1.44 Where a firm has a US listing, or has activities in, or linked to, the USA, whether through a branch, subsidiary, associated company or correspondent banking relationship, there is a risk that the application of US AML/CFT and financial sanctions regimes may apply to the non-US activities of the firm. Senior management should take advice on the extent to which the firm's activities may be affected in this way.

ANNEX 1-I

UK AML/CFT LEGISLATION AND REGULATION

Proceeds of Crime Act 2002 (as amended)

2002, ch 29
SOCPA, s102

1. POCA consolidated, updated and reformed previous UK legislation relating to money laundering. The legislation covers all criminal property, with no exceptions, and there is no de minimis threshold, (although for deposit-taking firms, a transaction under £250 may be made without consent under certain circumstances – see paragraph 7.64). Moreover, with some exceptions, the crimes covered include acts committed elsewhere in the world that would be an offence if committed in the UK. POCA:

   - establishes a series of criminal offences in connection with money laundering, failing to report, tipping off and prejudicing an investigation;
   - sets out a series of penalties for the various offences established under POCA;
   - establishes the Assets Recovery Agency (ARA), with power to investigate whether a person holds criminal assets and, if so, their location;
   - creates five investigative powers for law enforcement.

2. The text of POCA is available at www.legislation.hmso.gov.uk. The key provisions of POCA, as they affect firms in the financial sector, are summarised in Appendix II.

Terrorism Act 2000 (as amended by the Anti-terrorism, Crime and Security Act 2001)

2000, ch 11
Terrorism Act, ss 15-18, 39

3. The Terrorism Act establishes offences related to involvement in facilitating, raising, possessing or using funds for terrorism purposes. The Act also empowers the authorities to make a number of Orders on financial institutions in connection with terrorist investigations. The Act also establishes offences in connection with failing to report, tipping off or prejudicing an investigation.

Terrorism Act, s3

4. The Terrorism Act also establishes a list of proscribed organisations, with which financial services firms may not deal. The primary source of information on proscribed organisations, including up-to-date information on aliases, is the Home Office. The list of proscribed organisations can be found at: www.homeoffice.gov.uk/security/terrorism-and-the-law/terrorism-act/proscribed-groups?version=1.

2001, ch 24

5. The Anti-terrorism, Crime and Security Act gives the authorities power

to direct firms in the regulated sector to provide the authorities with specified information on customers and their (terrorism-related) activities.

6. The texts of the Terrorism Act and the Anti-terrorism, Crime and Security Act are available at www.legislation.hmso.gov.uk. The key provisions of the Terrorism Act and the Anti-terrorism, Crime and Security Act, as they affect firms in the financial sector, are summarised in Appendix II.

Money Laundering Regulations 2003

SI 2003/3075

7. The ML Regulations specify arrangements which all firms undertaking relevant business (whether or not regulated by the FSA) must have in place to forestall and prevent money laundering.

8. The ML Regulations apply to all firms that undertake relevant business. They apply to many firms in the financial sector, including:

- firms carrying on relevant business, including:
  - banks, building societies and other credit institutions;
  - individuals and firms engaged in regulated activities under FSMA;
  - insurance companies undertaking long-term life business, including the life business of Lloyd's of London;
  - issuers of electronic money;
- money service businesses (bureaux de change, cheque encashment centres and money transmission services);
- the National Savings Bank (now National Savings & Investments);
- corporate service providers, company formation agents, trust formation companies and trust service providers or managers.

9. The ML Regulations require firms to appoint a nominated officer to receive internal reports relating to knowledge or suspicion of money laundering.

FSMA s 402(1)(b)

10. FSMA makes the FSA a prosecuting authority (other than in Scotland) in respect of offences under the ML Regulations committed by financial services firms.

11. The text of the ML Regulations is available at www.legislation.hmso.gov.uk. The key provisions of the ML Regulations are summarised in Appendix II.

Financial sanctions

12. The Bank of England maintains a Consolidated List of targets listed by the United Nations, European Union and United Kingdom under legislation relating to current financial sanctions regimes. This list includes all individuals and entities that are subject to financial sanctions in the UK. This list can be found at: www.bankofengland.co.uk/publications/financialsanctions/index.htm.

13. It is a criminal offence to make payments, or to allow payments to be made, to targets on the list maintained by the Bank of England. This would include dealing direct with targets, or dealing with targets through intermediaries (such as lawyers or accountants). Firms therefore need to have an appropriate means of monitoring payment instructions to ensure that no payments are made to targets or their agents. In the regulated sector this obligation applies to all firms, and not just to banks.

14. Guidance on compliance with the financial sanctions regime is set out in paragraphs 5.2.8 – 5.2.30.

FSA-regulated firms – the FSA Handbook

APER 2.1.2P
COND 2.5.7(10) G
ENF 11.9.1 G
PRIN 2.1.1 R
SYSC 2 and 3

15. SYSC requires FSA-regulated firms (subject to some specified exceptions: see paragraph 1.31 above) to have effective systems and controls for countering the risk that a firm might be used to further financial crime, and specific provisions regarding money laundering risks. It also requires such firms to ensure that approved persons exercise appropriate responsibilities in relation to these AML systems and controls. Parts of the FSA Handbook that are relevant to AML procedures, systems and controls, include:

- APER - Principle 5 requires an approved person to take reasonable steps to ensure that the business of the firm for which he is responsible is organised so that it is controlled effectively;
- COND – In relation to its ongoing assessment as to whether a firm meets the fitness and properness criterion, a firm is specifically required to have in place systems and controls against money laundering of the sort described in SYSC 3.2.6 R to SYSC 3.2.6J G;
- ENF – When considering whether to take disciplinary action in respect of a breach of the money laundering rules in SYSC 3.2 the FSA will have regard to whether a firm has followed relevant provisions in the JMLSG guidance for the financial sector;
- PRIN - Principle 3 requires a firm to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems; and
- SYSC - Chapters 2 and 3 set out particular requirements relating to senior management responsibilities, and for systems and controls processes, including specifically addressing the risk that the firm may be used to further financial crime. SYSC 3.2.6A R to SYSC 3.2.6J G cover

systems and controls requirements in relation to money laundering.

16. The text of the FSA Handbook is available at www.fsa.gov.uk/handbook. Relevant provisions of the FSA Handbook are further summarised in Appendix II.

FSMA s 402

17. In addition to its ability to prosecute for offences under the ML Regulations, the FSA has a wide range of disciplinary powers against authorised firms and approved persons for breaches of its Rules.

CHAPTER 2

INTERNAL CONTROLS

Key points in this chapter
➢ **Relevant law/regulation** ▪ FSMA s 6 ▪ Regulation 3 ▪ SYSC Chapters 2, 3, 3A
➢ **Core obligations** ▪ Firms must establish and maintain appropriate procedures to forestall and prevent money laundering ▪ Appropriate controls should take account of the risks faced by the firm's business
➢ **Actions required, to be kept under regular review** ▪ Establish and maintain appropriate procedures to forestall and prevent money laundering ▪ Introduce appropriate controls to take account of the risks faced by the firm's business ▪ Maintain appropriate control and oversight over outsourced activities

General legal and regulatory obligations

General

Regulation 3 (1)(b)
SYSC 3

2.1 There is a requirement for firms to establish such procedures of internal control and communication as may be appropriate for the purposes of forestalling and preventing money laundering. FSA-regulated firms have similar, regulatory obligations under SYSC.

2.2 This chapter provides guidance on the internal controls that will help firms meet their obligations in respect of the prevention of money laundering and terrorist financing. There are general obligations on firms to maintain appropriate records and controls more widely in relation to their business; this guidance is not intended to replace or interpret these wider obligations.

Appropriate controls in the context of financial crime prevention

Regulation 3(1)

2.3 There are specific requirements under the ML Regulations for the firm to have procedures in place in relation to: customer identification (see Chapter 5); record keeping (see Chapter 9); reporting of suspicions (see Chapter 7); and staff awareness and training (see Chapter 8). The ML Regulations are not specific about what these controls should comprise, and so it is helpful to look to the FSA Handbook, which although only formally applying to FSA-regulated firms, provides helpful commentary on overall systems requirements.

FSMA s 6
SYSC 2, 3
SYSC 3.1.1 R
SYSC 3.1.2 G
SYSC 3.2.6 R
SYSC 3.2.6F G

2.4 FSA-regulated firms are required to have systems and controls appropriate to their business. Specifically, those systems and controls must include measures 'for countering the risk that the firm might be used to further financial crime'. Financial crime includes the handling of the proceeds of crime – that is, money laundering or

terrorist financing. The nature and extent of systems and controls will depend on a variety of factors, including:

- the nature, scale and complexity of the firm's business;
- the diversity of its operations, including geographical diversity;
- its customer, product and activity profile;
- its distribution channels;
- the volume and size of its transactions; and
- the degree of risk associated with each area of its operation.

SYSC 3.2.6G G
SYSC 3.2.6H R
SYSC 3.2.6J G
SYSC 3.2.6I R

2.5 An FSA-regulated firm's systems and controls (but see paragraph 1.31 for general insurance firms and mortgage intermediaries) are required to cover:

- senior management accountability, including allocation to a director or senior manager overall responsibility for the establishment and maintenance of effective AML systems and controls and the appointment of a person with adequate seniority and experience as MLRO;
- appropriate training on money laundering to ensure that employees are aware of, and understand, their legal and regulatory responsibilities and their role in handling criminal property and money laundering/terrorist financing risk management;
- appropriate provision of regular and timely information to senior management relevant to the management of the firm's criminal property/money laundering/terrorist financing risks;
- appropriate documentation of the firm's risk management policies and risk profile in relation to money laundering, including documentation of the firm's application of those policies; and
- appropriate measures to ensure that money laundering risk is taken into account in the day-to-day operation of the firm, including in relation to:
  - the development of new products;
  - the taking-on of new customers; and
  - changes in the firm's business profile.

Outsourcing and non-UK processing

SYSC 3A.9 G

2.6 Many firms outsource some of their systems and controls and/or processing to elsewhere within the UK and to other jurisdictions, and/or to other group companies. Involving other entities in the operation of a firm's systems brings an additional dimension to the risks that the firm faces, and this risk must be actively managed. It is important that outsourcing should not result in reduced standards or requirements being applied. In all cases, the firm should have regard to the FSA's guidance on outsourcing (www.fsahandbook.info/FSA/html/handbook/SYSC/3A/9).

SYSC 3.2.4 G
SYSC 3A.9 G

2.7 FSA-regulated firms cannot contract out of their regulatory responsibilities, and therefore remain responsible for systems and controls in relation to the activities outsourced, whether within the UK or to another jurisdiction. In all instances of outsourcing it is the delegating firm that bears the ultimate responsibility for the duties undertaken in its name. This will include the requirement to ensure that the provider of the outsourced services has in place satisfactory AML/CFT systems, controls and procedures, and that those policies and procedures are kept up to date to reflect changes in UK requirements.

2.8 Where UK operational activities are undertaken by staff in other jurisdictions (for example, overseas call centres), those staff should be subject to the AML/CFT policies and procedures that are applicable to UK staff, and internal reporting procedures implemented to ensure that all suspicions relating to UK-related accounts, transactions or activities are reported to the nominated officer in the UK. Service level agreements will need to cover the reporting of management information on money laundering prevention, and information on training, to the MLRO in the UK.

2.9 Firms should also be aware of local obligations, in all jurisdictions to which they outsource functions, for the detection and prevention of financial crime. Procedures should be in place to meet local AML/CFT regulations and reporting requirements. Any conflicts between the UK and local AML/CFT requirements, where meeting local requirements would result in a lower standard than in the UK, should be resolved in favour of the UK.

2.10 In some circumstances, the outsourcing of functions can actually lead to increased risk - for example, outsourcing to businesses in jurisdictions with less stringent AML/CFT requirements than in the UK. All financial services businesses that outsource functions and activities should therefore assess any possible AML/CFT risk associated with the outsourced functions, record the assessment and monitor the risk on an ongoing basis.

CHAPTER 3

NOMINATED OFFICER/MONEY LAUNDERING REPORTING OFFICER (MLRO)

Key points in this chapter
➢ **Relevant law/regulation** ▪ Regulation 7 ▪ PRIN, Principle 11 ▪ APER, Chapters 2 and 4 ▪ APER, Principles 4 and 7 ▪ SYSC, Chapter 3 ▪ SUP, Chapter 10
➢ **Core obligations** ▪ Nominated officer must receive and review internal disclosures, and make external reports ▪ Nominated officer is responsible for making external reports ▪ FSA approval required for MLRO, as it is a Controlled Function (CF 11) ▪ Threshold competence required ▪ MLRO should be able to act on his own authority ▪ Adequate resources must be devoted to AML/CFT ▪ MLRO is responsible for oversight of the firm's compliance with its requirements in respect of staff training
➢ **Actions required, to be kept under regular review** ▪ Senior management to ensure the MLRO has: o active support of senior management o adequate resources o independence of action o access to information o responsibility for oversight of the firm's compliance with its requirements in respect of staff training o an obligation to produce an annual report ▪ MLRO to ensure he has continuing competence ▪ MLRO to monitor the effectiveness of systems and controls

General legal and regulatory obligations

Legal obligations

Regulation 7 POCA ss337, 338 Terrorism Act ss21A, 21B

3.1 All firms (other than sole traders) carrying out relevant business under the ML Regulations, whether or not the firm is regulated by the FSA, must appoint a nominated officer, who is responsible for receiving internal money laundering disclosures, deciding whether these should be reported to NCIS, and, if appropriate, making such external reports. He is also responsible for receiving internal reports under POCA and the Terrorism Act.

SYSC 3.2.6 R

3.2 As noted in paragraph 1.31, general insurance firms and mortgage intermediaries are not covered by the ML Regulations, or the provisions of SYSC relating specifically to money laundering, even though they are regulated by the FSA. They therefore are under no obligation to appoint a nominated officer or an MLRO, or to allocate to a director or senior manager the responsibility for the establishment and maintenance of effective anti-money laundering systems and controls. They are, however, subject to the general requirements of SYSC, and so have an obligation to have appropriate

risk management systems and controls in place, including controls to counter the risk that the firm might be used to further financial crime. They are also subject to some of the provisions of POCA and the Terrorism Act.

POCA s 332
Terrorism Act s 19

3.3 For administrative convenience, and to assist their staff fulfil their obligations under POCA or the Terrorism Act, firms who have no legal obligation to do so, may nevertheless choose to appoint a nominated officer. Where they do so, he will be subject to the reporting obligations in s 332 of POCA and s 19 of the Terrorism Act.

Regulatory obligations

SYSC 3.2.6I R

3.4 In the case of FSA-regulated firms, other than sole traders and those firms covered by paragraph 3.2, there is a requirement to appoint an MLRO. The responsibilities of the MLRO under SYSC are different from those of the nominated officer under the ML Regulations, POCA or the Terrorism Act, but in many FSA-regulated firms it is likely that the MLRO and the nominated officer will be one and the same person.

SYSC 3.2.6I(1) R

3.5 The MLRO is responsible for oversight of the firm's compliance with the FSA's Rules on systems and controls against money laundering.

3.6 An MLRO should be able to monitor the day-to-day operation of the firm's AML/CFT policies, and respond promptly to any reasonable request for information made by the FSA or law enforcement.

Standing of the MLRO

SUP 10.7.13 R
SYSC 3.2.6J G
FSMA s59

3.7 The role of MLRO has been designated by the FSA as a controlled function under s 59 of FSMA. As a consequence, any person invited to perform that function must be individually approved by the FSA, on the application of the firm, before performing the function. The FSA expect that the MLRO will be based in the UK.

APER 4.7.9 E
APER, Principle 7

3.8 Failure by the MLRO to discharge the responsibilities imposed on him in SYSC 3.2.6I R is conduct that does not comply with Statement of Principle 7 for Approved Persons, namely that 'an approved person performing a significant influence function must take reasonable steps to ensure that the business of the firm for which he is responsible in his controlled function capacity complies with the relevant requirements and standards of the regulatory system'.

SYSC 3.2.6I R
SYSC 3.2.6J G
SYSC 2.1.1 R

3.9 In FSA-regulated firms, the MLRO is responsible for the oversight of all aspects of the firm's AML/CFT activities and is the focal point for all activity within the firm relating to anti-money laundering. The individual appointed as MLRO must have a sufficient level of seniority within the firm (see paragraph 1.24). As the MLRO is an Approved Person, his job description should clearly set out the extent of the responsibilities given to him, and his objectives. The MLRO will need to be involved in establishing the basis on which a risk-based approach to the prevention of money laundering/terrorist financing is put into practice.

SYSC 3.2.6I(1) R

3.10 An MLRO will support and co-ordinate senior management focus on managing the money laundering/terrorist financing risk in individual business areas. He will also help ensure that the firm's wider responsibility for forestalling and preventing money laundering/terrorist financing is addressed centrally, allowing a firm-wide view to be taken of the need for monitoring and accountability.

SYSC 3.2.6I(2)R

3.11 The MLRO must have the authority to act independently in carrying out his responsibilities. The MLRO must be free to have direct access to the FSA and (where he is the nominated officer) appropriate law enforcement agencies, including NCIS, in order that any suspicious activity may be reported to the right quarter as soon as is practicable. He must be free to liaise with NCIS on any question of whether to proceed with a transaction in the circumstances.

SYSC 3.2.6I(2)R

3.12 Senior management of the firm must ensure that the MLRO has sufficient resources available to him, including appropriate staff and technology. This should include arrangements to apply in his temporary absence.

3.13 Where a firm is part of a group, it may appoint as its MLRO an individual who performs that function for another firm within the group. If a firm chooses this approach, it may wish to permit the MLRO to delegate AML/CFT duties to other suitably qualified individuals within the firm. Similarly, some firms, particularly those with a number of branches or offices in different locations, may wish to permit the MLRO to delegate such duties within the firm. In larger firms, because of their size and complexity, the appointment of one or more permanent Deputy MLROs of suitable seniority may be necessary. In such circumstances, the principal, or group MLRO needs to ensure that roles and responsibilities within the group are clearly defined, so that staff of all business areas know exactly who they must report suspicions to.

SUP 10.5.5R

3.14 Where an MLRO is temporarily unavailable, no pre-approval for a deputy will be required for temporary cover of up to 12 weeks in any consecutive 12-month period. For longer periods, however, FSA approval will need to be sought. Rather than appointing a formal deputy, smaller firms may prefer to rely on temporary cover.

3.15 Where AML/CFT tasks are delegated by a firm's MLRO, the FSA will expect the MLRO to take ultimate managerial responsibility.

Internal and external reports

Regulation 7

3.16 A firm should take reasonable steps to ensure that an internal report of possible money laundering or terrorist financing is considered by the nominated officer as soon as is reasonably practicable.

Regulation 7(1)(c)

3.17 Any internal report should be considered by the nominated officer, in the light of all other relevant information, to determine whether or not the information contained in the report does give rise to knowledge or suspicion, or reasonable grounds for knowledge or suspicion, of money laundering or terrorist financing.

3.18 A firm is expected to use its existing customer information effectively by making such information readily available to its nominated officer.

3.19 In most cases, before deciding to make a report, the nominated officer is likely to need access to the firm's relevant business information. A firm should therefore take reasonable steps to give its nominated officer access to such information. Relevant business information may include details of:

- the financial circumstances of a customer or any person on whose behalf the customer has been or is acting; and
- the features of the transactions, including, where appropriate, the jurisdiction in which the transaction took place, which the firm entered into with or for the customer (or that person).

3.20 In addition, the nominated officer may wish:

- to consider the level of identity information held on the customer, and any information on his personal circumstances that might be available to the firm; and
- to review other transaction patterns and volumes through the account or accounts in the same name, the length of the business relationship and identification records held.

Regulation 7(1)(d)

3.21 If the nominated officer concludes that the internal report does give rise to knowledge or suspicion of money laundering or terrorist financing, he must make a report promptly to NCIS.

3.22 Guidance on reviewing internal reports, and reporting as appropriate to NCIS, is set out in Chapter 7.

Obtaining and using national and international findings

3.23 An MLRO should ensure that the firm obtains, and makes appropriate use of, any government or FATF findings concerning the approach to money laundering prevention in particular countries or jurisdictions. This is especially relevant where the approach has been found to be materially deficient by FATF. Reports on the mutual evaluations carried out by the FATF can be found at www.fatf-gafi.org. FATF-style regional bodies also evaluate their members. Not all evaluation reports are published (although there is a presumption that those in respect of FATF members will be). Where an evaluation has been carried out and the findings are not published, firms will take this fact into account in assessing the money laundering and terrorist financing risks posed by the jurisdiction in question. Depending on the firm's area of operation, it may be appropriate to take account of other international findings, such as those by the IMF or World Bank.

3.24 JMLSG will from time to time publish any such findings on its website (www.jmlsg.org.uk). Firms should check this information regularly to ensure they keep up to date with current findings. Additionally, NCIS periodically produces intelligence assessments, which are forwarded to the MLROs of the relevant sectors for internal dissemination only. No NCIS material is published through an open source.

3.25 Firms considering business relations and transactions with individuals and

firms – whether direct or through correspondents - located in higher risk jurisdictions, or jurisdictions against which the UK has outstanding advisory notices, should take account of the background against which the assessment, or the specific recommendations contained in the advisory notices, have been made.

Awareness and training

SYSC 3.2.6G(1) G
SYSC 3.2.6H R

3.26 The MLRO is responsible for oversight of the firm's compliance with its requirements in respect of staff training, including ensuring that adequate arrangements for awareness and training of employees are in place. Although this is a firm-wide responsibility, there may be some delegation to appropriate persons/functions in business areas. The MLRO, however, is responsible for ensuring that the training is offered, that the standards and scope of the training are appropriate, and that appropriate records are kept. Overall responsibility within the firm for the establishment and maintenance of effective training lies with the relevant director or senior manager (who may or may not be the MLRO).

3.27 Specific guidance on staff awareness, training and alertness is set out in Chapter 8.

Monitoring effectiveness of money laundering controls

SYSC 3.2.6C R
SYSC 3.2.6I(1) R

3.28 A firm is required to carry out regular assessments of the adequacy of its systems and controls to ensure that they manage the money laundering risk effectively. Oversight of the implementation of the firm's AML/CFT policies and procedures, including the operation of the risk-based approach, is the responsibility of the MLRO, under delegation from senior management. He must therefore ensure that appropriate monitoring processes and procedures across the firm are established and maintained.

Reporting to senior management

SYSC 3.2.6G(2) G

3.29 At least annually the senior management of an FSA-regulated firm must commission a report from its MLRO which assesses the operation and effectiveness of the firm's systems and controls in relation to managing money laundering risk.

3.30 In practice, senior management should determine the depth and frequency of information they feel necessary to discharge their responsibilities. The MLRO may also wish to report to senior management more frequently than annually, as circumstances dictate.

3.31 The firm's senior management should consider the report, and take any necessary action to remedy deficiencies identified in it, in a timely manner.

3.32 The MLRO will wish to bring to the attention of senior management areas where the operation of AML/CFT controls should be improved, and

proposals for making appropriate improvements. The progress of any significant remedial programmes will also be reported to senior management.

3.33 In addition, the MLRO should report on the outcome of any relevant quality assurance or internal audit reviews of the firm's AML/CFT processes, as well as the outcome of any review of the firm's risk assessment procedures (see paragraph 4.33).

3.34 Firms will need to use their judgement as to how the MLRO should be required to break down the figures of internal reports in his annual report.

3.35 In 2002, the British Bankers' Association, after discussion with the FSA, issued a template suggesting a suitable presentation and content framework for a working paper underpinning the production of the MLRO Annual Report. An updated version of this framework will be made available on the JMLSG website in due course.

3.36 An MLRO may choose to report in a different format, according to the nature and scope of their firm's business.

3.37 In practice, subject to the approval of the FSA, larger groups might prepare a single consolidated report covering all of its authorised firms. The MLRO of each authorised firm within the group still has a duty to report appropriately to the senior management of his authorised firm.

CHAPTER 4

RISK-BASED APPROACH

Key points in this chapter
➢ **Relevant law/regulation** ▪ Regulation 3 ▪ Regulation 4 (3) (b) ▪ SYSC 3.1.2 G, 3.2.6 R, 3.2.6A-C, 3.2.6F ➢ **Other authoritative pronouncements which endorse a risk-based approach** ▪ FATF Recommendation 5 ▪ Basel CDD Paper ▪ IAIS Guidance Paper 5 ▪ IOSCO Principles paper ▪ Basel Consolidated KYC Risk Management Paper
➢ **Core obligations** ▪ Appropriate systems and controls must reflect the degree of risk associated with the business and its customers ▪ Take into account the greater potential for money laundering and terrorist financing which arises when the customer is not physically present
➢ **Actions required, to be kept under regular review** ▪ Carry out a formal, and regular, money laundering/terrorist financing risk assessment, including market changes, and changes in products, customers and the wider environment ▪ Ensure internal procedures, systems and controls, including staff awareness, adequately reflect the risk assessment ▪ Ensure customer identification and acceptance procedures reflect the risk characteristics of customers ▪ Ensure arrangements for monitoring systems and controls are robust, and reflect the risk characteristics of customers

Introduction

4.1 Senior management of most firms, whatever business they are in, manages its affairs with regard to the risks inherent in its business and the effectiveness of the controls it has put in place to manage these risks. A similar approach is appropriate to managing the risks of the firm being used for money laundering or terrorist financing. Many authoritative international bodies operating in the financial services sector, have issued pronouncements endorsing, and encouraging firms to follow, a risk-based approach to managing money laundering/terrorist financing risk.

SYSC 3.2.6F G

4.2 A risk-based approach takes a number of discrete steps in assessing the most cost effective and proportionate way to manage and mitigate the money laundering and terrorist financing risks faced by the firm. These steps are to:

- identify the money laundering and terrorist financing risks that are relevant to the firm;
- assess the risks presented by the firm's particular
  - customers;
  - products;
  - delivery channels;
  - geographical areas of operation;
- design and implement controls to manage and mitigate these assessed risks;

- monitor and improve the effective operation of these controls; and
- record appropriately what has been done, and why.

4.3 No system of checks will detect and prevent all money laundering or terrorist financing. A risk-based approach will, however, serve to balance the cost burden placed on individual firms and their customers with a realistic assessment of the threat of the firm being used in connection with money laundering or terrorist financing. It focuses the effort where it is needed and will have most impact.

4.4 To assist the overall objective to prevent money laundering and terrorist financing, a risk-based approach:

- recognises that the money laundering/terrorist financing threat to firms varies across customers, jurisdictions, products and delivery channels;
- allows management to differentiate between their customers in a way that matches the risk in their particular business;
- allows senior management to apply its own approach to the firm's procedures, systems and controls, and arrangements in particular circumstances; and
- helps to produce a more cost effective system.

4.5 The appropriate approach in any given case is ultimately a question of judgement by senior management, in the context of the risks they consider the firm faces. The FSA has indicated in a letter to the chairman of JMLSG that

- "… If a firm demonstrates that it has put in place an effective system of controls that identifies and mitigates its money laundering risk, then [enforcement] action [by the FSA] is very unlikely."
- "…[The FSA] recognise[s] that any regime that is risk-based cannot be a zero failure regime. [The FSA] appreciate[s] the importance of a non-zero failure regime; not least because a 100% standard will not be cost effective and will damage innovation, competition and legitimate commercial success."

The text of this letter is available on the FSA website at www.fsa.gov.uk/pubs/other/money_laundering/jmslg.pdf.

A risk-based approach

SYSC 3.2.6A R

4.6 All firms must assess their money laundering/terrorist financing risk in some way and decide how they will manage it. Firms may choose to carry out this assessment in a sophisticated way, or in a more simple way, having regard to the business they undertake, their customer base and their geographical area of operation. There is no requirement, or expectation, that a risk-based approach must involve a complex set of procedures to put it into effect; the particular circumstances of the firm will determine the most appropriate approach.

4.7 The business of many firms, their product and customer base, can be relatively simple, involving few products, with most customers falling into similar categories. In such circumstances, a simple approach, building on the risk the firm's products are assessed to present, may be appropriate for most customers, with the focus being on those customers who fall outside the 'norm'. Other firms may have a greater level of business, but large numbers of their customers may be predominantly retail, served through delivery channels that offer the possibility of

adopting a standardised approach to many AML/CFT procedures. Here, too, the approach for most customers may be relatively straightforward, building on the product risk.

4.8 Some other firms, however, often (but not exclusively) those dealing in wholesale markets, may offer a more 'bespoke' service to customers, many of whom are already subject to extensive due diligence by lawyers and accountants for reasons other than AML/CFT. In such cases, the business of identifying the customer will be more complex, but will take account of the considerable additional information that already exists in relation to the prospective customer.

4.9 How a risk-based approach is implemented will also depend on the firm's operational structure. For example, a firm that operates through multiple business units will need a different approach from one that operates as a single business.

4.10 Whatever approach is considered most appropriate to the firm's money laundering/terrorist financing risk, the broad objective is that the firm should know who their customers are, what they do, and whether or not they are likely to be engaged in criminal activity. The profile of their financial behaviour will build up over time, allowing the firm to identify transactions or activity that may be suspicious.

4.11 However carried out, a risk-based approach requires the full commitment and support of senior management, and the active co-operation of business units. The risk-based approach needs to be part of the firm's philosophy, and as such reflected in its procedures and controls. There needs to be a clear communication of policies and procedures across the firm, along with robust mechanisms to ensure that they are carried out effectively, weaknesses are identified, and improvements are made wherever necessary.

4.12 A risk assessment will often result in a stylised categorisation of risk: e.g., high/medium/low. Criteria will be attached to each category to assist in allocating customers and products to risk categories, in order to determine the different treatments of identification, verification, additional KYC information and monitoring for each category, in a way that minimises complexity.

Identifying and assessing the risks faced by the firm

4.13 Senior management should decide on the appropriate approach in the light of the firm's structure. The firm may adopt an approach that starts at the business area level, or one that starts from business streams. The firm may start with its customer assessments, and overlay these assessments with the product and delivery channel risks; or it may choose an approach that starts with the product risk, with the overlay being the customer and delivery channel risks, taking account of any geographical considerations relating to the customer, or the transaction.

4.14 A risk-based approach starts with the identification and assessment of the risk that has to be managed. Examples of the risks in particular industry sectors are set out in the sectoral guidance in Part II, and on the JMLSG website, www.jmlsg.org.uk.

4.15 The firm should assess its risks in the context of how it might most likely be involved in money laundering or terrorist financing. In this respect, senior management should ask themselves a number of questions; for example:

- What risk is posed by the firm's customers? For example:

  - Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale;
  - An individual in a public position and/or location which carries a higher exposure to the possibility of corruption (i.e., a PEP);
  - Customers based in, or conducting business in or through, a high risk jurisdiction, or a jurisdiction with known higher levels of corruption or organised crime, or drug production/distribution; and
  - Customers engaged in a business which involves significant amounts of cash.

- What risk is posed by a customer's behaviour? For example:

  - Where there is no commercial rationale for the customer buying the product he seeks;
  - Requests to associate undue levels of secrecy with a transaction;
  - Situations where the origin of wealth and/or source of funds cannot be easily verified or where the audit trail has been deliberately broken and/or unnecessarily layered; and
  - The unwillingness of non-personal customers to give the names of their real owners and controllers.

- How does the way the customer comes to the firm affect the risk? For example:

  - One-off transactions (see paragraph 5.2.7) v business relationships (see paragraph 5.2.6);
  - Introduced business, depending on the effectiveness of the due diligence carried out by the introducer; and
  - Non face-to-face acceptance.

- What risk is posed by the products/services the customer is using? For example:

  - Can the product features be used for money laundering or terrorist financing, or to fund other crime?
  - Do the products allow/facilitate payments to third parties?
  - Is the main risk that of inappropriate assets being placed with, or moving from, or through, the firm?
  - Does a customer migrating from one product to another within the firm carry a risk?

4.16 Many customers, by their nature or through what is already known about them by the firm, carry a lower money laundering or terrorist financing risk. These might include:

- Customers who are employment-based or with a regular source of income from a known source which supports the activity being undertaken; (this applies equally to pensioners or benefit recipients, or to those whose income originates from their partners' employment);
- Customers with a long-term and active business relationship with the firm; and
- Customers represented by those whose appointment is subject to court approval or ratification (such as executors).

4.17 Firms should not, however, judge the level of risk solely on the nature of the customer or the product. Where, in a particular customer/product combination, *either or both* the customer and the product are considered to carry a higher risk of money laundering or terrorist financing, the overall risk of the customer should be considered carefully. Firms need to be aware that allowing a higher risk customer to acquire a lower risk product or service on the basis of a verification standard that is appropriate to that lower risk product or service, can lead to a requirement for further verification requirements, particularly if the customer wishes subsequently to acquire a higher risk product or service.

4.18 Further considerations to be borne in mind in carrying out a risk assessment are set out in the sectoral guidance in Part II.

Design and implement controls to manage and mitigate the risks

4.19 Once the firm has identified and assessed the risks it faces in respect of money laundering or terrorist financing, senior management must ensure that appropriate controls to manage and mitigate these risks are designed and implemented.

4.20 As regards money laundering and terrorist financing, managing and mitigating the risks will involve measures to verify the customer's identity; collecting additional KYC information about the customer; and monitoring his transactions and activity, to determine whether there are reasonable grounds for knowing or suspecting that money laundering or terrorist financing may be taking place. Part of the control framework will involve decisions as to whether verification should take place electronically, and the extent to which the firm should use customer verification procedures carried out by other firms.

4.21 To decide on the most appropriate and relevant controls for the firm, senior management should ask themselves what measures the firm can adopt, and to what extent, to manage and mitigate these threats/risks most cost effectively, and in line with the firm's risk appetite. Examples of control procedures include:

- Introducing a customer identification programme that varies the procedures in respect of customers appropriate to their assessed money laundering/terrorist financing risk;
- Requiring the quality of evidence - documentary/electronic/third party assurance - to be of a certain standard;
- Obtaining additional customer information, where this is appropriate to their assessed money laundering/terrorist financing risk; and
- Monitoring customer transactions/activities.

It is possible to try to assess the extent to which each customer should be subject to each of these checks, but it is the balance of these procedures as appropriate to the risk assessed in the individual customer, or category of customer, to which he belongs that is relevant.

4.22 A customer identification programme that is graduated to reflect risk could involve:

- a standard information dataset to be held in respect of all customers;
- a standard verification requirement for all customers;
- more extensive due diligence (more identification checks and/or requiring additional KYC information) on customer acceptance for higher risk customers;
- where appropriate, more limited identity verification measures for specific lower risk customer/product combinations; and

- an approach to monitoring customer activities and transactions that reflects the risk assessed to be presented by the customer, which will identify those transactions or activities that may be unusual or suspicious.

4.23 Where a customer is assessed as carrying a higher risk, then depending on the product sought, it may be appropriate to seek additional information in respect of the customer, to be better able to judge whether or not the higher risk that the customer is perceived to present is likely to materialise. Such additional information may include an understanding of where the customer's funds and wealth have come from. Guidance on the types of additional information that may be sought is set out in section 5.6.

4.24 In order to be able to identify customer transactions or activity that may be suspicious, it will generally be necessary to monitor such transactions or activity in some way. Guidance on monitoring customer transactions and activity is given in Chapter 6. Monitoring customer activity should be carried out on the basis of a risk-based approach, with higher risk customer/product combinations being subjected to an appropriate frequency and depth of scrutiny, which is likely to be greater than may be appropriate for lower risk combinations.

4.25 The firm must decide, on the basis of its assessment of the risks posed by different customer/product combinations, on the level of verification that should be applied at each level of risk presented by the customer. Consideration should be given to all the information a firm gathers about a customer, as part of the normal business and vetting processes. Consideration of the overall information held may alter the risk profile of the customer.

4.26 Identifying a customer as carrying a higher risk of money laundering or terrorist financing does not automatically mean that he is a money launderer, or a financier of terrorism. Similarly, identifying a customer as carrying a low risk of money laundering or terrorist financing does not mean that the customer is not. Staff therefore need to be vigilant in using their experience and common sense in applying the firm's risk-based criteria and rules (see Chapter 8 – Staff awareness, training and alertness).

Monitor and improve the effective operation of the firm's controls

4.27 The firm will need to have some means of assessing that its risk mitigation procedures and controls are working effectively, or, if they are not, where they need to be improved. Its policies and procedures will need to be kept under regular review. Aspects the firm will need to consider include:

- Appropriate procedures to identify changes in customer characteristics, which come to light in the normal course of business;
- Reviewing ways in which different products and services may be used for money laundering/terrorist financing purposes, and how these ways may change, supported by typologies/law enforcement feedback, etc;
- Adequacy of staff training and awareness;
- Monitoring compliance arrangements (such as internal audit/quality assurance processes or external review);
- The balance between technology-based and people-based systems;
- Capturing appropriate management information;
- Upward reporting and accountability;
- Effectiveness of liaison with other parts of the firm; and
- Effectiveness of the liaison with regulatory and law enforcement agencies.

Record appropriately what has been done and why

4.28 The responses to consideration of the issues set out above, or to similar issues, will enable the firm to tailor its policies and procedures on the prevention of money laundering and terrorist financing. Documentation of those responses should enable the firm to demonstrate to its regulator and/or to a court:

- how it assesses the threats/risks of being used in connection with money laundering or terrorist financing;
- how it agrees and implements the appropriate systems and procedures, including due diligence requirements, in the light of its risk assessment;
- how it monitors and, as necessary, improves the effectiveness of its systems and procedures; and
- the arrangements for reporting to senior management on the operation of its control processes.

Risk management is dynamic

SYSC 3.2.6C R

4.29 Risk management generally is a continuous process, carried out on a dynamic basis. A money laundering/terrorist financing risk assessment is not a one-time exercise. Firms should therefore ensure that their risk management processes for managing money laundering and terrorist financing risks are kept under regular review.

4.30 There is a need to monitor the environment within which the firm operates. Success in preventing money laundering and terrorist financing in one area of operation or business will tend to drive criminals to migrate to another area, business, or product stream. Periodic assessment should therefore be made of activity in the firm's market place. If displacement is happening, or if customer behaviour is changing, the firm should be considering what it should be doing differently to take account of these changes.

4.31 In a stable business change may occur slowly: most businesses are evolutionary. Customers' activities change (without always notifying the firm) and the firm's products and services – and the way these are offered or sold to customers – change. The products/transactions attacked by prospective money launderers or terrorist financiers will also vary as perceptions of their relative vulnerability change.

4.32 There is, however, a balance to be achieved between responding promptly to environmental changes, and maintaining stable systems and procedures.

4.33 A firm should therefore keep its risk assessment(s) up to date. An annual, formal reassessment might be too often in most cases, but still appropriate for a dynamic, growing business. It is recommended that a firm revisit its assessment at least annually, even if it decides that there is no case for revision. Firms should include details of the assessment, and any resulting changes, in the MLRO's annual report (see paragraphs 3.29 to 3.37).

CHAPTER 5

CUSTOMER DUE DILIGENCE

Key points in this chapter

- **Relevant UK law/regulation**
  - Regulations 2 - 5
  - Regulation 30(1)
  - POCA ss330 - 331
  - POCA s 334(2)
  - POCA s 342
  - Financial sanctions legislation
- **Customers that may not be dealt with**
  - Regulation 28 – Treasury powers to forbid forming relationships with customers from a given country
  - UN Sanctions resolutions 1267 (1999), 1373 (2001), 1333 (2002), 1390 (2002) and 1617 (2005)
  - EC Regulation 2580/2001 and 881/2002 (as amended)
  - Terrorism Act, 2000, Sch 2
  - Terrorism (United Nations Measures) Order 2001
  - Al-Qa'ida and Taliban (United Nations Measures) Order 2002
  - Bank of England Sanctions Notices and News Releases
- **Regulatory regime**
  - SYSC 3.2.6 R, 3.2.6G(5) G
- **Other material pointing to good practice**
  - FATF Recommendations
  - Basel CDD paper
  - IAIS Guidance Paper 5
  - IOSCO Principles paper
  - Basel Consolidated KYC Risk Management Paper
- **Other relevant industry guidance**
  - Wolfsberg Principles

- **Core obligations**
  - Must have processes for identifying different types of customer
  - Must have systems to deal with identification issues in relation to those who cannot produce the standard evidence
  - Processes must take account of the greater potential for money laundering which arises when the customer is not physically present when being identified
  - Some persons/entities must not be dealt with
  - Must have specific policies in relation to the financially (and socially) excluded
  - If satisfactory evidence of identity is not obtained, the business relationship must not proceed further
  - Must have some system for updating customer information

5.1 What is customer due diligence, and why does it matter?

Why is it necessary to 'know your customer'?

Regulation 4(3)(a)
POCA, ss 327-334
Terrorism Act s 21A

5.1.1 The obligation on firms to be reasonably satisfied that their customers are who they say they are, and what to do if they appear to be acting on behalf of others, are set out in legislation and regulation. The obligations are designed to make it more difficult for the financial services industry to be used for money laundering or terrorist financing.

5.1.2 Firms also need to know their customers to guard against fraud, including impersonation fraud, and the risk of committing offences under POCA and the Terrorism Act, relating to money laundering and terrorist financing.

5.1.3 Firms therefore need to carry out customer due diligence for two broad reasons:

- to help the firm, at the time due diligence is carried out, to be reasonably satisfied that customers are who they say they are, to know whether they are acting on behalf of another, and that there is no legal barrier (e.g. government sanctions) to providing them with the product or service requested; and
- to enable the firm to assist law enforcement, by providing available information on customers or activities being investigated.

5.1.4 It may often be appropriate for the firm to know rather more about the customer than his identity: it will, for example, often need to be aware of the customer's business in order to assess the extent to which his transactions and activity undertaken with or through the firm is consistent with that business.

Customer due diligence

5.1.5 The due diligence carried out on new customers is in two distinct parts. As well as verifying his identity, the risk-based approach will lead to a need, in appropriate cases, to obtain additional information in respect of some customers. In this guidance, the additional information collected in respect of customers is referred to as "know your customer" or "KYC" information.

5.1.6 Firms will therefore take a combination of appropriate steps, on the basis of their assessment of the money laundering/terrorist financing risk that each customer, or class/category of customer, presents, addressing:

ID - verifying the customer's identity

- determining exactly who the customer is, whose identity needs to be verified (see section 5.2); and
- appropriately verifying that customer's identity (see section 5.4)

KYC - obtaining appropriate additional information (see section 5.6)

- understanding the customer's circumstances and business – including, where appropriate, the source of funds, and in some cases the source of wealth and the purpose of specific transactions - and the expected nature and level of transactions; and
- keeping such information current and valid

5.1.7 The amount and balance of resource applied across a firm to ID and to KYC will reflect the money laundering or terrorist financing risk customers present, taking account of the nature of their business and geographical location, and of the product or service sought.

Other material, pointing to good practice

5.1.8 FATF, the Basel Committee, IAIS, IOSCO and the Wolfsberg Group have issued recommendations on the steps that should be taken to identify customers. In addition, the Basel Committee has issued a paper on Consolidated KYC Risk Management. Although the Basel papers are addressed to banks, the IAIS Guidance Paper 5 to insurance entities, and IOSCO's Principles paper to the securities industry, their principles are worth considering by providers of other forms of financial services. These recommendations are available at the following websites: www.fatf-gafi.org; www.bis.org; www.iaisweb.org; www.iosco.org; www.wolfsberg-principles.com. Where relevant, firms are encouraged to use these websites to keep up to date with developing industry guidance from these bodies.

5.2 Who is the customer?

5.2.1 The law dealing with customer identification refers to 'applicants for business'. Under the ML Regulations, the term 'applicant for business' includes any natural or legal person who seeks to enter into a business relationship or conduct a one-off transaction, with a firm, as principal or as an agent for someone else.

Regulation 2(1)

5.2.2 Firms must therefore decide, in any proposed relationship, which individual or entity meets the definition of 'applicant for business' under the ML Regulations and therefore whose identity may have to be verified. In many cases this may be straightforward, but where legal entities are involved, or the person who makes contact with the firm acts for others, it is often less clear.

5.2.3 The FSA Glossary definition of 'customer' is not relevant for AML/CFT purposes.

5.2.4 A practical distinction between an applicant for business and a customer is that an 'applicant for business' can be turned away before a relationship is formed, whereas a person who is a 'customer' has been accepted into a relationship. It is the customer whose identity must (subject to certain exceptions) be appropriately verified. In setting out steps to be taken to verify identity, this guidance therefore refers to 'customers', rather than to 'applicants for business'.

Regulation 4 (3)(d)

5.2.5 A person for whom the principal is acting is not an applicant for business under the ML Regulations. Nevertheless, subject to the exemption set out in paragraph 5.2.34, reasonable measures must be taken to establish the identity of that other person.

Regulation 2(1)

5.2.6 A "business relationship" is defined in the ML Regulations as any arrangement, the purpose of which is to facilitate the carrying out of transactions on a 'frequent, habitual or regular' basis, and where the total amount of any payments to be made by any person to any other in the course of the arrangement is not known or capable of being ascertained at the outset. One-off transactions are not 'business relationships' under this definition (but see paragraph 5.2.7). A relationship need not involve the firm in an actual transaction; giving advice may often constitute establishing a business relationship.

Regulation 2(1)
Regulation 4(2)(c)

5.2.7 A "one-off transaction" means any transaction carried out other than in the course of a business relationship, e.g. a single foreign currency transaction, or an isolated instruction to purchase shares, for a customer who does not have a continuing relationship with the firm concerned. Where a number of "one-off transactions" take place that, in the view of the firm, are linked, their value is to be aggregated when measured against any one-off transaction exemption threshold for identity verification (see paragraph 5.2.35).

Persons firms should not accept as customers

5.2.8 The United Nations, European Union, and United Kingdom are each able to designate persons and entities as being subject to financial sanctions, in accordance with legislation explained below. Such sanctions normally include a prohibition on making funds available to the designated target or a more comprehensive asset freeze. A Consolidated List of all targets to whom financial sanctions apply is maintained by the Bank of England, and includes all individuals and entities that are subject to financial sanctions in the UK. This list can be found at: www.bankofengland.co.uk/publications/financialsanctions/index.htm.

5.2.9 The obligations under the UK financial sanctions regime apply to all firms, and not just to banks. The Consolidated List is the definitive list as regards the obligations under UK law. Firms will not normally have any obligation under UK law to have regard to lists issued by other organisations or authorities. Depending on the geographical area in which firms, or their customers, do business, however, firms need to be aware of the scope and focus of relevant financial sanctions regimes. The other websites referred to below may contain useful background information, but all the names that firms legally have to know about are on the Bank of England's list. All firms to whom this guidance applies, therefore, whether or not they are FSA-regulated or subject to the ML Regulations, will need either:

- for manual checking: to register with the Bank of England update service (directly or via a third party, such as a trade association); or
- if checking is automated: to ensure that relevant software includes checks against the relevant list and that this list is up to date.

5.2.10 The origins of such sanctions and the sources of information for the Consolidated List are covered below.

5.2.11 The Bank of England website contains general guidance on the implementation of financial sanctions and various electronic versions of the Consolidated List to assist with compliance, as well as regime-specific target lists, details of all Notices updating the Consolidated List and News Releases issued by the Bank of England, and links to other useful websites. The Bank of England may also be contacted direct to provide guidance and to assist with any concerns regarding the implementation of financial sanctions:

Financial Sanctions Unit
Tel: +44 (0) 20 7601 4768/5811/4783/4607
Fax: +44 (0) 20 7601 4309
Email: sanctions.unit@bankofengland.co.uk

5.2.12 It is a criminal offence to make funds or financial services available to targets on the list maintained by the Bank of England. This would include dealing direct with targets, and dealing with targets through intermediaries (such as lawyers or accountants). Firms therefore need to have an appropriate means of monitoring payment instructions to ensure that no payments are made to targets or their agents, to avoid leaving themselves open to breaching financial sanctions legislation.

5.2.13 The obligation under UK law is absolute – it is a criminal offence to make funds or financial services available to a target or its agent. However, in line with the principles set out in the Code for Crown Prosecutors, prosecution of a firm suspected to be in breach of the financial sanctions regime in the UK would be likely only where the prosecuting authorities consider this to be in the public interest, and where they believe that there is enough evidence to provide a realistic prospect of conviction. The Code for Crown Prosecutors can be accessed at www.cps.gov.uk/publications/docs/code2004english.pdf.

5.2.14 To reduce the risk of breaching their obligations under financial sanctions regimes, firms are likely to focus their resources on areas of their business that carry a greater likelihood of involvement with targets, or their agents. Within this approach, firms are likely to focus their prevention and detection procedures on direct customer relationships, and then have appropriate regard to other parties involved.

5.2.15 Firms need to have some means of monitoring payment instructions to ensure that proposed payments to targets or their agents are not made. The majority of payments made by many firms will, however, be to other regulated firms, rather than to individuals or entities that may be targets.

5.2.16 Where a firm freezes funds under financial sanctions legislation, or where it has suspicions of terrorist financing, it must make a report to the Bank of England, and/or to NCIS. Guidance on such reporting is given in paragraphs 7.30 to 7.44.

Terrorism

UNSCR 1373 (2001)

5.2.17 The UN Security Council has passed UNSCR 1373 (2001), which calls on all member states to act to prevent and suppress the financing of terrorist acts. Guidance issued by the UN Counter Terrorism Committee in relation to the implementation of UN Security Council Resolutions regarding terrorism can be found at: www.un.org/Docs/sc/committees/1373/.

UNSCR 1267 (1999); 1390 (2002); 1617 (2005)

5.2.18 The UN has also published the names of individuals and organisations subject to UN financial sanctions in relation to involvement with Usama bin Laden, Al-Qa'ida, and the Taliban under UNSCR 1267 (1999), 1390 (2002) and 1617 (2005). All UN member states are required under international law to freeze the funds and economic resources of any legal person(s) named in this list and to report any suspected name matches to the relevant authorities.

EC Regulation 2580/2001 (as amended)

5.2.19 The EU directly implements all UN financial sanctions, including financial sanctions against terrorists, through binding and directly applicable EC Regulations. The EU implemented UNSCR 1373 through the adoption of Regulation EC 2580/2001 (as amended). This Regulation introduces an obligation in Community law to freeze all funds and economic resources belonging to named persons and entities, and not to make any funds or economic resources available, directly or indirectly, to those named.

EC Regulation 881/2002 (as amended)

5.2.20 UNSCR 1267 and its successor resolutions are implemented at EU level by Regulation EC 881/2002 (as amended).

5.2.21 The texts of the EC Regulations referred to in paragraphs 5.2.19 and 5.2.20, and the lists of persons targeted, are available on the European Commission's sanctions website: europa.eu.int/comm/external_relations/cfsp/sanctions/measures.htm. As noted above, names of persons and entities on the EU list will be included in the Consolidated List maintained by the Bank of England.

Terrorism (United Nations Measures) Order 2001
Al-Qa'ida and Taliban (United Nations Measures) Order 2002

5.2.22 The UK has implemented UNSCR 1373 under the Terrorism (United Nations Measures) Order 2001, and UNSCR 1267 and its successor resolutions under the Al-Qa'ida and the Taliban (United Nations Measures) Order 2002.

5.2.23 Acting under the Terrorism (United Nations Measures) Order 2001, or the Al-Qa'ida and the Taliban (United Nations Measures) Order 2002, where the Treasury has reasonable grounds for suspecting that the person by, for, or on behalf of whom any funds are held, is, or may be, a person who commits, attempts to commit, facilitates or participates in the commission of acts of terrorism, it can, by notice, direct that such funds be frozen. This might result in the addition of a name to the Bank of England list that might not appear on the equivalent UN or EU lists.

Terrorism Act Sch 2

5.2.24 A number of organisations have been proscribed under UK anti-terrorism legislation. Where such organisations are also subject to financial sanctions (an asset freeze), they are included on the Consolidated List maintained by the Bank of England.

5.2.25 The primary source of information on proscribed organisations, however, including up-to-date information on aliases, is the Home Office. Firms can find the list of proscribed organisations at: www.homeoffice.gov.uk/security/terrorism-and-the-law/terrorism-act/proscribed-groups?version=1.

Country-specific

5.2.26 The UN Security Council also maintains a range of country-based financial sanctions that target specific individuals and entities connected with the political leadership of targeted countries. Each UN sanctions regime has a relevant Security Council Committee that maintains general guidance on the implementation of financial sanctions and current lists of targeted persons and entities. The list of currently applicable Security Council Resolutions can be found at www.un.org/Docs/sc/committees/INTRO.htm.

EC Regulation 2580/2001

5.2.27 The EU directly implements all UN financial sanctions against countries/regimes; it can also initiate autonomous measures under the auspices of its Common Foreign and Security Policy. Detail on UN-derived and EU autonomous financial sanctions regimes (including targets) is available on the European Commission's sanctions website, europa.eu.int/comm/external_relations/cfsp/sanctions/measures.htm.

5.2.28 The UK implements all UN and EU country/regime-specific measures

by means of assorted statutory instruments. Unlike the arrangements under the terrorism measures, the UK would not normally make autonomous additions to the target lists for these types of sanctions. The prohibition on making funds available, and the absolute nature of the legal obligation, applies to country-specific sanctions as it does to terrorism sanctions. Where relevant, any specific individuals and entities subject to such targeted countries/regimes will be included on the Bank of England Consolidated List.

Regulation 28

5.2.29 The Treasury may direct that a firm may not enter a business relationship or carry out a one-off transaction in relation to a person who is based or incorporated in a country (other than an EEA state) to which the FATF has decided to apply counter-measures. Details of any such Treasury directions will be found on www.hm-treasury.gov.uk or www.jmlsg.org.uk.

5.2.30 Trade sanctions – such as embargoes on making military hardware or know-how available to certain named countries or jurisdictions – can be imposed by governments or other international authorities, and these can have financial implications. Firms which operate internationally should be aware of such sanctions, and should consider whether these affect their operations; if so, they should decide whether they have any implications for the firm's procedures. Further information and links to lists of affected countries can be found at: www.dti.gov.uk/export.control/.

Customers whose identity might not need to be verified

5.2.31 There are three groups of customer whose identity might not need to be verified:

- those specifically exempted under the ML Regulations;
- customers with an existing business relationship with the firm at the point the obligation to verify identity was introduced; and
- customers who come to the firm through the acquisition of one financial services firm, or a portfolio of customers, by another.

Regulation 5(1)
Regulation 4(2)(b)(i)

5.2.32 There is no exemption from the obligation to verify identity where the firm knows or suspects that a proposed relationship or one-off transaction involves money laundering or terrorist financing.

Customers specifically exempted

Regulation 5

5.2.33 There are three broad categories of exemption from the obligation to verify identity, and these are set out in the following paragraphs.

Regulation 5 (2)

5.2.34 First, no verification of identity of any person is required - other than to confirm that the applicant is, in fact, regulated - where the customer, whether acting as principal or as agent for others:

(i) carries on financial services business which is subject to the ML Regulations, or to the EU Money Laundering Directive, and is not a money service operator; or

(ii) is regulated by an overseas regulatory authority and is based or incorporated in a non-EEA state whose law contains comparable provisions to those contained in the EU Directive.

5.2.35 Secondly, no verification of identity is required in any of the following three situations relating to one-off transactions:

Regulation 4(2)(b)(ii)
Regulation 4(2)(c)

(i) a one-off transaction (see paragraph 5.2.7) for less than €15,000 (other than where there are two or more such transactions which the firm believes are linked, and which together would amount to €15,000 or more);

Regulation 5(3)

(ii) a one-off transaction (see paragraph 5.2.7) carried out with or for a third party introduced by a person or firm that falls under paragraph 5.2.34, on condition that the introducer provides written assurance to the firm that evidence of the identity of all third parties introduced by him will have been obtained and recorded under procedures maintained by him**;**

Note: The reference to 'all third parties' does not include those customers where the transaction is less than €15,000, nor those who benefit from a specific exemption from identification.

Regulation 5(5)

(iii) where the proceeds of a one-off transaction are payable to the customer, but are directly reinvested on his behalf in another transaction of which a record is kept, and which can result only in another reinvestment made on the customer's behalf or in a payment made directly to the customer.

5.2.36 The one-off transaction exemption will therefore apply in any of the following situations:

- when the payment to be made by or to the customer is, in total, less than €15,000, and the customer is not expected to require further services from the firm; and
- the total funds to be deposited or invested are known at the outset;

or

- when the proceeds of a one-off transaction are re-invested for the benefit of the customer, irrespective of the amount involved.

5.2.37 Conversely, if a customer undertakes frequent or regular transactions (regardless of the amount), or if the total value of a number of intended transactions is not known at the outset, this will constitute a business relationship (see paragraph 5.2.6), and the customer's identity must be verified at the outset, regardless of the value of the first, or subsequent,

transaction.

5.2.38 The factors linking transactions to assess whether there is a business relationship are inherent in the characteristics of the transactions, rather than in taking any arbitrary time limit – for example, where several payments are made to the same recipient from one or more sources over a short period of time, or where a customer regularly transfers funds to one or more sources. For lower-risk investment products where there are no third party receipts or payments, a three-month period for linking transactions might be appropriate, assuming this is not a regular occurrence.

Introduction of one-off transactions by financial institutions from comparable jurisdictions

5.2.39 In situations where reliance is being placed on a general written undertaking from the introducer (see paragraph 5.2.34) or general assurance in signed terms of business, firms are recommended to ensure that the division of responsibilities between themselves and the introducer is clearly agreed and understood.

5.2.40 This exemption applies only to one-off transactions. If the person being introduced is opening a bank or investment account or forming any other continuous business relationship with the firm, a separate confirmation of verification of identity must be obtained in respect of each introduced customer in line with the guidance given in section 5.6.

5.2.41 Thirdly, in relation to insurance contracts:

Regulation 5(4)(a)

(i) in relation to a contract of long-term insurance associated with a pension scheme taken out by virtue of a person's contract of employment or occupation, no verification is required where the contract contains no surrender value, and may not be used as collateral for a loan.

Regulation 5(4)(b)

(ii) in relation to contracts of long-term insurance, there are de minimis limits of €2,500 in respect of single premium business, and €1,000 per annum in respect of regular premiums.

Note: Further guidance on the application of these exemptions is given in Part II, sector 7: *Life assurance, and life-related pensions and investment products*.

5.2.42 Where a firm has taken on business that falls under one of the exemption categories, evidence should be retained which shows that the firm has satisfied itself that identification of the customer, or class/category of customer, was not required.

Regulation 3(1)(b)
POCA s330 (2)(b)
Terrorism Act s 21A

5.2.43 An exemption from the basic verification obligation does not remove the need for the firm to comply with other customer due diligence procedures that are in place to forestall and prevent money laundering, and the duty to report knowledge or suspicion of money laundering or terrorist financing.

Customers with an existing business relationship with the firm

Regulation 30(1)

5.2.44 Where a business relationship with a customer was established before 1 April 1994 (the date the Money Laundering Regulations 1993 came into force) and has continued since then, there is no legal requirement to verify the customer's identity. However, the exemption in respect of pre-April 1994 customers only extends to the requirement to identify the customer. The obligation to report suspicions of money laundering, or terrorist financing, applies in respect of all the firm's customers, as does the UK financial sanctions regime (see paragraphs 5.2.8-5.2.30).

5.2.45 The exemption from identifying pre-April 1994 customer relationships does not extend to existing customers with whom the firm only undertook a one-off transaction before that date. Any such persons entering into a new business relationship, or a one-off transaction of €15,000 or more, with the firm are subject to the full identification obligations under the ML Regulations.

5.2.46 The general obligation that a firm know its customers, however, implies that this covers all its customers, and not just those who have been taken on since 1994. As risk dictates, therefore, firms are recommended to take steps to ensure that they hold appropriate information to demonstrate that they know all their customers. A range of trigger events, such as an existing customer applying to open a new account or establish a new relationship, might prompt a firm to seek appropriate evidence.

FSA Briefing Note, July 2003
SYSC 3.2.6 R

5.2.47 In July 2003, senior management of FSA-regulated firms were reminded of their regulatory responsibilities to maintain effective systems and controls for countering the risk that they may be used to further financial crime. The FSA reminded firms that, when carrying out risk assessment and mitigation, the FSA would expect them – as part of their overall approach to AML/CFT – to have considered the risk posed by existing customers who have not been identified. The FSA also expect firms (if appropriate) to take steps or put controls in place to mitigate this risk. Senior management and MLROs were encouraged to consider specific questions in relation to this risk, and to take any appropriate steps.

FSA Briefing Note, July 2003

5.2.48 Firms that do not seriously address risks (including the risk that they have not confirmed the identity of existing customers) are exposing themselves to the possibility of action for breach of the FSA Rules, or of the ML Regulations. The FSA briefing note is at www.fsa.gov.uk/pubs/other/id_customers.pdf.

5.2.49 A firm may hold considerable information in respect of a customer of some years' standing. In some cases the issue may be more one of collating and assessing information already held than approaching customers for more identification data or information.

Acquisition of one financial services firm, or a portfolio of customers, by another

5.2.50 When a firm acquires the business and customers of another firm, either as a whole, or as a portfolio, it is not necessary for the identity of

all existing customers to be re-verified, provided that:

- all underlying customer records are acquired with the business; **or**
- a warranty is given by the acquired firm, or by the vendor where a portfolio of customers or business has been acquired, that customers have been identified.

It is, however, important that the acquiring firm's due diligence enquiries include some sample testing in order to confirm that the customer identification procedures previously followed by the acquired firm (or by the vendor, in relation to a portfolio) have been carried out in accordance with UK requirements.

5.2.51 In the event that:

- the sample testing of the customer identification procedures previously undertaken shows that these have not been carried out to an appropriate standard; or
- the procedures cannot be checked; or
- the customer records are not accessible by the acquiring firm,

verification of identity will need to be undertaken as soon as is practicable for all transferred customers who are not existing verified customers of the transferee, in line with the acquiring firm's risk-based approach, and the requirements for existing customers opening new accounts.

5.3 Nature and evidence of identity

Nature of identity

5.3.1 The identity of an individual has a number of aspects: e.g., his/her given name (which of course may change), date of birth, place of birth. Other facts about an individual accumulate over time (the so-called electronic "footprint"): e.g., family circumstances and addresses, employment and business career, contacts with the authorities or with other financial sector firms, physical appearance.

5.3.2 The identity of a non-personal customer is a combination of its constitution, its business, and its legal and ownership structure.

Evidence of identity

Regulation 4(3)(a)
Regulation 2(5)

5.3.3 The stated objectives of the ML Regulations are first, that the evidence offered is reasonably capable of establishing the customer's identity, and secondly, that the person who is assessing the evidence is satisfied that the customer is the person he claims to be. The ML Regulations require that:

- the applicant for business will produce satisfactory evidence of his identity; **or**
- procedures established by the firm will produce such satisfactory evidence.

Regulation 4(3)(a)

5.3.4 Being reasonably satisfied that a customer is the person he claims to be is therefore a combination of being satisfied that:

- the named person exists: from appropriate identity data and information; and
- the customer is that person: by verifying from reliable, independent source documents, data or information, satisfactory confirmatory evidence of appropriate parts of the customer's accumulated profile.

Nature and extent of evidence

5.3.5 Evidence of identity can take a number of forms. In respect of individuals, much weight is placed on so-called 'identity documents', such as passports and photocard driving licences, and these are often the easiest way of being reasonably satisfied as to someone's identity. It is, however, possible to be reasonably satisfied as to a customer's identity based on other forms of confirmation, including, in appropriate circumstances, written or otherwise documented assurances from persons or organisations that have dealt with the customer for some time.

5.3.6 How much identity information or evidence to ask for, and what to verify, in order to be reasonably satisfied as to a customer's identity, are matters for the judgement of the firm, which will be exercised on a risk-based approach, as set out in Chapter 4, taking into account factors such as:

- the nature of the product or service sought by the customer (and any other products or services to which they can migrate without further identity verification);
- the nature and length of any existing or previous relationship between the customer and the firm;
- the nature and extent of any assurances from other regulated firms that may be relied on; and
- whether the customer is physically present.

5.3.7 Evidence of identity can be in documentary or electronic form. An appropriate record of the steps taken, and copies of the evidence held, to identify the customer must be kept.

Documentary evidence

5.3.8 Documentation purporting to offer evidence of identity may emanate from a number of sources. These documents differ in their integrity, reliability and independence. Some are issued after due diligence on an individual's identity has been undertaken; others are issued on request, without any such checks being carried out. There is a broad hierarchy of documents:

- certain documents issued by government departments and agencies, or by a court; then
- certain documents issued by other public sector bodies or local authorities; then
- certain documents issued by regulated firms in the financial services sector; then
- those issued by other firms subject to the ML Regulations, or to comparable legislation; then
- those issued by other organisations.

5.3.9 Firms should recognise that some documents are more easily forged than others. If suspicions are raised in relation to any document offered, firms should take whatever practical and proportionate steps are available to establish whether the document offered has been reported as lost or stolen.

5.3.10 In their procedures, therefore, firms will in many situations need to be prepared to accept a range of documents, and they may wish also to employ electronic checks, either on their own or in tandem with documentary evidence.

Electronic evidence

5.3.11 Electronic data sources can provide a wide range of confirmatory material without involving the customer. Where such sources are used for a credit check, the customer's permission is required under the Data Protection Act; a search for identity verification for AML/CFT purposes, however, leaves a different 'footprint' on the customer's electronic file, and the customer's permission is not required, but they must be informed that this check is to take place.

5.3.12 External electronic databases are accessible directly by firms, or through independent third party organisations. The size of the electronic 'footprint' (see paragraph 5.3.1) in relation to the depth, breadth and quality of data, and the degree of corroboration of the data supplied by the customer, may provide a useful basis for an assessment of the degree of confidence in their identity.

Nature of electronic checks

5.3.13 A number of commercial agencies which access many data sources are accessible online by firms, and may provide firms with a composite and comprehensive level of electronic verification through a single interface. Such agencies use databases of both positive and negative information, and many also access high-risk alerts that utilise specific data sources to identify high-risk conditions, for example, known identity frauds or inclusion on a sanctions list. Some of these sources are, however, only available to closed user groups.

5.3.14 Positive information (relating to full name, current address, date of birth) can prove that an individual exists, but some can offer a higher degree of confidence than others. Such information should include data from more robust sources - where an individual has to prove their identity, or address, in some way in order to be included, as opposed to others, where no such proof is required.

5.3.15 Negative information includes lists of individuals known to have committed fraud, including identity fraud, and registers of deceased persons. Checking against such information can indicate an increased risk of impersonation fraud.

5.3.16 For an electronic check to provide satisfactory evidence of identity on its own, it must use data from multiple sources, and across time, or incorporate qualitative checks that assess the strength of the information supplied. An electronic check that accesses data from a single source (e.g., a single check against the Electoral Roll) is not normally enough on its own to verify identity.

Criteria for use of an electronic data provider

5.3.17 Before using a commercial agency for electronic verification, firms should be satisfied that information supplied by the data provider is considered to be sufficiently extensive, reliable and accurate. This judgement may be assisted by considering whether the provider meets all the following criteria:

- it is recognised, through registration with the Information Commissioner's Office, to store personal data;
- it uses a range of positive information sources that can be called upon to link an applicant to both current and previous circumstances;
- it accesses negative information sources, such as databases relating to identity fraud and deceased persons;
- it accesses a wide range of alert data sources; and
- it has transparent processes that enable the firm to know what checks were carried out, what the results of these checks were, and what they

mean in terms of how much certainty they give as to the identity of the subject.

5.3.18 In addition, a commercial agency should have processes that allow the enquirer to capture and store the information they used to verify an identity.

5.4 Initial identity checks

5.4.1 Identifying a customer is a two-part process. The firm first *identifies* the customer, by obtaining a range of information from him. The second part – the *verification* – consists of the firm verifying some of this information through the use of reliable, independent source documents, data or information.

5.4.2 The guidance in this section first addresses personal customers, and, secondly, non-personal customers. In each case, the guidance discusses the standard identification requirement, and then goes on to provide further guidance on steps that may be applied as part of a risk-based approach.

5.4.3 The guidance in this section should be read in conjunction with that on the risk-based approach set out in Chapter 4, and supplemented by the sectoral guidance set out in Part II.

5.4.4 The introduction of this guidance does not require firms to hold the standard range of personal information in respect of all existing customers. Firms should, however, have regard to paragraphs 5.2.44 to 5.2.49, which give guidance on what they should do in respect of existing customers.

At what point does identity have to be verified?

5.4.5 A person who is an 'applicant for business' can be turned away before a relationship is formed. A person who is a 'customer', however, has been accepted into a relationship, and his identity must be appropriately verified (see paragraphs 5.2.1 – 5.2.4).

Regulation 4 (3) (a)

5.4.6 Satisfactory identification of the customer must take place as soon as reasonably practicable after first contact between the firm and the customer.

5.4.7 Sometimes, in the normal conduct of business, it is possible that a business relationship has to commence before verification of the customer's identity can be completed. This might be the case, for example, in respect of some non face-to-face business, some investment transactions, or some types of life assurance business. In such circumstances, firms' risk management procedures should take account of these conditions, and should require controls to be placed over the extent of the relationship entered into, or any funds held under the relationship, until verification has been completed.

Regulation 4 (3) (c)

5.4.8 Where a customer's identity cannot be verified satisfactorily, the firm must not proceed further with the transaction or the business relationship. The firm should consider whether the inability to verify the customer's identity is due to the customer not being in possession of the standard documents or other information appropriate to the risk they are assessed

to present, or whether the circumstances give grounds for making a report to NCIS.

5.4.9 If the inability is caused by the customer not possessing the right documents or information, the firm should consider whether there are any other ways of being reasonably satisfied as to the customer's identity.

5.4.10 If the firm concludes that there are no grounds for making a report, it will need to decide on the appropriate course of action. This may be to retain the funds while it seeks other ways of being reasonably satisfied as to the customer's identity, or to use its best endeavours to return the funds to the source from which they came, if possible without being banked.

5.4.11 If the firm concludes that the circumstances do give reasonable grounds for knowledge or suspicion of money laundering or terrorist financing, a report must be made to NCIS (see Chapter 7). The firm must then retain the funds until consent has been given to return the funds to the source from which they came.

Keeping information up to date

5.4.12 Where information is held about customers, it should, as far as reasonably possible, be kept up to date. Once the identity of a customer has been satisfactorily verified, there is no obligation to re-verify identity; as risk dictates, however, firms are recommended to take steps to ensure that they hold appropriate up-to-date information on their customers.

Electronic transfer of funds

5.4.13 To implement FATF Special Recommendation VII, the EU is in the process of finalising a Regulation on information on the payer accompanying the electronic transfer of funds. This draft Regulation will require certain information on the payer to be verified. Guidance on meeting firms' obligations under this Regulation will be provided once the terms of the Regulation have been finally agreed.

Personal customers

General

5.4.14 Paragraphs 5.4.15 to 5.4.32 refer to the standard identification requirement for personal customers; paragraphs 5.4.33 to 5.4.60 provide further guidance on steps that may be applied as part of a risk-based approach.

Obtain standard evidence

Identification

5.4.15 The firm should obtain the following information in relation to the personal customer:

- full name
- residential address
- date of birth

5.4.16 Verification of the information obtained should be based either on a document or documents produced by the customer, or electronically by the firm, or by a combination of both. Where business is conducted face-to-face, firms should see originals of any documents involved in the verification. Customers should be discouraged from sending original valuable documents by post.

Documentary verification

5.4.17 If documentary evidence of an individual's identity is to provide a high level of confidence, it will typically have been issued by a government department or agency, or by a court, because there is a greater likelihood that the authorities will have checked the existence and characteristics of the persons concerned. In cases where such documentary evidence of identity may not be available to an individual, other evidence of identity may give the firm reasonable confidence in the customer's identity, although the firm should weigh these against the risks involved.

5.4.18 Non-government-issued documentary evidence complementing identity should normally only be accepted if it originates from a public sector body or another regulated financial services firm, or is supplemented by knowledge that the firm has of the person or entity, which it has documented.

5.4.19 If identity is to be verified from documents, this should be based on:

Either a government-issued document which incorporates:

- the customer's full name and photograph, and
  - **either** his residential address

- **or** his date of birth.

Government-issued documents with a photograph include:
➢ Valid passport ➢ Valid photocard driving licence (full or provisional) ➢ National Identity card (non-UK nationals) ➢ Firearms certificate or shotgun licence ➢ Identity card issued by the Electoral Office for Northern Ireland

or a government-issued document (without a photograph) which incorporates the customer's full name, ***supported by*** a second document, either government-issued, or issued by a judicial authority, a public sector body or authority, or another FSA-regulated firm in the UK financial services sector, or in a comparable jurisdiction, which incorporates:

- the customer's full name and
  - **either** his residential address
  - **or** his date of birth

Government-issued documents without a photograph include:	Other documents include:
➢ Valid (old style) full UK driving licence ➢ Recent evidence of entitlement to a state or local authority-funded benefit (including housing benefit and council tax benefit), tax credit, pension, educational or other grant	➢ Instrument of a court appointment (such as liquidator, or grant of probate) ➢ Current council tax demand letter, or statement ➢ Current bank statements, or credit/debit card statements, issued by a regulated financial sector firm in the UK, EU or comparable jurisdiction (but not ones printed off the internet) ➢ Utility bills (but not ones printed off the internet)

5.4.20 Where a member of the firm's staff has visited the customer at his home address, a record of this visit may constitute evidence corroborating that the individual lives at this address (i.e. as a second document).

5.4.21 In practical terms, this means that, for face-to-face verification, production of a valid passport or photocard driving licence should enable most individuals to meet the identification requirement for AML/CFT purposes. The firm's risk-based procedures may dictate additional checks for the management of credit and fraud risk, or may restrict the use of certain options, e.g., restricting the acceptability of National Identity Cards in face-to-face business in the UK to cards issued only by EEA member states and Switzerland. For customers who cannot provide the standard evidence, other documents may be appropriate (see paragraphs 5.4.44 to 5.4.60).

5.4.22 Some consideration should be given as to whether the documents relied upon are forged. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity.

Electronic verification

5.4.23 If identity is verified electronically, this should be by the firm, using as its basis the customer's full name, address and date of birth, carrying out electronic checks either direct, or through a supplier which meets the criteria in paragraphs 5.3.17 and 5.3.18, that provide a reasonable assurance that the customer is who he says he is.

5.4.24 As well as requiring a commercial agency used for electronic verification to meet the criteria set out in paragraphs 5.3.17 and 5.3.18, it is important that the process of electronic verification meets a standard level of confirmation before it can be relied on. The standard level of confirmation, in circumstances that do not give rise to concern or uncertainty, is:

- one match on an individual's full name and current address, **and**
- a second match on an individual's full name and **either** his current address **or** his date of birth.

Commercial agencies that provide electronic verification use various methods of displaying results - for example, by the number of documents checked, or through scoring mechanisms. Firms should ensure that they understand the basis of the system they use, in order to be satisfied that the sources of the underlying data reflect the guidance in paragraphs 5.3.13-5.3.16, and cumulatively meet the standard level of confirmation set out above.

5.4.25 To mitigate the risk of impersonation fraud, firms should either verify with the customer additional aspects of his identity which are held electronically, or follow the guidance in paragraph 5.4.32.

Non face-to-face identification and verification

Regulation 4 (3) (b)

5.4.26 Many firms base their business model on accepting customers remotely, and do not offer them the option of attending the firm's premises. Firms are required, however, to take account of the greater potential for money laundering or terrorist financing which may arise when the customer is not physically present when being identified. This would include assessing the possibility that the customer is deliberately avoiding face-to-face contact. It is therefore important to be clear on the appropriate approach in these circumstances.

5.4.27 Whilst some types of financial transaction have traditionally been conducted on a non-face-to-face basis, other types of transaction and relationships are increasingly being undertaken in this way: e.g., internet and telephone banking, online share dealing.

5.4.28 Although applications and transactions undertaken across the internet may in themselves not pose any greater risk than other non face-to-face business, such as applications submitted by post, there are other factors that

may, taken together, aggravate the typical risks:

- the ease of access to the facility, regardless of time and location;
- the ease of making multiple fictitious applications without incurring extra cost or the risk of detection;
- the absence of physical documents; and
- the speed of electronic transactions.

5.4.29 The extent of verification in respect of non face-to-face customers will depend on the nature and characteristics of the product or service requested and the assessed money laundering risk presented by the customer. There are some circumstances where the customer is typically not physically present - such as in many wholesale markets, or when purchasing some types of collective investments - which would not in themselves increase the risk attaching to the transaction or activity. A firm should take account of such cases in developing their systems and procedures.

5.4.30 Where a customer approaches a firm remotely (by post, telephone or over the internet), the firm should carry out non face-to-face verification, either electronically (see paragraphs 5.4.23 -5.4.25), or by reference to documents (see paragraphs 5.4.17 – 5.4.22).

5.4.31 Non face-to-face identification and verification carries an inherent risk of impersonation fraud, and firms should follow the guidance in paragraph 5.4.32 to mitigate this risk.

Mitigation of impersonation risk

5.4.32 Where identity is verified electronically, or copy documents are relied on, a firm should apply an additional verification check to manage the risk of impersonation fraud. The additional check may consist of robust anti-fraud checks that the firm routinely undertakes as part of its existing procedures, or another measure, such as:

- requiring the first payment to be carried out through an account in the customer's name with a UK or EU regulated credit institution or one from a comparable jurisdiction;

- verifying additional aspects of the customer's identity, or of his electronic 'footprint' (see paragraph 5.3.1);

- telephone contact with the customer prior to opening the account on a home or business number which has been verified (electronically or otherwise), or a "welcome call" to the customer before transactions are permitted, using it to verify additional aspects of personal identity information that have been previously provided during the setting up of the account;

- communicating with the customer at an address that has been verified (such communication may take the form of a direct mailing of account opening documentation to him, which, in full or in part, might be required to be returned completed or acknowledged without alteration);

- internet sign-on following verification procedures where the

customer uses security codes, tokens, and/or other passwords which have been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address;

- requiring copy documents to be certified by an appropriate person.

Variation from the standard

5.4.33 The standard identification requirement (for documentary or electronic approaches) is likely to be sufficient for most situations. If, however, the customer, and/or the product or delivery channel, is assessed to present a higher money laundering or terrorist financing risk – whether because of the nature of the customer, or his business, or its location, or because of the product features available – the firm will need to decide whether it should require additional identity information to be provided, and/or whether to verify additional aspects of identity.

5.4.34 Where the result of the standard verification check gives rise to concern or uncertainty over identity, or other risk considerations apply, so the number of matches that will be required to be reasonably satisfied as to the individual's identity will increase.

5.4.35 For higher risk customers, the need to have additional information needs to be balanced against the possibility of instituting enhanced monitoring (see section 5.6 and Chapter 6).

Source of funds as evidence

5.4.36 Under certain conditions, where the money laundering or terrorist financing risk in a product is considered to be at its lowest, a payment drawn on an account with a UK or EU regulated credit institution, or one from a comparable jurisdiction, and which is in the sole or joint name of the customer, may satisfy the standard identification requirement. Whilst the payment may be made between accounts with regulated firms or by cheque or debit card, the accepting firm must be able to confirm that the payment (by whatever method) is from a bank or building society account in the sole or joint name(s) of the customer. Part II, sector 7: *Life assurance, and life-related pensions and investment products*, has an exception to this in respect of direct debits.

5.4.37 Whilst it is immaterial whether the transaction is effected remotely or face-to-face, each type of relationship or transaction that is entered into must be considered before determining that it is appropriate to rely on this method of verification. Firms will need to be able to demonstrate why they considered it to be reasonable to have regard to the source of funds as evidence in a particular instance.

5.4.38 One of the restrictions that will apply to a product that qualifies for using the source of funds as evidence will be an inability to make payments direct to, or to receive payments direct from, third parties. If, subsequent to using the source of funds to verify the customer's identity, the firm decides to allow such a payment or receipt to proceed, it should verify the identity of the third party. A further restriction would be that cash withdrawals should not be permitted, other than by the investors themselves, on a face-to-face basis where identity can be confirmed.

5.4.39 If a firm proposing to rely on the source of funds has reasonable grounds for believing that the identity of the customer has not been verified by the firm on which the payment has been drawn, it should not permit the source of funds to be used as evidence, and should verify the customer's identity in line with the appropriate standard requirement.

5.4.40 In some cases, the obligation to verify identity arises at the time of redemption, such as where, in respect of the previous transactions with the customer, the firm has been able to rely on a one-off transaction exemption. In these cases, depending on the assessment of risk presented by the customer, it may be possible to satisfy the standard identification requirement by means of a payment to an account in the sole or joint name of the customer.

5.4.41 If a firm has reason to suspect the motives behind a particular transaction, or believes that the business is being structured to avoid the standard identification requirement, it should not permit the use of the source of funds as evidence to identify the customer.

Executors and attorneys

5.4.42 Where an account is opened for the purpose of winding up the estate of a deceased person, firms may accept the court documents granting probate or letters of administration as evidence of identity of the executors/administrators of the estate. Lawyers and accountants acting in the course of their business as regulated firms, who are not named as executors/administrators, can be verified by reference to their practising certificates.

5.4.43 The authority to deal with assets under a power of attorney constitutes a business relationship. Consequently, the identity of holders of powers of attorney, as well as the principals they represent, should be verified. Except where the attorney is a solicitor acting in the normal course of a client relationship, it is important to ascertain the reason for the granting of the power of attorney. Any new arrangements should always be recorded and new appointees should be verified.

Customers who cannot provide the standard evidence

5.4.44 Some customers may not be able to produce identification information equivalent to the standard. Such cases may include, for example, some low-income customers in rented accommodation, customers with a legal, mental or physical inability to manage their affairs, individuals dependent on the care of others, dependant spouses or minors, students, refugees and asylum seekers, migrant workers and prisoners. The firm will therefore need an approach that compensates for the difficulties that such customers

may face in providing the standard evidence of identity.

SYSC 3.2.6G(5) G Promoting Financial Inclusion, December 2004

5.4.45 The FSA Rules adopt a broad view of financial exclusion, in terms of ensuring that, where people cannot reasonably be expected to produce standard evidence of identity, they are not unreasonably denied access to financial services. The term is sometimes used in a narrower sense, for example, HM Treasury refers to those who, for specific reasons, do not have access to mainstream banking or financial services - that is, those at the lower end of income distribution who are socially/financially disadvantaged and in receipt of benefits, or those who chose not to seek access to financial products because they believed that they will be refused.

5.4.46 Firms offering financial services directed at the financially aware may wish to consider whether any apparent inability to produce standard levels of identification evidence is consistent with the targeted market for these products.

5.4.47 As a first step, before concluding that a customer cannot produce evidence of identity, firms will have established that the guidance on initial identity checks for personal customers set out in paragraphs 5.4.15 to 5.4.32 cannot reasonably be applied.

5.4.48 Guidance on verifying the identity of most categories of customers who cannot provide the standard evidence is given in Part II, sector 1: *Retail banking*. Guidance on cases with more general application is given in paragraphs 5.4.50 to 5.4.60.

5.4.49 Where a firm concludes that an individual customer cannot reasonably meet the standard identification requirement, and that the provisions in Part II, sector 1: *Retail banking*, Annex 1-I, cannot be met, it may accept as identification evidence a letter or statement from an appropriate person who knows the individual, that indicates that the person is who he says he is.

Persons without standard documents, in care homes, or in receipt of pension

5.4.50 An entitlement letter from the DWP, or a letter from the DWP confirming that the person is in receipt of a pension, could provide evidence of identity. If this is not available, or is inappropriate, a letter from an appropriate person, for example, the matron of a care home, may provide the necessary evidence.

Those without the capacity to manage their financial affairs

5.4.51 Guidance on dealing with mentally incapacitated customers, and customers with learning difficulties, covering Enduring Power of Attorney (EPA); Receivership (or short) order; and Appointeeship, and a BBA leaflet, "Banking for mentally incapacitated customers", can be obtained from the British Bankers' Association at www.bba.org.uk.

Gender reassignment

5.4.52 A firm should satisfy itself (for example, on the basis of documentary medical evidence) that the gender transfer of a customer is genuine (as with a change of name). Such cases usually involve transferring a credit history to a reassigned gender. This involves data protection, not money

laundering issues. The consent of the person involved is necessary.

Students and young people

5.4.53 When opening accounts for students or other young people, the standard identification requirement should be followed as far as possible. In practice, it is likely that many students, and other young people, will have a passport, and possibly a driving licence. Where the standard requirement would not be relevant, however, or where the customer cannot satisfactorily meet this, other evidence could be obtained by obtaining appropriate confirmation(s) from the applicant's workplace, school, college, university or care institution (see DfES website www.dfes.gov.uk/providersregister/). Any confirmatory letter should be on appropriately headed notepaper; in assessing the strength of such confirmation, firms should have regard to the period of existence of the educational or other institution involved, and whether it is subject to some form of regulatory oversight.

5.4.54 Guidance on identification for international students is available on the JMLSG website (see International Students: Basic Bank Account Opening Procedures - 12 August 2005). Guidance on the money laundering aspects of Child Trust Funds is also available at www.jmlsg.org.uk.

5.4.55 Often, a business relationship in respect of a minor will be established by a family member or guardian. In cases where the adult opening the account or establishing the relationship does not already have an existing relationship with the firm, the identity of that adult should be verified and, in addition, the firm should see one of the following in the name of the child:

- birth certificate
- passport
- NHS Medical Card
- Child benefit documentation
- Child Tax Credit documentation
- National Insurance Card (for those aged 16 and over)

Financially excluded

5.4.56 Further guidance on verifying the identity of financially excluded persons is given in Part II, sector 1: *Retail banking*, paragraphs 1.38 – 1.41. A proportionate and risk-based approach will be needed to determine whether the evidence available gives reasonable confidence as to the identity of a customer.

5.4.57 Where a firm has concluded that it should treat a customer as financially excluded for the purposes of customer identification, and the customer is identified by means other than standard evidence, the reasons for doing so should be documented.

5.4.58 The "financially excluded" are not a homogeneous category of uniform risk. Some financially excluded persons may represent a higher risk of money laundering regardless of whether they provide standard or non-

standard tokens to confirm their identity, e.g., a passport holder who qualifies only for a basic account on credit grounds. Firms may wish to consider whether any additional KYC information (see section 5.6) or monitoring (see Chapter 6) of the size and expected volume of transactions would be useful in respect of some financially excluded categories, based on the firm's own experience of their operation.

5.4.59 In other cases, where the available evidence of identity is limited, and the firm judges that the individual cannot reasonably be expected to provide more, but that the business relationship should nevertheless go ahead, it should consider instituting enhanced monitoring arrangements over the customer's transactions and activity (see Chapter 6). In addition, the firm should consider whether restrictions should be placed on the customer's ability to migrate to other, higher risk products or services.

5.4.60 Where an applicant produces non-standard documentation, staff should be discouraged from citing the ML Regulations as an excuse for not opening an account without giving proper consideration to the evidence available, referring up the line for advice as necessary. It may be that at the conclusion of that process a considered judgement may properly be made that the evidence available does not provide a sufficient level of confidence that the applicant is who he claims to be, in which event a decision not to open the account would be fully justified. Firms should bear in mind that the ML Regulations are not explicit as to what is and is not acceptable evidence of identity.

Non-personal customers

5.4.61 Non-personal entities may be registered in the names of specific individuals or other entities. The beneficial ownership may, however, rest with others, either because the legal owner is acting for the beneficial owner, or because there is a legal obligation for the ownership to be registered in a particular way.

Regulation 4 (3) (d)

5.4.62 In deciding who the customer is in non-personal cases, the firm's objective must be to know who has control over the funds which form or otherwise relate to the relationship, and/or form the controlling mind and/or management of any legal entity involved in the funds. The subsequent judgement as to whose identity to verify will be made following a risk-based approach, and will take account of the number of individuals, the nature and distribution of their interests in the entity and the nature and extent of any business, contractual or family relationship between them.

5.4.63 Certain information about the entity comprising the non-personal customer should be obtained as a standard requirement. Thereafter, on the basis of the money laundering/terrorist financing risk assessed in the customer/product/delivery channel combination, a firm should decide the extent to which the identity of the entity and of specific individuals should be verified, using reliable, independent source documents, data or information. The firm should also decide what additional information in respect of the entity and, potentially, some of the individuals behind it, should be obtained (see section 5.6).

5.4.64 Many entities, both in the UK and elsewhere, operate internet websites, which contain information about the entity. Firms should bear in mind that this information, although helpful in providing much of the material that a firm might need in relation to the company, its directors and business, is not independently verified before being made publicly available in this way.

5.4.65 This section provides guidance on verifying the identity of a range of non-personal entities, as follows:

- Corporates (other than regulated firms) (paragraphs 5.4.66 to 5.4.92)
- HMRC -approved pension schemes (paragraphs 5.4.93 to 5.4.99)
- Charities, church bodies and places of worship (paragraphs 5.4.100 to 5.4.110)
- Other trusts, foundations and similar entities (paragraphs 5.4.111 to 5.4.123)
- Other regulated financial services firms subject to the ML Regulations (paragraphs 5.4.124 to 5.4.127)
- Other firms subject to the ML Regulations (paragraphs 5.4.128 to 5.4.131)
- Partnerships and unincorporated businesses (paragraphs 5.4.132 to 5.4.142)
- Clubs and societies (paragraphs 5.4.143 to 5.4.150)

- Public sector bodies, governments, state-owned companies and supranationals (paragraphs 5.4.151 to 5.4.161)

Corporates (other than regulated firms)

5.4.66 To the extent consistent with the risk assessment carried out in accordance with the guidance in Chapter 4, the firm should ensure that it fully understands the company's legal form, structure and ownership, and should obtain sufficient additional information on the nature of the company's business, and the reasons for seeking the product or service.

5.4.67 Corporate customers may be publicly accountable in several ways. Some public companies are listed on stock exchanges or other regulated markets, and are subject to market regulation and to a high level of public disclosure in relation to their ownership and business activities. Other public companies are unlisted, but are still subject to a high level of disclosure through public filing obligations. Private companies are not generally subject to the same level of disclosure, although they may often have public filing obligations. In their verification processes, firms should take account of the availability of public information in respect of different types of company.

5.4.68 The structure, ownership, purpose and activities of many corporates will be clear and understandable. Corporate customers can use complex ownership structures, which can increase the steps that need to be taken to be reasonably satisfied as to their identities; this does not necessarily indicate money laundering or terrorist financing. The use of complex structures without an obvious legitimate commercial purpose may, however, give rise to concern and increase the risk of money laundering or terrorist financing.

5.4.69 Paragraphs 5.4.70 – 5.4.73 refer to the standard evidence for corporate customers, and paragraphs 5.4.74 – 5.4.92 provide further supplementary guidance on steps that may be applied as part of a risk-based approach.

Obtain standard evidence

5.4.70 The firm should obtain the following in relation to the corporate concerned:

- full name
- registered number
- registered office in country of incorporation
- business address

and, additionally, for private companies:

- names of all directors (or equivalent)
- names of beneficial owners holding over 25%

5.4.71 The firm should verify the identity of the corporate from:

either a search of the relevant company registry

or confirmation of the company's listing on a regulated market

or a copy of the company's Certificate of Incorporation

5.4.72 Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer and is who he says he is.

5.4.73 Some consideration should be given as to whether documents relied upon are forged. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity.

Variation from the standard

5.4.74 The standard evidence is likely to be sufficient for most corporate customers. If, however, the customer, or the product or delivery channel, is assessed to present a higher money laundering or terrorist financing risk – whether because of the nature of the customer, its business or its location, or because of the product features available – the firm will need to decide whether it should require additional identity information to be provided and/or verified.

5.4.75 Higher risk corporate customers may be, among others, smaller and more opaque entities, with little or no industry profile and those in less transparent jurisdictions, taking account of issues such as their size, industry profile, industry risk.

5.4.76 Where an entity is known to be linked to a PEP, or to a jurisdiction assessed as carrying a higher money laundering/terrorist financing risk, or where the company is engaged in activities that are assessed to carry a higher money laundering risk, further verification and/or monitoring may be required (see section 5.6 and Chapter 6).

Publicly quoted companies

5.4.77 Corporate customers that are listed on a regulated market are publicly owned and generally accountable. Corporate customers that are subject to statutory licensing and regulation of their industry (for example, energy, telecommunications) may be considered to be similarly owned and accountable.

5.4.78 Where the firm has satisfied itself that the customer is:

- a publicly quoted company, subject to public disclosure rules; or
- a majority-owned and consolidated subsidiary of such a publicly quoted company; or
- subject to the licensing and prudential regulatory regime of a statutory regulator (e.g., OFGEM, OFWAT, OFCOM)

it need take no further steps to verify identity over and above obtaining the standard evidence.

5.4.79 If a regulated market is located in the UK, the EU, or in a comparable jurisdiction (see the JMLSG website www.jmlsg.org.uk), there is no requirement to undertake checks on the market itself. Firms should, however, record the steps they have taken to ascertain the status of the market.

Private companies

5.4.80 Unlike publicly quoted companies, the activities of private companies are often carried out for the profit/benefit of a small and defined group of individuals or entities. Such firms are also subject to a lower level of public disclosure than public companies. In general, however, the structure, ownership, purposes and activities of many private companies will be clear and understandable.

5.4.81 Where private companies are well known, reputable organisations, with long histories in their industries and substantial public information about them, the standard evidence may well be sufficient to meet the firm's obligations.

5.4.82 In the UK, a company registry search will confirm that the applicant company has not been, or is not in the process of being, dissolved, struck off or wound up. In the case of non-UK companies, firms should make similar search enquiries of the registry in the country of incorporation of the applicant for business.

5.4.83 Standards of control over the issue of documentation from company registries vary between different countries. Attention should be paid to the jurisdiction the documents originate from and the background against which they are produced.

5.4.84 Whenever faced with less transparency, less of an industry profile, or less independent means of verification of the client entity, firms should consider the money laundering or terrorist financing risk presented by the entity, and therefore the extent to which, in addition to the standard evidence, they should verify the identities of the principal beneficial owners, shareholders and/or controllers. It is important to know and understand any associations the entity may have with other jurisdictions (headquarters, operating facilities, branches, subsidiaries, etc) and the individuals who may influence its operations (political connections, etc). A visit to the place of business may be helpful to confirm the existence and activities of the entity.

5.4.85 Firms may find the sectoral guidance in Part II helpful in understanding some of the business relationships that may exist between the customer and other entities in particular business areas.

Directors

5.4.86 Following the firm's assessment of the money laundering or terrorist financing risk presented by the company, it may decide to verify the identity of one or more directors, as appropriate, in accordance with the

guidance for personal customers (paragraphs 5.4.15 to 5.4.60). In that event, verification is likely to be appropriate for those who have authority to operate an account or to give the firm instructions concerning the use or transfer of funds or assets, but might be waived for other directors.

Beneficial owners

5.4.87 Control over companies may be exercised through a direct shareholding or through intermediate holding companies. As part of the standard evidence, the firm will know the names of all individual beneficial owners of private companies holding 25% or more, even where these interests are held indirectly.

5.4.88 Following the firm's assessment of the money laundering or terrorist financing risk presented by the company, the firm may feel it appropriate to verify the identity of appropriate beneficial owners holding 25% or more. Where a principal owner is another corporate entity or trust, the firm should take measures to look behind that company or trust and establish the identities of its beneficial owners or trustees, unless that company is publicly quoted. The firm will then judge which of the beneficial owners exercise effective control, and whose identities should therefore be verified.

5.4.89 Control may also rest with those who have power to manage funds or transactions without requiring specific authority to do so, and who would be in a position to override internal procedures and control mechanisms. Firms should make an evaluation of the effective distribution of control in each case. What constitutes a significant shareholding or control for this purpose will depend on the nature of the company, the distribution of shareholdings, and the nature and extent of any business or family connections between the beneficial owners.

5.4.90 Extra care must be taken in the case of companies with capital in the form of bearer shares, because in such cases it is often difficult to identify the beneficial owner(s). Companies that issue bearer shares are frequently incorporated in high risk jurisdictions. Firms should adopt procedures to establish the identities of the holders and material beneficial owners of such shares and to ensure that they are notified whenever there is a change of holder and/or beneficial owner.

5.4.91 As a minimum, these procedures should require a firm to obtain an undertaking in writing from the beneficial owner which states that immediate notification will be given to the firm if the shares are transferred to another party. Depending on its risk assessment of the client, the firm may consider it appropriate to have this undertaking certified by an accountant, lawyer or equivalent, or even to require that the shares be held by a named custodian, with an undertaking from that custodian that the firm will be notified of any changes to records relating to these shares and the custodian.

Signatories

5.4.92 For operational purposes, the firm is likely to have a list of those

authorised to give instructions for the movement of funds or assets, along with an appropriate instrument authorising one or more directors (or equivalent) to give the firm such instructions. The identities of individual signatories need only be verified on a risk-based approach.

HMRC-approved pension schemes

5.4.93 UK pension schemes can take a number of legal forms. Some may be companies limited by guarantee; some may take the form of trusts; others may be unincorporated associations. Many obtain HMRC approval in order to achieve tax-exempt status.

Obtain standard evidence

5.4.94 Where a pension scheme has HMRC approval, a firm's identification obligation may be met by confirming the scheme's approval.

5.4.95 In other cases, a pension scheme should be treated for AML/CFT purposes, and standard evidence obtained, according to its legal form.

Signatories

5.4.96 For operational purposes, the firm is likely to have a list of those authorised to give instructions for the movement of funds or assets, along with an appropriate instrument authorising one or more directors (or equivalent) to give the firm such instructions. The identities of individual signatories need only be verified on a risk-based approach.

Variation from the standard

5.4.97 The identity of the principal employer should be verified in accordance with the guidance given for companies in paragraphs 5.4.66 to 5.4.92 and the source of funding recorded to ensure that a complete audit trail exists if the employer is wound up.

Payment of benefits

5.4.98 Any payment of benefits by, or on behalf of, the trustees of an occupational pension scheme will not require verification of identity of the recipient. (The transaction will either not be relevant financial business or will be within the scope of the exemption for policies of insurance in respect of occupational pension schemes.)

5.4.99 Where individual members of an occupational pension scheme are to be given personal investment advice, their identities must be verified. However, where the trustees and principal employer have been satisfactorily identified (and the information is still current), it may be appropriate for the employer to provide confirmation of identities of individual employees.

Charities, church bodies and places of worship

5.4.100 Charities have their status because of their purposes, and can take a number of legal forms. Some may be companies limited by guarantee; some may take the form of trusts; others may be unincorporated associations.

Obtain standard evidence

5.4.101 In each case, a charity should be treated for AML/CFT purposes, and standard evidence obtained, according to its legal form.

5.4.102 Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer and is who he says he is.

Registered charities – England and Wales, and Scotland

5.4.103 The Charity Commission is required to hold a central register of charities in England and Wales and allocates a registered number to each. The Office of the Scottish Charity Regulator carries out a similar function for Scottish charities. When dealing with an application which includes the name of a registered charity, the Charity Commission, or the Office of the Scottish Charity Regulator, can confirm the registered number of the charity and the name and address of the regulator's correspondent for the charity concerned. Details of all registered charities can be accessed on the Charity Commission website (www.charity-commission.gov.uk), the Office of the Scottish Charity Regulator website (www.oscr.org.uk), or a check can be made by telephone to the respective regulator's enquiry line (see JMLSG website www.jmlsg.org.uk). Firms should be aware that simply being registered is not in itself a guarantee of the bona fides of an organisation, although it does indicate that it is subject to some ongoing regulation.

Charities in Northern Ireland

5.4.104 Applications from, or on behalf of, charities in Northern Ireland should be dealt with in accordance with procedures for private companies set out in paragraphs 5.4.80 to 5.4.92, if they are limited by guarantee, and for clubs and societies, those in paragraphs 5.4.143 to 5.4.150. Verification of the charitable status can normally be obtained through HMRC.

Church bodies and places of worship

Registered Places of Worship Act 1855

5.4.105 Places of worship (other than the Church of England, which is a registered charity) are in general exempted by law from registering as charities and may not therefore have a registered number. Instead, they can apply for a certified building of worship from the General Register Office (GRO). For tax purposes, however, they may notify HMRC of their charitable status; verification of their status may therefore be obtained through HMRC. Their identity may be verified by reference to the GRO certificate, or, where appropriate, through the headquarters or regional organisation of the denomination, or religion.

Schools and colleges

5.4.106 Where an independent school or college is a registered charity, it should be treated in accordance with the guidance for charities. Any such body which is not registered as a charity should be treated in accordance with the guidance for private companies in paragraphs 5.4.80 to 5.4.92.

Variation from the standard

5.4.107 The identities of unregistered charities or church bodies, whether in the UK or elsewhere, cannot be verified by reference to registers maintained by independent bodies. Applications from, or on behalf of, unregistered charities should therefore be dealt with in accordance with the procedures for private companies set out in paragraphs 5.4.80 to 5.4.92, for trusts, as set out in paragraphs 5.4.111 to 5.4.123, or for clubs and societies, as set out in paragraphs 5.4.143 to 5.4.150. Firms should take particular note of those paragraphs addressing customers where the money laundering or terrorist financing risk is greater in relation to particular customers, and if it should be followed in these circumstances.

5.4.108 In assessing the risks presented by different charities, a firm should make appropriate distinction between those with a limited geographical remit; and those with unlimited geographical scope, such as medical and emergency relief charities.

5.4.109 If they have a defined area of benefit, charities are only able to expend their funds within that defined area. If this area is an overseas country or jurisdiction, the charity can quite properly be transferring funds to that country or jurisdiction. It would be less clear why the organisation should be transferring funds to a third country (which may, within the general context of the firm's risk assessment have a lower profile) and this would therefore be unusual. Such activity would lead to the charity being regarded as higher risk.

5.4.110 Non-profit organisations have been known to be abused, to divert funds to terrorist financing and other criminal activities. FATF published a paper 'Combating the abuse of non-profit organisations - International Best Practices' in October 2002 (available on the publications link on the FATF website www.fatf-gafi.org), in support of Special Recommendation VIII. In November 2005, the European Commission adopted a Recommendation to member states containing a Framework for a code of conduct for non-profit organisations. The Recommendation is available on the JMLSG website www.jmlsg.org.uk.

Other trusts, foundations and similar entities

5.4.111 There is a wide variety of trusts, ranging from large, nationally and internationally active organisations subject to a high degree of public interest and quasi-accountability, through trusts set up under testamentary arrangements, to small, local trusts funded by small, individual donations from local communities, serving local needs. It is important, in putting proportionate AML/CFT processes into place, and

in carrying out their risk assessments, that firms take account of the different money laundering or terrorist financing risks that trusts of different sizes and areas of activity present.

5.4.112 Most trusts are not separate legal entities – it is the trustees collectively who are the customer. In these cases, the obligation to identify the customer attaches to the trustees, rather than to the trust itself. The purpose and objects of most trusts are set out in a trust deed.

Obtain standard evidence

5.4.113 In respect of trusts, the firm should obtain the following information:

- Full name of the trust
- Nature and purpose of the trust (e.g., discretionary, testamentary, bare)
- Country of establishment
- Names of all trustees
- Name and address of any protector or controller

5.4.114 The firm should verify the identities of the trustees (or equivalent) who have authority to operate an account or to give the firm instructions concerning the use or transfer of funds or assets.

5.4.115 Where a trustee is itself a regulated entity, or a publicly quoted company, or other type of entity, the identification procedures that should be carried out should reflect the standard approach for such an entity.

5.4.116 Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer and is who he says he is.

5.4.117 Some consideration should be given as to whether documents relied upon are forged. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity.

Variation from the standard

5.4.118 Firms should make appropriate distinction between those trusts that serve a limited purpose (such as inheritance tax planning) or have a limited range of activities and those where the activities and connections are more sophisticated, or are geographically based and/or with financial links to other countries.

5.4.119 For trusts presenting a lower money laundering or terrorist financing risk, the standard evidence will be sufficient. However, less transparent and more complex structures, with numerous layers, may pose a higher money laundering or terrorist financing risk. Also, some trusts established in jurisdictions with favourable tax regimes have in the past been associated with tax evasion and money laundering. In respect of trusts in the latter category, the firm's risk assessment may lead it to require additional information on the purpose, funding and beneficiaries of the trust.

5.4.120 Where a trust is assessed as carrying a higher risk of money laundering or terrorist financing, the firm should carry out a higher level of verification:

either by searching an appropriate register maintained in the country of establishment,

or by obtaining a summary of the instrument establishing the trust.

5.4.121 Other information that might be appropriate to ascertain for higher risk customers includes:

- Donor/settler/grantor of the funds (except where there are large numbers of small donors)
- Domicile of business/activity
- Nature of business/activity
- Location of business/activity (operating address)
- Names, or classes, of beneficiaries

5.4.122 Following its assessment of the money laundering risk presented by the trust, the firm may decide to verify the identities of additional trustees, and/or of the settler(s) and beneficiaries.

Non-UK trusts

5.4.123 The guidance in paragraphs 5.4.111 to 5.4.122 applies equally to UK based trusts and non-UK based trusts. On a risk-based approach, a firm will need to consider whether the geographical location of the trust gives rise to additional concerns, and if so, what they should do.

Other regulated financial services firms that are subject to the ML Regulations

Regulation 5(2)

5.4.124 The identities of other financial services firms which are subject to the ML Regulations or equivalent, and which are regulated in the UK by the FSA, or in the EU or a comparable jurisdiction, by an equivalent regulator, do not need to be verified.

5.4.125 Firms should, however, make enquiries to establish that the customer is in fact regulated. To assist firms, a list of the regulatory authorities in EU and FATF member states is available on the JMLSG website www.jmlsg.org.uk.

5.4.126 Firms should record the steps they have taken to check the status of the other regulated firm.

5.4.127 Firms should take appropriate steps to be reasonably satisfied that the person they are dealing with is properly authorised by the customer and is who he says he is.

Other firms that are subject to the ML Regulations

5.4.128 Customers which are subject to the ML Regulations or equivalent, but which are not regulated in the UK, the EU or a comparable jurisdiction as a financial services business, should be treated, for AML/CFT purposes, according to their legal form: for example, as private companies, in accordance with the guidance set out in paragraphs 5.4.80 to 5.4.92; or if partnerships, by confirming their regulated status through reference to the current membership directory of the relevant professional association (for example, law society or accountancy body). However, when they are acting in their personal capacity, for example, as trustees, their identity should normally be verified as for any other individual acting in that capacity.

5.4.129 Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer and is who he says he is.

5.4.130 Some consideration should be given as to whether documents relied upon are forged. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity.

5.4.131 Where professional firms that are subject to the ML Regulations hold client money, they are obliged to verify the identities of their clients. Under client confidentiality rules, it may not be possible for the firm holding the client account to establish the identity of the person(s) for whom a solicitor or accountant is acting. Firms will therefore need to take a commercial decision, based on their knowledge of the intermediary, as to the nature and extent of the business that they are prepared to conduct if the professional firm is not willing to identify the underlying clients concerned. Firms should be prepared to make reasonable enquiries about transactions passing through client accounts that give cause for concern, and should report any transactions where suspicions cannot be satisfied.

Partnerships and unincorporated businesses

5.4.132 Partnerships and unincorporated businesses, although principally operated by individuals, or groups of individuals, are different from personal customers in that there is an underlying business. This business is likely to have a different money laundering or terrorist financing risk profile from that of an individual.

Obtain standard evidence

5.4.133 Where partnerships or unincorporated businesses are well known, reputable organisations, with long histories in their industries, and with substantial public information about them and their principals and controllers, the standard evidence for publicly quoted companies will be sufficient to meet the firm's obligations.

5.4.134 Professional firms that are partnerships, and that are subject to the ML

Regulations, the EU Money Laundering Directive, or comparable legislation, should be treated as set out under paragraphs 5.4.128 – 5.4.131.

5.4.135 Other partnerships and unincorporated businesses should be treated as private companies, as set out in paragraphs 5.4.80 to 5.4.92.

5.4.136 For identification purposes, Scottish partnerships, limited partnerships and limited liability partnerships should be treated as corporate customers.

5.4.137 Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer and is who he says he is.

5.4.138 Some consideration should be given as to whether documents relied upon are forged. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity.

Variation from the standard

5.4.139 Most partnerships and unincorporated businesses are smaller, less transparent, and less well known entities, and are not subject to the same accountability requirements as, for example, listed companies.

5.4.140 Where the money laundering or terrorist financing risk is considered to be at its lowest, the firm may be able to use the source of funds as evidence of the customer's identity. The guidance in paragraphs 5.4.36 to 5.4.41 should be followed.

5.4.141 Whenever faced with less transparency, less of an industry profile, or less independent means of verification of the client entity, firms should consider the money laundering or terrorist financing risk presented by the entity, and therefore the extent to which, in addition to the standard evidence, they should verify the identity of the principal beneficial owners, shareholders and/or controllers. It is important to know and understand any associations the entity may have with other jurisdictions (headquarters, operating facilities, branches, subsidiaries, etc) and the individuals who may influence its operations (political connections, etc). A visit to the place of business may be helpful to confirm the existence and activities of the business.

Principals and beneficial owners

5.4.142 Following its assessment of the money laundering or terrorist financing risk presented by the entity, the firm may decide to verify the identity of one or more of the partners/owners. In that event, verification requirements are likely to be appropriate for partners/owners who have authority to operate an account or to give the firm instructions concerning the use or transfer of funds or assets, but might be waived for other partners/owners.

Clubs and societies

5.4.143 Where an application is made on behalf of a club or society, firms should make appropriate distinction between those that serve a limited social or regional purpose and those where the activities and connections are more sophisticated, or are geographically based and/or with financial links to other countries.

Obtain standard evidence

5.4.144 For many clubs and societies, the money laundering or terrorist financing risk will be low. The following information should be obtained about the customer:

- Full name of the club/society
- Legal status of the club/society
- Purpose of the club/society
- Names of all officers

5.4.145 The firm should verify the identities of the officers who have authority to operate an account or to give the firm instructions concerning the use or transfer of funds or assets.

5.4.146 Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer and is who he says he is.

5.4.147 Some consideration should be given as to whether documents relied upon are forged. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity.

Variation from the standard

5.4.148 Where the money laundering or terrorist financing risk is considered to be at its lowest, the firm may be able to use the source of funds as evidence of the customer's identity. The guidance in paragraphs 5.4.36 to 5.4.41 should be followed.

5.4.149 The firm's risk assessment may lead it to conclude that the money laundering or terrorist financing risk is higher, and that it should require additional information on the purpose, funding and beneficiaries of the club or society. This might include seeing a copy of the constitution (or equivalent) of the club or society.

5.4.150 Following its assessment of the money laundering or terrorist financing risk presented by the club/society, the firm may decide to verify the identities of additional officers, and/or institute additional transaction monitoring arrangements (see Chapter 6).

Public sector bodies, governments, state-owned companies and supranationals

5.4.151 In respect of customers which are UK or overseas governments (or their representatives), supranational organisations, government departments, state-owned companies or local authorities, the approach to identification and verification has to be tailored to the circumstances of the customer. Public sector bodies include schools, colleges, universities and NHS trusts.

Obtain standard evidence

5.4.152 Firms should obtain the following information about customers who are public sector bodies, governments, state-owned companies and supranationals:

- Full name of the entity
- Nature and status of the entity [e.g., overseas government, treaty organisation]
- Address of the entity
- Name of the home state authority
- Names of directors (or equivalent)

5.4.153 Firms should take appropriate steps to understand the ownership of the customer, and the nature of its relationship with its home state authority.

5.4.154 Firms should, where appropriate, verify the identities of the directors (or equivalent) who have authority to give the firm instructions concerning the use or transfer of funds or assets.

5.4.155 Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer and is who he says he is.

Signatories

5.4.156 For operational purposes, the firm is likely to have a list of those authorised to give instructions for the movement of funds or assets, along with an appropriate instrument authorising one or more directors (or equivalent) to give the firm such instructions. The identities of individual signatories need only be verified on a risk-based approach.

Schools, colleges and universities

5.4.157 Schools, colleges and universities should be treated as public sector bodies, in accordance with the guidance set out in paragraphs 5.4.152 to 5.4.156. The Department for Education and Skills maintains lists [www.dfes.gov.uk/providersregister] of approved educational establishments, which may assist firms in verifying the existence of such customers.

5.4.158 For independent schools and colleges, firms should refer to the guidance given at paragraph 5.4.106.

Variation from the standard

5.4.159 The firm's assessment of the money laundering or terrorist financing risk presented by such customers should aim to identify higher risk countries or jurisdictions.

5.4.160 The guidance in paragraphs 5.4.152 to 5.4.158 should be applied to overseas entities, as appropriate to the firm's assessment of the risk that such entities present.

5.4.161 Many governmental, supranational and state-owned organisations will be managed and controlled by individuals who may qualify as PEPs (see paragraphs 5.6.12 to 5.6.18). Firms need to be aware of the increased likelihood of the existence of such individuals in the case of such applicants, and deal with them appropriately, having regard to the risk that the funds of such entities may be used for improper purposes.

5.5 Multipartite relationships

5.5.1 Frequently, a customer may have contact with two or more firms in respect of the same transaction. This can be the case in both the retail market, where customers are routinely introduced by one firm to another, or deal with one firm through another, and in some wholesale markets, such as syndicated lending, where several firms may participate in a single loan to a customer.

5.5.2 However, several firms requesting the same information from the same customer in respect of the same transaction not only does not help in the fight against financial crime, but also adds to the inconvenience of the customer. It is important, therefore, that in all circumstances each firm is clear as to its relationship with the customer and its related AML/CFT obligations, and as to the extent to which it needs to take account of the verification of the customer that another firm has carried out. Such account must be taken in a balanced way that appropriately reflects the money laundering or terrorist financing risks. Account must also be taken of the fact that some of the firms involved may not be UK-based.

5.5.3 How one firm should take account of the work carried out by other firms is not a one-dimensional issue. It is not possible to generalise about how the various responsibilities may be met; as well as giving guidance in some areas of more limited application, this guidance draws on a number of stylised examples of such cases, allowing firms to apply these as appropriate to their own situation.

One firm acting solely as introducer

5.5.4 At one end of the spectrum, one firm may act solely as an introducer between the customer and the firm providing the product or service, and may have no further relationship with the customer. The introducer plays no part in the transaction between the customer and the firm, and has no relationship with either of these parties that would constitute a business relationship. This would be the case, for example, in respect of name-passing brokers in inter-professional markets, on which specific guidance is given in Part II, sector 19: *Name passing brokers in the inter-professional market.*

5.5.5 In these circumstances, where the introducer neither gives advice nor plays any part in the negotiation or execution of the transaction, the identification and verification obligations under the ML Regulations lie with the product/service provider. This does not, of course, preclude the introducing firm carrying out identification and verification of the customer on behalf of the firm providing the product or service, as agent for that firm.

Other multipartite relationships

5.5.6 There are a number of other situations where there can be contact between a customer and two or more firms. Some of these situations can be straightforward, whilst others can be complex, involving several firms with a range of interests in the customer and/or the transaction. Some of these situations occur commonly; others are of more restricted application.

5.5.7 Three cases where the relationships may be stylised are:

(i) where a customer enters into a transaction with a product/service provider through an intermediary who is an agent of the provider
(ii) where a customer, using an intermediary as his agent, enters into a transaction with the product/service provider
(iii) where a customer, advised by an intermediary, enters into a transaction or relationship with a product/service provider

5.5.8 In other cases, a customer may be an existing customer of another regulated firm in the same group. Guidance on meeting AML/CFT obligations in this relationship is given in paragraphs 5.5.22 to 5.5.25.

5.5.9 In a more specialist situation, a customer may have the execution and settlement aspects of the same transaction dealt with by different firms. Guidance on meeting AML/CFT obligations in this relationship is given in Part II, sector 18: *Wholesale markets*.

(i) Where the intermediary is the agent of the product/service provider

Regulation 6 (5)

5.5.10 If the intermediary is an agent or appointed representative of the product or service provider, it is an extension of that firm. The intermediary may actually obtain the appropriate verification evidence in respect of the customer, but the product/service provider is responsible for specifying what should be obtained, and for ensuring that records of the appropriate verification evidence taken in respect of the customer are retained.

5.5.11 Similarly, where the product/service provider has a direct sales force, they are part of the firm, whether or not they operate under a separate group legal entity. The firm is responsible for specifying what is required, and for ensuring that records of the appropriate verification evidence taken in respect of the customer are retained.

(ii) Where the intermediary is the agent of the customer

5.5.12 From the point of view of a product/service provider, the position of an intermediary, as agent of the customer, is influenced by a number of factors. The intermediary may be subject to the ML Regulations, or otherwise to the EU Money Laundering Directive, or to similar legislation in a comparable jurisdiction. It may be regulated; it may be based in the UK, elsewhere within the EU, or in a country or jurisdiction outside the EU, which may or may not be a FATF member. Guidance on which countries or jurisdictions are "comparable jurisdictions" is given on the JMLSG website at www.jmlsg.org.uk.

Regulation 5 (2)

5.5.13 Where the intermediary is carrying on appropriately regulated business (see below), and is acting on behalf of a customer (whether or not the customer's name is disclosed to the product or service provider), there is no obligation on the provider firm to identify the customer. Where the firm takes instruction from the underlying customer, however, the firm does have such an obligation. This paragraph only applies where the intermediary meets the following criteria:

(a) In the case of a UK firm, it must be:
- authorised by the FSA and carrying on relevant business within the meaning of Regulation 2(2)(a); or
- the National Savings Bank or carrying on business under the auspices of the Director of National Savings for the purposes of raising money under the National Loans Act 1968; or
- otherwise subject to the Banking Consolidation Directive and carrying on one of the activities set out in Schedule 1 to the Regulations.

(b) In the case of non-UK firm, it must be:
- carrying on business comparable to that described in (a) above; and
- regulated by a relevant overseas regulatory authority and subject to the Money Laundering Directive or similar legislation in a comparable jurisdiction.

Regulation 5(2)
Regulation 4(3)(d)

5.5.14 Where the intermediary is unregulated, or is regulated in a country that is not a comparable jurisdiction, or is regulated for business that is not financial services business, the product/service provider is obliged to verify the identity of the intermediary and, as the intermediary acts for another, the identity of the underlying customer.

5.5.15 In these circumstances, in verifying the identity of the underlying customer, the firm should take a risk-based approach. It will need to assess the AML/CFT regime in the intermediary's jurisdiction, the level of reliance that can be placed on the intermediary and the verification work it has carried out, and as a consequence, the amount of evidence that should be obtained direct from the customer.

5.5.16 In particular, where the intermediary is located in a higher risk jurisdiction, or in a country listed as having material deficiencies [www.jmlsg.org.uk], the risk-based approach should be aimed at ensuring that the business does not proceed unless the underlying customers have been identified to the product/service provider's satisfaction.

(iii) Advising intermediary

5.5.17 Where a customer enters into a relationship with a product or service provider to purchase a product or service, with the active involvement of an intermediary, both the product/service provider and the intermediary have an obligation to identify the customer.

Regulation 4(3)(a)(ii)

5.5.18 In such circumstances, where the intermediary is carrying on appropriately regulated business (see paragraph 5.5.13), the product/service provider's procedures may provide that, on the basis

that the firm concludes that it may accept such confirmation (see paragraph 5.5.27), confirmation from the intermediary that it has appropriately identified the customer will itself constitute satisfactory evidence of the customer's identity.

5.5.19 A confirmation can only evidence verification work carried out by the firm giving the confirmation; that firm cannot 'pass on' verification of identity that it has received from another firm. The verification that the firm has carried out must also have been based on the standard level of customer identification and not on the source of funds, or on the basis of the firm having carried out a limited re-verification exercise in respect of its current customers.

5.5.20 The intermediary has no obligation to provide such confirmation to the product/service provider, and may choose not to do so. In such circumstances, or if the product/service provider decides that it should not accept confirmation from the intermediary, then the firm must carry out its own verification of the customer's identity.

5.5.21 In order to standardise the process of firms confirming to one another that customers have been identified, guidance is given in paragraphs 5.5.26 to 5.5.33 below on the use of pro-forma confirmations.

Group introductions

5.5.22 Where customers are introduced between different parts of the same financial sector group, entities that are part of the group should be able to rely on identification procedures conducted by that part of the group which first dealt with the customer. One member of a group should be able to confirm to another part of the group that the identity of the customer has been appropriately verified.

5.5.23 Where a customer is introduced by one part of a financial sector group to another, it is not necessary for his identity to be re-verified, provided that:

- the identity of the customer has been verified by the introducing part of the group in line with AML/CFT standards in the UK, the EU or a comparable jurisdiction; and
- a group introduction confirmation is obtained and held with the customer's records.

5.5.24 The acceptance by a UK firm of confirmation from another group entity that the identity of a customer has been satisfactorily verified is dependent on the relevant records being readily accessible from the UK.

5.5.25 Where UK firms have day-to-day access to all group customer information and records, there is no need to obtain a group introduction confirmation, if the identity of that customer has been verified previously to AML/CFT standards in the EU, or in a comparable jurisdiction. However, if the identity of the customer has not previously been verified, for example because the group customer relationship pre-dates the introduction of anti-money laundering regulations, or if the verification evidence is inadequate, any missing

verification evidence will need to be obtained.

Use of pro-forma confirmations

Regulation 5(2)

5.5.26 Confirmations may only be accepted from another regulated firm carrying on appropriately regulated business (see paragraph 5.5.13). The assessment as to whether or not a firm should accept confirmation from an intermediary that a customer's identity has been verified will be risk-based, and cannot be based simply on a single factor.

5.5.27 The firm's judgement of the intermediary may, depending on the sector, take account of such matters as:

- the public disciplinary record of the intermediary, to the extent that this is available;
- the nature of the customer, the product/service sought and the sums involved;
- any adverse experience of the intermediary's general efficiency in business dealings;
- any other knowledge, whether obtained at the outset of the relationship or subsequently, that the firm has regarding the standing of the intermediary.

Regulation 4(3)(a)(ii)

5.5.28 Part of the firm's AML/CFT policy statement should address the circumstances where confirmation of identity may be accepted from other firms. Provided that the policy sets out considered criteria for judging whether to accept a confirmation, taking account of matters such as set out in paragraph 5.5.27, and that such acceptance is not reckless or negligent, a confirmation will meet the firm's AML/CFT obligations in respect of verification of the customer's identity.

5.5.29 The personal information supplied by the customer as part of an intermediary's customer identification procedures will generally be set out in the application form that the firm will require to be completed, and will therefore be passed to the firm.

5.5.30 A confirmation meets the standard level of customer identification. Where a customer whose identity has been verified by means of a confirmation requests an additional product or service direct from the firm, the firm will need to consider whether the level of verification of identity that the confirmation represents is appropriate to the level of money laundering or terrorist financing risk assessed in the additional product or service. In accordance with the guidance in section 5.4, any necessary additional verification procedures that are required will need to be undertaken before the additional product or service is provided.

5.5.31 Pro-forma confirmations for customer identification and verification are attached as Annex 5-I to this chapter.

5.5.32 Pro-forma confirmations in respect of group introductions are attached as Annex 5-II to this chapter.

3MLD articles 14-18

5.5.33 Under the Third Money Laundering Directive, when implemented in the UK, there will be a legal requirement on an intermediary to make

identification data available on request to a firm relying on its confirmation. (In practice, such requests should not be common.) No such legal requirement currently exists; but it would be good practice on the part of an intermediary to accede to a request, if, exceptionally, one is made as part of a firm's risk-based customer acceptance procedures. Where a firm makes such a request, and it is not met, it will need to take account of that fact in its assessment of the intermediary in question, and of the acceptability of the intermediary's confirmations.

5.6 KYC - Additional customer information

5.6.1 A firm may conclude, under its risk-based approach, that the standard evidence of identity (see section 5.4) is insufficient in relation to the money laundering or terrorist financing risk, and that it should obtain additional information about a particular customer.

5.6.2 As a part of a risk-based approach, therefore, firms may need to hold sufficient information about the circumstances and business of their customers for two principal reasons:

- to inform its risk assessment process, and thus manage its money laundering/terrorist financing risks effectively; and
- to provide a basis for monitoring customer activity and transactions, thus increasing the likelihood that they will detect the use of their products and services for money laundering and terrorist financing.

5.6.3 The extent of additional information sought, and of any monitoring carried out in respect of any particular customer, or class/category of customer, will depend on the money laundering or terrorist financing risk that the customer, or class/category of customer, is assessed to present to the firm.

5.6.4 In practice, under a risk-based approach, it will not be appropriate for every product or service provider to know their customers equally well, regardless of the purpose, use, value, etc., of the product or service provided. Firms' information demands need to be proportionate, appropriate and discriminating, and to be able to be justified to customers.

5.6.5 A firm should hold a fuller set of information in respect of those customers, or class/category of customers, assessed as carrying a higher money laundering or terrorist financing risk, or who are seeking a product or service that carries a higher risk of being used for money laundering or terrorist financing purposes.

5.6.6 At all times, firms should bear in mind their obligations under the Data Protection Act only to seek information that is needed for the declared purpose, not to retain personal information longer than is necessary, and to ensure that information that is held is kept up to date.

5.6.7 At the time this guidance comes into effect, firms are not expected to obtain additional information in respect of existing customers, or classes/categories of customer. However, firms should have regard to paragraphs 5.2.44 to 5.2.49, which give guidance on what they should do in respect of existing customers.

Existing sources of additional customer information

5.6.8 Information additional to the customer's identity, for a personal or non-personal customer, as appropriate, might include some or all of the following, depending on the firm's risk assessment of the customer:

- nature and details of the business/occupation/employment;
- record of changes of address;
- the expected source and origin of the funds to be used in the relationship;
- initial and ongoing source(s) of wealth or income (particularly within a private banking or wealth management relationship);
- copies of recent and current financial statements;
- the various relationships between signatories and with underlying beneficial owners;
- the anticipated level and nature of the activity that is to be undertaken through the relationship.

5.6.9 The purpose and reason for opening the account or establishing the relationship should also be understood. In many cases, of course, this will be self-evident, but in other cases, the firm may have to find this out.

5.6.10 For example, when someone becomes a new customer, or applies for a new product or service, to enable the firm to decide whether to accept the application, account and product application forms often include requests for such information as residential status, employment details, income, and other sources of income.

5.6.11 The availability and use of other financial information held is important for reducing the additional costs of collecting KYC information. Where appropriate and practical, therefore, and where there are no data protection restrictions, firms should take reasonable steps to ensure that where they have KYC information in one part of the business, they are able to link it to information in another.

Politically exposed persons (PEPs)

5.6.12 Individuals who have, or have had, a high political profile, or hold, or have held, public office, can pose a higher money laundering risk to firms as their position makes them vulnerable to corruption. This risk also extends to members of their immediate families and to known close associates. PEP status itself does not, of course, incriminate individuals or entities. It may, however, put a customer into a higher risk category.

3MLD article 3(8)

5.6.13 There is no current definition of PEPs in the UK. The Third EU Money Laundering Directive defines PEPs as "natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons". This definition only applies to those outside the UK.

3MLD article 13(4)

5.6.14 This definition of PEP would include heads of state or of government,

senior politicians, senior government, judicial or military officials, senior executives of publicly owned enterprises and important political party officials.

CDD, paragraph 44
3MLD article 13(4)

5.6.15 Under the Basel CDD paper, firms are encouraged to have in place additional due diligence measures in respect of PEPs. The Third EU Money Laundering Directive will require firms, on a risk-sensitive basis, to:

- have appropriate risk-based procedures to determine whether a customer is a PEP;
- obtain appropriate senior management approval for establishing or maintaining business relationships with such customers;
- take reasonable measures to establish the source of wealth and source of funds of such customers; and
- conduct enhanced ongoing monitoring of the business relationship.

5.6.16 The nature and scope of a particular firm's business will generally determine whether the existence of PEPs in their customer base is an issue for the firm, and whether the firm needs to consider screening all customers for this purpose.

5.6.17 Establishing whether individuals or legal entities qualify as PEPs is not always straightforward and can present difficulties. Where firms need to carry out specific checks, they may be able to rely on an internet search engine, or consult relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations. Resources such as the Transparency International Corruption Perceptions Index, which ranks approximately 150 countries according to their perceived level of corruption, may be helpful in terms of assessing the risk. If there is a need to conduct more thorough checks, or if there is a high likelihood of a firm having PEPs for customers, subscription to a specialist PEP database may be the only adequate risk mitigation tool.

5.6.18 New and existing customers may not initially meet the definition of a PEP. The firm should, as far as practicable, be alert to public information relating to possible changes in the status of its customers with regard to political exposure.

ANNEX 5-I/1

CONFIRMATION OF VERIFICATION OF IDENTITY

PRIVATE INDIVIDUAL

INTRODUCTION BY AN FSA-REGULATED FIRM

1 DETAILS OF INDIVIDUAL (see explanatory notes below)

Full name of Customer	

Current Address		Previous address if individual has changed address in the last three months

Date of Birth	

2 CONFIRMATION

I/we confirm that

(a) the information in section 1 above was obtained by me/us in relation to the customer;

(b) the evidence I/we have obtained to verify the identity of the customer:
[tick only one]

meets the standard evidence set out within the guidance for the UK Financial Sector issued by JMLSG ; or	
exceeds the standard evidence (written details of the further verification evidence taken are attached to this confirmation).	

Signed:	
Name:	
Position:	
Date:	

3 DETAILS OF INTRODUCING FIRM (OR SOLE TRADER)

Full Name of Regulated Firm (or Sole Trader):	
FSA Reference Number:	

Explanatory notes

1. A separate confirmation must be completed for each customer (e.g. joint holders, trustee cases and joint life cases). Where a third party is involved, e.g. a payer of contributions who is different from the customer, the identity of that person must also be verified, and a confirmation provided.

2. This form cannot be used to verify the identity of any customer that falls into one of the following categories:

   - those who are exempt from verification as being an existing client of the introducing firm prior to the introduction of the requirement for such verification;
   - those whose identity has not been verified by virtue of the application of a permitted exemption under the Money Laundering Regulations; or
   - those whose identity has been verified using the source of funds as evidence.

3. This confirmation must carry an original signature, or an electronic equivalent.

ANNEX 5-I/2

CONFIRMATION OF VERIFICATION OF IDENTITY

PRIVATE INDIVIDUAL

INTRODUCTION BY AN EU REGULATED FINANCIAL SERVICES FIRM

1 DETAILS OF INDIVIDUAL (see explanatory notes below)

Full name of Customer	

Current Address		Previous address if individual has changed address in the last three months

Date of Birth	

2 CONFIRMATION

We confirm that

(a) the information in section 1 above was obtained by us in relation to the customer;

(b) the evidence we have obtained to verify the identity of the customer meets the requirements of our national money laundering legislation that implements the EU Money Laundering Directive, and any relevant authoritative guidance provided as best practice in relation to the type of business or transaction to which this confirmation relates;

(c) where the underlying evidence taken in relation to the verification of the customer's identity is held outside the UK, in the event of any enquiry from UK law enforcement agencies or regulators, copies of the relevant customer records will be made available under court order or relevant mutual assistance procedure, to the extent that we are required under local law to retain these records.

Signed:	
Name:	
Position:	
Date:	

3 DETAILS OF INTRODUCING FIRM

Full Name of Regulated Firm:	
Jurisdiction:	
Name of Regulator:	
Regulator Reference Number:	

Explanatory notes

1 A separate confirmation must be completed for each customer (e.g. joint holders, trustee cases and joint life cases). Where a third party is involved, e.g. a payer of contributions who is different from the customer, the identity of that person must also be verified, and a confirmation provided.

2 This form cannot be used to verify the identity of any customer that falls into one of the following categories:

- those who are exempt from verification as being an existing client of the introducing firm prior to the adoption of our national legislation that implements the EU Money Laundering Directive; or
- those whose identity has not been verified by virtue of the application of a permitted exemption under the EU Money Laundering Directive.

3 This confirmation must carry an original signature, or electronic equivalent.

ANNEX 5-I/3

CONFIRMATION OF VERIFICATION OF IDENTITY

PRIVATE INDIVIDUAL

INTRODUCTION BY A NON-EU REGULATED FINANCIAL SERVICES FIRM (which the receiving firm has accepted as being from a comparable jurisdiction)

1 DETAILS OF INDIVIDUAL (see explanatory notes below)

Full name of Customer	

Current Address		Previous address if individual has changed address in the last three months

Date of Birth	

2 CONFIRMATION

We confirm that:

(a) the information in section 1 above was obtained by us in relation to the customer;

(b) the evidence we have obtained to verify the identity of the customer meets the requirements of local law and regulation;

(c) where the underlying evidence taken in relation to the verification of the customer's identity is held outside the UK, in the event of any enquiry from UK law enforcement agencies or regulators, copies of the relevant customer records will be made available under court order or relevant mutual assistance procedure, to the extent that we are required under local law to retain these records.

Signed:	
Name:	
Position:	
Date:	

3 DETAILS OF INTRODUCING FIRM

Full Name of Regulated Firm:	
Jurisdiction:	
Name of Regulator:	
Regulator Reference Number:	

Explanatory notes

1 A separate confirmation must be completed for each customer (e.g. joint holders, trustee cases and joint life cases). Where a third party is involved, e.g. a payer of contributions who is different from the customer, the identity of that person must also be verified, and a confirmation provided.

2 This form cannot be used to verify the identity of any customer that falls into one of the following categories:

- those who are exempt from verification as being an existing client of the introducing firm prior to the adoption of local anti money laundering laws or regulation requiring such verification; or
- those whose identity has not been verified by virtue of the application of a permitted exemption under local anti money laundering laws or regulation.

3 This confirmation must carry an original signature, or electronic equivalent.

ANNEX 5-I/4

CONFIRMATION OF VERIFICATION OF IDENTITY

CORPORATE AND OTHER NON-PERSONAL ENTITY

INTRODUCTION BY AN FSA-REGULATED FIRM

1 DETAILS OF CUSTOMER (see explanatory notes below)

Full name of customer	
Type of entity (corporate, trust, etc)	
Location of business (full operating address)	
Registered office in country of incorporation	
Registered number, if any (or appropriate)	
Relevant company registry or regulated market listing authority	
Names of directors (or equivalent)	
Names of principal beneficial owners (over 25%)	

2 CONFIRMATION

I/we confirm that

(a) the information in section 1 above was obtained by me/us in relation to the customer;

(b) the evidence I/we have obtained to verify the identity of the customer: [tick only one]

meets the guidance for standard evidence set out within the guidance for the UK Financial Sector issued by JMLSG; or	
exceeds the standard evidence (written details of the further verification evidence taken are attached to this confirmation).	

Signed:	
Name:	
Position:	
Date:	

3 DETAILS OF INTRODUCING FIRM (OR SOLE TRADER)

Full Name of Regulated Firm (or Sole Trader):	
FSA Reference Number:	

Explanatory notes

1. "Relevant company registry" includes other registers, such as those maintained by charity commissions (or equivalent) or chambers of commerce.
2. This form cannot be used to verify the identity of any customer that falls into one of the following categories:
   - those who are exempt from verification as being an existing client of the introducing firm prior to the introduction of the requirement for such verification;
   - those whose identity has not been verified by virtue of the application of a permitted exemption under the Money Laundering Regulations; or
   - those whose identity has been verified using the source of funds as evidence.
3. This confirmation must carry an original signature, or electronic equivalent.

ANNEX 5-I/5

CONFIRMATION OF VERIFICATION OF IDENTITY

CORPORATE AND OTHER NON-PERSONAL ENTITY

INTRODUCTION BY AN EU REGULATED FINANCIAL SERVICES FIRM

1 DETAILS OF CUSTOMER (see explanatory notes below)

Full name of customer	
Type of entity (corporate, trust, etc)	
Location of business (full operating address)	
Registered office in country of incorporation	
Registered number, if any (or appropriate)	
Relevant company registry or regulated market listing authority	
Names of directors (or equivalent)	
Names of principal beneficial owners (over 25%)	

2 CONFIRMATION

We confirm that

(a) the information in section 1 above was obtained by us in relation to the customer;

(b) the evidence we have obtained to verify the identity of the customer meets the requirements of our national money laundering legislation that implements the EU Money Laundering Directive, and any relevant authoritative guidance provided as best practice in relation to the type of business or transaction to which this confirmation relates;

(c) where the underlying evidence taken in relation to the verification of the customer's identity is held outside the UK, in the event of any enquiry from UK law enforcement agencies or regulators, copies of the relevant customer records will be made available under court order or relevant mutual assistance procedure, to the extent that we are required under local law to retain these records.

Signed:	
Name:	
Position:	
Date:	

3 DETAILS OF INTRODUCING FIRM

Full Name of Regulated Firm:	
Jurisdiction:	
Name of Regulator:	
Regulator	

Reference Number:	

Explanatory notes

1. "Relevant company registry" includes other registers, such as those maintained by charity commissions (or equivalent) or chambers of commerce.
2. This form cannot be used to verify the identity of any customer that falls into one of the following categories:
   - those who are exempt from verification as being an existing client of the introducing firm prior to the adoption of our national legislation that implements the EU Money Laundering Directive; or
   - those whose identity has not been verified by virtue of the application of a permitted exemption under the EU Money Laundering Directive.
3. This confirmation must carry an original signature, or electronic equivalent.

ANNEX 5-I/6

CONFIRMATION OF VERIFICATION OF IDENTITY

CORPORATE AND OTHER NON-PERSONAL ENTITY
INTRODUCTION BY A NON-EU REGULATED FINANCIAL SERVICES FIRM
(which the receiving firm has accepted as being from a comparable jurisdiction)

1 DETAILS OF CUSTOMER (see explanatory notes below)

Full name of customer	
Type of entity (corporate, trust, etc)	
Location of business (full operating address)	
Registered office in country of incorporation	
Registered number, if any (or appropriate)	
Relevant company registry or regulated market listing authority	
Names of directors (or equivalent)	
Names of principal beneficial owners (over 25%)	

2 CONFIRMATION

We confirm that:

(a) the information in section 1 above was obtained by us in relation to the customer;

(b) the evidence we have obtained to verify the identity of the customer meets the requirements of local law and regulation;

(c) where the underlying evidence taken in relation to the verification of the customer's identity is held outside the UK, in the event of any enquiry from UK law enforcement agencies or regulators, copies of the relevant customer records will be made available under court order or relevant mutual assistance procedure, to the extent that we are required under local law to retain these records.

Signed:	
Name:	
Position:	
Date:	

3 DETAILS OF INTRODUCING FIRM

Full Name of Regulated Firm:	
Jurisdiction:	
Name of Regulator:	
Regulator Reference Number:	

Explanatory notes

1 "Relevant company registry" includes other registers, such as those maintained by charity commissions (or equivalent) or chambers of commerce.

2 This form cannot be used to verify the identity of any customer that falls into one of the following categories:

- those who are exempt from verification as being an existing client of the introducing firm prior to the adoption of local anti money laundering laws or regulation requiring such verification; or
- those whose identity has not been verified by virtue of the application of a permitted exemption under local anti money laundering laws or regulation.

3 This confirmation must carry an original signature, or electronic equivalent.

ANNEX 5-II/1

CONFIRMATION OF VERIFICATION OF IDENTITY
GROUP INTRODUCTION
PRIVATE INDIVIDUAL

1 DETAILS OF INDIVIDUAL (see explanatory notes below)

Full name of Customer		
Current Address		Previous address if customer has changed address in the last three months
Date of Birth		

2 CONFIRMATION

We confirm that

(a) the verification of the identity of the above customer meets the requirements:

i. of the Money Laundering Regulations 2003, and the guidance for standard evidence set out within the guidance for the UK Financial Sector issued by JMLSG; or

ii. of our national money laundering legislation that implements the EU Money Laundering Directive, and any relevant authoritative guidance provided as best practice in relation to the type of business or transaction to which this confirmation relates; or

iii. of local law and regulation.

(b) where the underlying evidence taken in relation to the verification of the customer's identity is held outside the UK, in the event of any enquiry from UK law enforcement agencies or regulators, copies of the relevant customer records will be made available under court order or relevant mutual assistance procedure, to the extent that we are required under local law to retain these records.

Signed:	
Name:	
Position:	
Date:	

3 DETAILS OF GROUP FIRM

Full Name of Regulated Firm:	
Relationship to receiving firm:	
Jurisdiction:	
Name of Regulator:	
Regulator Reference Number:	

Explanatory notes

1. A separate confirmation must be completed for each customer (e.g. joint holders). Where a third party is involved, e.g. a payer of contributions who is different from the customer, the identity of that person must also be verified, and a confirmation provided.
2. This form cannot be used to verify the identity of any customer that falls into one of the following categories:
   - those who are exempt from verification as being an existing client of the introducing firm prior to the introduction of the requirement for such verification;
   - those whose identity has not been verified by virtue of the application of a permitted exemption under local anti money laundering law or regulation; or
   - those whose identity has been verified using the source of funds as evidence.

3 This confirmation must carry an original signature, or an electronic equivalent.

ANNEX 5-II/2

CONFIRMATION OF VERIFICATION OF IDENTITY
GROUP INTRODUCTION
CORPORATE AND OTHER NON-PERSONAL ENTITY

1 DETAILS OF CUSTOMER (see explanatory notes below)

Full name of customer	
Type of entity (corporate, trust, etc)	
Location of business (full operating address)	
Registered office in country of incorporation	
Registered number, if any (or appropriate)	
Relevant company registry or regulated market listing authority	
Names of directors (or equivalent)	
Names of principal beneficial owners (over 25%)	

2 CONFIRMATION

We confirm that

(a) the verification of the identity of the above customer meets the requirements:

(i) of the Money Laundering Regulations 2003, and the guidance for standard evidence set out within the guidance for the UK Financial Sector issued by JMLSG; or

(ii) of our national money laundering legislation that implements the EU Money Laundering Directive, and any authoritative relevant guidance provided as best practice in relation to the type of business or transaction to which this confirmation relates; or

(iii) of local law and regulation.

(b) where the underlying evidence taken in relation to the verification of the customer's identity is held outside the UK, in the event of any enquiry from UK law enforcement agencies or regulators, copies of the relevant customer records will be made available under court order or relevant mutual assistance procedure, to the extent that we are required under local law to retain these records.

Signed:	
Name:	
Position:	
Date:	

3 DETAILS OF GROUP FIRM

Full Name of Regulated Firm:	
Relationship to receiving firm:	
Jurisdiction:	
Name of Regulator:	
Regulator Reference Number:	

Explanatory notes

1. "Relevant company registry" includes other registers, such as those maintained by charity commissions (or equivalent) or chambers of commerce.
2. This form cannot be used to verify the identity of any customer that falls into one of the following categories:
   - those who are exempt from verification as being an existing client of the introducing firm prior to the introduction of the requirement for such verification;
   - those whose identity has not been verified by virtue of the application of a permitted exemption under local anti money laundering law or regulation; or
   - those whose identity has been verified using the source of funds as evidence.

3 This confirmation must carry an original signature, or an electronic equivalent.

CHAPTER 6

MONITORING CUSTOMER ACTIVITY

The need to monitor customers' activities

Regulation 3(1)(b)
POCA ss330, 331

6.1 There is no specific legal or regulatory requirement that customers' activities be monitored, but having regard to the following obligations:

- the general requirement to establish appropriate procedures of internal control for the purposes of forestalling and preventing money laundering/terrorist financing
- the requirement to report knowledge or suspicion of possible money laundering/terrorist financing
- the 'reasonable grounds' test for making such reports under POCA and the Terrorism Act

there is an expectation that, where the situation so warrants (see paragraph 6.9), a firm will establish and maintain an appropriate approach to enable it to detect transactions or activity that may indicate money laundering or terrorist financing.

6.2 In addition to carrying out customer due diligence, therefore, a firm may need to monitor customer activity to identify, during the course of a continuing relationship, unusual activity. If unusual events cannot be rationally explained, they may involve money laundering or terrorist financing. Monitoring customer activity and transactions throughout a relationship helps give greater assurance that the firm is not being used for the purposes of financial crime.

What is monitoring?

6.3 The essentials of any system of monitoring are that:

- it flags up transactions and/or activities for further examination;
- these reports are reviewed promptly by the right person(s); and
- appropriate action is taken on the findings of any further examination.

6.4 Monitoring can be either:

- in real time, in that transactions and/or activities can be reviewed as they take place or are about to take place, or
- after the event, through some independent review of the transactions and/or activities that a customer has undertaken

and in either case, unusual transactions or activities will be flagged for further examination.

6.5 Monitoring may be by reference to specific types of transactions, to the profile of the customer, or by comparing their activity or profile with that of a similar, peer group of customers, or through a combination of these approaches.

6.6 Firms should also have systems and procedures to deal with customers who have not had contact with the firm for some time, in circumstances where regular contact might be expected, and with dormant accounts or relationships, to be able to identify future reactivation and unauthorised use.

6.7 In designing monitoring arrangements, it is important that appropriate account be taken of the frequency, volume and size of transactions with customers, in the context of the assessed customer and product risk.

6.8 Monitoring is not a mechanical process and does not necessarily require sophisticated electronic systems. The scope and complexity of the process will be influenced by the firm's business activities, and whether the firm is large or small. The key elements of any system are having up-to-date customer information, on the basis of which it will be possible to spot the unusual, and asking pertinent questions to elicit the reasons for unusual transactions or activities in order to judge whether they may represent something suspicious.

Nature of monitoring

6.9 Some financial services business typically involves transactions with customers about whom the business has a good deal of information, acquired for both business and regulatory reasons. Other types of financial services business involve transactions with customers about whom the business may need to have only limited information. The nature of the monitoring in any given case will therefore depend on the business of the firm, the frequency of customer activity, and the types of customer that are involved.

6.10 Effective monitoring is likely to be based on a considered identification of transaction characteristics, such as:

- the unusual nature of a transaction: e.g., abnormal size or frequency for that customer or peer group; the early surrender of an insurance policy;
- the nature of a series of transactions: for example, a number of cash credits;
- the geographic destination or origin of a payment: for example, to or from a high-risk country; and
- the parties concerned: for example, a request to make a payment to or from a person on a sanctions list.

6.11 The arrangements should include the training of staff on procedures to spot and deal specially (e.g. by referral to management) with situations that arise that suggest a heightened money laundering risk; or they could involve arrangements for exception reporting by reference to objective triggers (e.g. transaction amount). Staff training is not, however, a substitute for having in place some form of regular monitoring activity.

6.12 Higher risk accounts and customer relationships will generally require more frequent or intensive monitoring.

Manual or automated?

6.13 A monitoring system may be manual, or may be automated to the extent that a standard suite of exception reports are produced. One or other of these approaches may suit most firms. In the relatively few firms where there are major issues of volume, or where there are other factors that make a basic exception report regime inappropriate, a more sophisticated automated system may be necessary.

6.14 It is essential to recognise the importance of staff alertness. Such factors as staff intuition, direct exposure to a customer face-to-face or on the telephone, and the ability, through practical experience, to recognise transactions that do not seem to make sense for that customer, cannot be automated (see Chapter 8: Staff awareness, training and alertness).

6.15 In relation to a firm's monitoring needs, an automated system may add value to manual systems and controls, provided that the parameters determining the outputs of the system are appropriate. Firms should understand the workings and rationale of an automated system, and should understand the reasons for its output of alerts, as it may be asked to explain this to its regulator.

6.16 The greater the volume of transactions, the less easy it will be for a firm to monitor them without the aid of some automation. Systems available include those that many firms, particularly those that offer credit, use to monitor fraud. Although not specifically designed to identify money laundering or terrorist financing, the output from these anti-fraud monitoring systems can often indicate possible money laundering or terrorist financing.

6.17 There are many automated transaction monitoring systems available on the market; they use a variety of techniques to detect and report unusual/uncharacteristic activity. These techniques can range from artificial intelligence to simple rules. The systems available are not designed to detect money laundering or terrorist financing, but are able to detect and report unusual/uncharacteristic behaviour by customers, and patterns of behaviour that are characteristic of money laundering or terrorist financing, which after analysis may lead to suspicion of money laundering or terrorist financing. The implementation of transaction monitoring systems is difficult due to the complexity of the underlying analytics used and their heavy reliance on customer reference data and transaction data.

6.18 Monitoring systems, manual or automated, can vary considerably in their approach to detecting and reporting unusual or uncharacteristic behaviour. It is important for firms to ask questions of the supplier of an automated system, and internally within the business, whether in support of a manual or an automated system, to aid them in selecting a solution that meets their particular business needs best. Questions that should be addressed include:

- How does the solution enable the firm to implement a risk-based approach to customers, third parties and transactions?
- How do system parameters aid the risk-based approach and consequently affect the quality and volume of transactions alerted?

- What are the money laundering/terrorist financing typologies that the system addresses, and which component of the system addresses each typology? Are the typologies that are included with the system complete? Are they relevant to the firm's particular line of business?
- What functionality does the system provide to implement new typologies, how quickly can relevant new typologies be commissioned in the system and how can their validity be tested prior to activation in the live system?
- What functionality exists to provide the user with the reason that a transaction is alerted and is there full evidential process behind the reason given?
- Does the system have robust mechanisms to learn from previous experience and how is the false positive rate continually monitored and reduced?

6.19 What constitutes unusual or uncharacteristic behaviour by a customer, is often defined by the system. It will be important that the system selected has an appropriate definition of 'unusual or uncharacteristic' and one that is in line with the nature of business conducted by the firm.

6.20 The effectiveness of a monitoring system, automated or manual, in identifying unusual activity will depend on the quality of the parameters which determine what alerts it makes, and the ability of staff to assess and act as appropriate on these outputs. The needs of each firm will therefore be different, and each system will vary in its capabilities according to the scale, nature and complexity of the business. It is important that the balance is right in setting the level at which an alert is generated; it is not enough to fix it so that the system generates just enough output for the existing staff complement to deal with – but equally, the system should not generate large numbers of 'false positives', which require excessive resources to investigate.

CHAPTER 7

SUSPICIOUS ACTIVITIES, REPORTING AND DATA PROTECTION

Key points in this chapter

- **Relevant law/regulation**
  - Regulation 7
  - POCA ss327-335, s339, s340, s342
  - Terrorism Act, s21A, s39
  - Data Protection Act 1998, s7, s29
  - Financial sanctions legislation
- **Core obligations**
  - All staff must raise an internal report where they have knowledge or suspicion, or where there are reasonable grounds for having knowledge or suspicion, that another person is engaged in money laundering, or that terrorist property exists
  - The firm's nominated officer must consider all internal reports
  - The firm's nominated officer must make an external report to the National Criminal Intelligence Service (NCIS) as soon as is practicable if he considers that there is knowledge, suspicion, or reasonable grounds for knowledge or suspicion, that another person is engaged in money laundering, or that terrorist property exists
  - The firm must seek consent from NCIS before proceeding with a suspicious transaction or entering into arrangements
  - Firms must freeze funds if a customer is identified as being on the Consolidated List on the Bank of England website of suspected terrorists or sanctioned individuals and entities, and make an external report to the Bank of England
  - It is a criminal offence for anyone, following a disclosure to a nominated officer or to NCIS, to do or say anything that might either 'tip off' another person that a disclosure has been made or prejudice an investigation
  - The firm's nominated officer must report suspicious approaches, even if no transaction takes place
- **Actions required, to be kept under regular review**
  - Enquiries made in respect of disclosures must be documented
  - The reasons why a Suspicious Activity Report (SAR) was, or was not, submitted should be recorded
  - Any communications made with or received from the authorities, including NCIS, in relation to a SAR should be maintained on file
  - In cases where advance notice of a transaction or of arrangements is given, the need for prior consent before it is allowed to proceed should be considered

General legal and regulatory obligations

Regulation 7 (1) (b)
POCA ss 330, 331
Terrorism Act s 21A

7.1 Persons in the regulated sector are required to make a report in respect of information that comes to them within the course of a business in the regulated sector:

- where they *know* or
- where they *suspect* or
- where they *have reasonable grounds for knowing or suspecting*

that a person is engaged in money laundering or terrorist financing. Within this guidance, the above obligations are collectively referred to as "grounds for knowledge or suspicion".

Regulation 7 (1)
POCA s 330

7.2 In order to provide a framework within which suspicion reports may be raised and considered:

- each firm must ensure that any member of staff reports to the firm's nominated officer (who may also be the MLRO in an FSA-regulated firm), where they have grounds for knowledge or suspicion that a person or customer is engaged in money laundering or terrorist financing;
- the firm's nominated officer must consider each such report, and determine whether it gives grounds for knowledge or suspicion;
- firms should ensure that staff are appropriately trained in their obligations, and in the requirements for making reports to their nominated officer.

Regulation 7 (1) (d)
POCA, s 331
Terrorism Act s 21A

7.3 If the nominated officer determines that a report does give rise to grounds for knowledge or suspicion, he must report the matter to NCIS. Under POCA, the nominated officer is required to make a report to NCIS as soon as is practicable if he has grounds for suspicion that another person, whether or not a customer, is engaged in money laundering. Under the Terrorism Act, similar conditions apply in relation to disclosure where there are grounds for suspicion of terrorist financing.

7.4 A sole trader with no employees who knows or suspects, or where there are reasonable grounds to know or suspect, that a customer of his, or the person on whose behalf the customer is acting, is or has been engaged in money laundering or terrorist financing, must make a report promptly to NCIS.

POCA ss 333 -334, s 342
Terrorism Act s 39

7.6 It is a criminal offence for anyone, following a disclosure to a nominated officer or to NCIS, to release information that might 'tip off' another person that a disclosure has been made and prejudice an investigation.

Financial sanctions legislation

7.7 It is a criminal offence to make funds, economic resources or, in certain circumstances, financial services available to those persons listed as the targets of financial sanctions legislation. There is also a requirement to report to the Bank of England both details of funds frozen and where firms have knowledge or suspicion that a customer of the firm or a person with whom the firm has had business dealings is a listed person, a person acting on behalf of a listed person or has committed an offence under the sanctions legislation.

What is meant by "knowledge" and "suspicion"?

POCA, s 330 (2),(3), s331 (2), (3)
Terrorism Act s21A

7.8 Having knowledge means actually knowing something to be true. In a criminal court, it must be proved that the individual *in fact* knew that a person was engaged in money laundering. That said, knowledge can be *inferred* from the surrounding circumstances; so, for example, a failure to ask obvious questions may be relied upon by a jury to imply knowledge. The knowledge must, however, have come to the firm (or

to the member of staff) in the course of business, or (in the case of a nominated officer) as a consequence of a disclosure under s330 of POCA or s21A of the Terrorism Act. Information that comes to the firm or staff member in other circumstances does not come within the scope of the regulated sector obligation to make a report. This does not preclude a report being made should staff choose to do so, or are obligated to do so by other parts of these Acts.

7.9 Suspicion is more subjective and falls short of proof based on firm evidence. Suspicion has been defined by the courts as being beyond mere speculation and based on some foundation, for example:

> *"A degree of satisfaction and not necessarily amounting to belief but at least extending beyond speculation as to whether an event has occurred or not";* and
>
> *"Although the creation of suspicion requires a lesser factual basis than the creation of a belief, it must nonetheless be built upon some foundation."*

7.10 A transaction which appears unusual is not necessarily suspicious. Even customers with a stable and predictable transactions profile will have periodic transactions that are unusual for them. Many customers will, for perfectly good reasons, have an erratic pattern of transactions or account activity. So the unusual is, in the first instance, only a basis for further enquiry, which may in turn require judgement as to whether it is suspicious. A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report then arises.

7.11 A member of staff, including the nominated officer, who considers a transaction or activity to be suspicious, would not necessarily be expected either to know or to establish the exact nature of any underlying criminal offence, or that the particular funds or property were definitely those arising from a crime or terrorist financing.

7.12 Transactions, or proposed transactions, as part of '419' scams are attempted advance fee frauds, and not money laundering; they are therefore not reportable under POCA or the Terrorism Act, unless the fraud is successful, and the firm is aware of resulting criminal property.

What is meant by "reasonable grounds to know or suspect"?

POCA, s 330 (2)(b), s331 (2)(b)
Terrorism Act s 21A

7.13 In addition to establishing a criminal offence when suspicion or actual knowledge of money laundering/terrorist financing is proved, POCA and the Terrorism Act introduce criminal liability for failing to disclose information when reasonable grounds exist for knowing or suspecting that a person is engaged in money laundering/terrorist financing. This introduces an objective test of suspicion. The test would likely be met when there are demonstrated to be facts or circumstances, known to the member of staff, from which a reasonable person engaged in a business subject to the ML Regulations would have inferred knowledge, or formed the suspicion, that another person was engaged in money

laundering or terrorist financing.

7.14 To defend themselves against a charge that they failed to meet the objective test of suspicion, staff within financial sector firms would need to be able to demonstrate that they took reasonable steps in the particular circumstances, in the context of a risk-based approach, to know the customer and the rationale for the transaction, activity or instruction. It is important to bear in mind that, in practice, members of a jury may decide, with the benefit of hindsight, whether the objective test has been met.

7.15 Depending on the circumstances, a firm being served with a court order in relation to a customer may give rise to reasonable grounds for suspicion in relation to that customer. In such an event, firms should review the information it holds about that customer across the firm, in order to determine whether or not such grounds exist.

Internal reporting

Regulation 7 (1) (b)
POCA s330(5)

7.16 The obligation to report to the nominated officer within the firm where they have grounds for knowledge or suspicion of money laundering or terrorist financing is placed on all relevant employees in the regulated sector. All financial sector firms therefore need to ensure that all relevant employees know who they should report suspicions to.

Regulation 7(1)(b)

7.17 Firms may wish to set up internal systems that allow staff to consult with their line manager before sending a report to the nominated officer. The obligation under the ML Regulations is to report 'as soon as is reasonably practicable', and so any such consultations should take this into account. Where a firm sets up such systems it should ensure that they are not used to prevent reports reaching the nominated officer whenever staff have stated that they have knowledge or suspicion that a transaction or activity may involve money laundering or terrorist financing.

7.18 Whether or not a member of staff consults colleagues, the legal obligation remains with the staff member to decide for himself whether a report should be made; he must not allow colleagues to decide for him. Where a colleague has been consulted, he himself will then have knowledge on the basis of which he must consider whether a report to the nominated officer is necessary. In such circumstances, firms should make arrangements such that the nominated officer only receives one report in respect of the same information giving rise to knowledge or suspicion.

7.19 Short reporting lines, with a minimum number of people between the person with the knowledge or suspicion and the nominated officer, will ensure speed, confidentiality and swift access to the nominated officer.

7.20 All suspicions reported to the nominated officer should be documented, or recorded electronically. The report should include full details of the customer who is the subject of concern and as full a

statement as possible of the information giving rise to the knowledge or suspicion. All internal enquiries made in relation to the report should also be documented, or recorded electronically. This information may be required to supplement the initial report or as evidence of good practice and best endeavours if, at some future date, there is an investigation and the suspicions are confirmed or disproved.

7.21 Once an employee has reported his suspicion in an appropriate manner to the nominated officer, or to an individual to whom the nominated officer has delegated the responsibility to receive such internal reports, he has fully satisfied his statutory obligation.

7.22 Until the nominated officer advises the member of staff making an internal report that no report to NCIS is to be made, further transactions or activity in respect of that customer, whether of the same nature or different from that giving rise to the previous suspicion, should be reported to the nominated officer as they arise.

Non-UK offences

POCA, s 340 (2), (11)
SOCPA, s 102

7.23 The offence of money laundering, and the duty to report under POCA, apply in relation to the proceeds of any criminal activity, wherever conducted (including abroad), that would constitute an offence if it took place in the UK. SOCPA proposes to amend this scope to exclude offences (other than offences of a description prescribed by the Secretary of State by order) which the firm, staff member or nominated officer knows, or believes on reasonable grounds, to have been committed in a country or territory outside the UK and not to be unlawful under the criminal law then applying in the country or territory concerned. This amendment has, however, not yet been brought into force.

Terrorism Act s21A(11)

7.24 The duty to report under the Terrorism Act applies in relation to taking any action, or being in possession of a thing, that is unlawful under sections 15-18 of that Act, that would have been an offence under these sections of the Act had it occurred in the UK.

Regulation 7 (1)(b)
POCA s 331
POCA ss327-329
Terrorism Act s 21A

7.25 The obligation to consider reporting to NCIS applies only when the nominated officer has received a report made by someone working within the UK regulated sector, or when he himself becomes aware of such a matter in the course of relevant business (which may come from overseas, or from a person overseas). The nominated officer is not, therefore, obliged to report everything that comes to his attention from outside of the UK, although he would be prudent to exercise his judgement in relation to information that comes to his attention from non-business sources. In reaching a decision on whether to make a disclosure, the nominated officer must bear in mind the need to avoid involvement in an offence under ss327-329 of POCA.

Evaluation and determination by the nominated officer

Regulation 7 (1) (c) and (d)

7.26 The firm's nominated officer must consider each report and determine whether it gives rise to knowledge or suspicion, or reasonable grounds for knowledge or suspicion. The firm must permit the nominated officer to have access to any information, including 'know your customer' information, in the firm's possession which could be relevant. The nominated officer may also require further information to be obtained, from the customer if necessary, or from an intermediary who introduced the customer to the firm, to the extent that the introducer still holds the information (bearing in mind his own record keeping requirements). Any approach to the customer or to the intermediary should be made sensitively, and probably by someone other than the nominated officer, to minimise the risk of alerting the customer or an intermediary that a disclosure to NCIS may be being considered.

7.27 When considering an internal suspicion report, the nominated officer, taking account of the risk posed by the transaction or activity being addressed, will need to strike the appropriate balance between the requirement to make a timely disclosure to NCIS, especially if consent is required, and any delays that might arise in searching a number of unlinked systems and records that might hold relevant information.

7.28 As part of the review, other known connected accounts or relationships may need to be examined. Connectivity can arise commercially (through linked accounts, introducers, etc.), or through individuals (third parties, controllers, signatories etc.). Given the need for timely reporting, it may be prudent for the nominated officer to consider making an initial report to NCIS prior to completing a full review of linked or connected relationships, which may or may not subsequently need to be reported to NCIS.

7.29 If the nominated officer decides not to make a report to NCIS, the reasons for not doing so should be clearly documented, or recorded electronically, and retained with the internal suspicion report.

External reporting

Regulation 7 (1)(b)
POCA, s 331
Terrorism Act, s 21A

7.30 The firm's nominated officer must report to NCIS any transaction or activity that, after his evaluation, he knows or suspects, or has reasonable grounds to know or suspect, may be linked to money laundering or terrorist financing. Such reports must be made as soon as is reasonably practicable after the information comes to him.

POCA, s 339

7.31 POCA provides that the Secretary of State may by order prescribe the form and manner in which a disclosure under s330, s331, s332 or s338 may be made. To date, no order has been laid in this respect. NCIS has, however, prepared a standard disclosure report form, and a limited intelligence value report form. These are available at www.ncis.gov.uk/disclosure.asp. The NCIS website also contains guidance on completing the forms.

7.32 The means of making reports that is preferred by NCIS is electronically through the NCIS Money Web interface. Where this route is not practicable, reports should be made either electronically through encrypted e-mail links approved by NCIS, or by fax, first class post, or courier. There is no need to fax and post the same disclosure. Where reports are submitted in paper format, they should be typed or word-processed on the standard forms, to enable them to be scanned.

7.33 In order that an informed overview of the situation may be maintained, all contact between particular departments/branches and law enforcement agencies should be controlled through, or reported back to a single contact point, which will typically be the nominated officer. In the alternative, it may be appropriate to route communications through an appropriate member of staff in the firm's legal or compliance department.

7.34 A SAR's intelligence value is related to the quality of information it contains. A firm needs to have good base data from which to draw the information to be included in the SAR; there needs to be a system to enable the relevant information to be produced in hard copy for the law enforcement agencies, if requested under a court order. When a SAR is submitted to NCIS, the basis for the knowledge or suspicion of money laundering or terrorist financing should be set out in a clear and concise manner.

7.35 Firms should include in each SAR as much relevant information about the customer, transaction or activity that it has in its records. In particular, the law enforcement agencies have indicated that details of an individual's occupation/company's business and National Insurance number are valuable in enabling them to access other relevant information about the customer. As there is no obligation to collect this information (other than in very specific cases), a firm may not hold these details for all its customers; where it has obtained this information, however, it would be helpful to include it as part of a SAR made by the firm. NCIS' website (www.ncis.co.uk/disclosure.asp#forms) contains guidance on completing SARs in a way that make them of most assistance to law enforcement.

Financial sanctions legislation

7.36 Firms must report to the Bank of England details of funds frozen under financial sanctions legislation and where the firm has knowledge or a suspicion that the financial sanctions measures have been or are being contravened, or that a customer is a listed person, or a person acting on behalf of a listed person. The firm may also need to consider whether the firm has an obligation also to report under POCA or the Terrorism Act.

Where to report

7.37 To avoid committing a failure to report offence, nominated officers must make their disclosures to NCIS. The national reception point for disclosure of suspicions, and for seeking consent to continue to proceed with the transaction or activity, is the Financial Intelligence Division of NCIS.

7.38 The Financial Intelligence Division's postal address is PO Box 8000, London SE11 5EN. The unit can be contacted during office hours on: 020 7238 8282. Urgent disclosures, i.e. those requiring consent, should be transmitted electronically over a previously agreed secure link or by fax as specified on the NCIS website at www.ncis.co.uk/disclosure.asp#forms. Speed of response is assisted if the appropriate consent request is clearly mentioned in the title of any faxed report.

7.39 To avoid committing a failure to report offence under financial sanctions legislation, firms must make their reports to the Bank of England. The relevant unit is the Financial Sanctions Unit, Bank of England, Threadneedle Street, London EC2R 8AH. Reports can be submitted electronically and the FSU can be contacted by telephone on 020 7604 4768/5811/4328/4783 and fax on 020 7601 4309.

Attempted fraud and attempted money laundering

POCA, s 330

7.40 POCA provides that a disclosure must be made where there are grounds for suspicion that a person is engaged in money laundering. "Money laundering" is defined in POCA to include an attempt to commit an offence under ss327-329 of POCA There is no duty under s330 to disclose information about the person who unsuccessfully attempts to commit fraud. This is because the attempt was to commit fraud, rather than to commit an offence under ss327-329 of POCA.

7.41 However, as soon as the firm has reasonable grounds to know or suspect that any benefit has been acquired, whether by the fraudster himself or by any third party, so that there is criminal property in existence, then, subject to paragraph 7.42, knowledge or suspicion of money laundering or terrorist financing must be reported to NCIS. Who carried out the criminal conduct, and who benefited from it, or whether the conduct occurred before or after the passing of POCA, is immaterial to the obligation to disclose, but should be reported if known.

POCA, s330(3A)

7.42 In circumstances where neither the identity of the fraudster, nor the location of the criminal property, is known nor is likely to be discovered, limited useable information is available for disclosure. An example of such circumstances would be the theft of a cheque book, debit card, credit card, or charge card, which can lead to multiple low value fraudulent transactions over a short, medium, or long term. In such instances, there is no obligation to make a report to NCIS where none of the following is known or suspected:

- the identity of the person who is engaged in money laundering;
- the whereabouts of any of the laundered property;
- that any of the information that is available would assist in identifying that person, or the whereabouts of the laundered property.

Sanctions and penalties

Regulation 7
POCA s334

7.43 Where a person fails to comply with the obligation under POCA or the

Terrorism Act s21A

Terrorism Act to make disclosures to a nominated officer and/or NCIS as soon as practicable after the information giving rise to the knowledge or suspicion comes to the member of staff, a firm is open to criminal prosecution or regulatory censure. The criminal sanction, under POCA or the Terrorism Act, is a prison term of up to five years, and/or a fine.

Financial sanctions legislation

7.44 Where a firm fails to comply with the obligations to freeze funds, not to make funds, economic resources and, in relation to suspected terrorists, financial services, available to listed persons or to report knowledge or suspicion, it is open to prosecution.

Consent

7.45 Care should be taken that the requirement to obtain consent for a particular transaction does not lead to the unnecessary freezing of a customer's account, thus affecting other, non-suspicious transactions.

Consent under POCA

POCA s 336

7.46 Reporting before or reporting after the event are not equal options which a firm can choose between. Where a customer instruction is received prior to a transaction or activity taking place, or arrangements being put in place, and there are grounds for knowledge or suspicion that the transaction, arrangements, or the funds/property involved, may relate to money laundering, a report must be made to NCIS and consent sought to proceed with that transaction or activity. In such circumstances, it is an offence for a nominated officer to consent to a transaction or activity going ahead within the seven working day notice period from the working day following the date of disclosure, unless NCIS gives consent. Where urgent consent is required, use should be made of the process referred to in paragraph 7.38 above.

POCA ss 330 (6)(a), 331(6), 338 (3)(b)

7.47 When an activity or transaction (or a related transaction) which gives rise to concern is already within an automated clearing or settlement system, where a delay would lead to a breach of a contractual obligation, or where it would breach market settlement or clearing rules, the nominated officer may need to let the transaction proceed and report it later. Where the nominated officer intends to make a report, but delays doing so for such reasons, POCA provides a defence from making a report where there is a reasonable excuse for not doing so. However, it should be noted that this defence is untested by case law, and would need to be considered on a case-by-case basis.

7.48 When consent is needed to undertake a future transaction or activity, or to enter into an arrangement, the disclosure should be faxed to the NCIS Financial Intelligence Division Consent Desk (see NCIS website www.ncis.gov.uk/disclosure.asp) immediately the suspicion is identified. The Consent Desk will apply the ACPO-agreed consent criteria to each submission, carrying out the necessary internal enquiries, and will contact the appropriate law enforcement agency, where necessary, for a consent decision. Once a decision has been

reached, the disclosing firm will be informed of the decision by telephone, and be given a consent number, which should be recorded. A formal consent letter will follow.

POCA, s 335

7.49 In the event that NCIS does not refuse consent within seven working days following the working day after the disclosure is made, the firm may process the transaction or activity, subject to normal commercial considerations. If, however, consent is refused within that period, a restraint order must be obtained by the authorities within a further 31 calendar days (the moratorium period) from the day consent is refused, if they wish to prevent the transaction going ahead after that date. In cases where consent is refused, the law enforcement agency refusing consent should be consulted to establish what information can be provided to the customer.

POCA, s 335(1)(b)

7.50 Consent from NCIS (referred to as a 'notice' in POCA), or the absence of a refusal of consent within seven working days following the working day after the disclosure is made, provides the person handling the transaction or carrying out the activity, or the nominated officer of the reporting firm, with a defence against a possible later charge of laundering the proceeds of crime in respect of that transaction or activity if it proceeds.

7.51 The consent provisions can only apply where there is prior notice to NCIS of the transaction or activity; NCIS cannot provide consent after the transaction or activity has occurred. The receipt of a SAR after the transaction or activity has taken place will be acknowledged by NCIS, and in the absence of any instruction to the contrary, a firm will be free to operate the customer's account under normal commercial considerations until such time as the LEA determines otherwise through its investigation.

7.52 Where there is a need to take urgent action in respect of an account, and the seven working day consent notice period applies, NCIS will endeavour to provide a response in the shortest timeframe, taking into consideration the circumstances of the particular case. Where possible, this will be sooner than the seven working day time limit. If the customer makes strong demands for the transaction/activity to proceed, NCIS will put the firm in touch with the investigating law enforcement agency for guidance, in order to prevent the customer being alerted to the fact of suspicion and that a disclosure has been made. In these circumstances, each case will be dealt with on its merits.

7.53 In order to provide a defence against future prosecution for failing to report, the reasons for any conscious decision not to report should be documented, or recorded electronically. An appropriate report should be made as soon as is practicable after the event, including full details of the transaction, the circumstances precluding advance notice, and to where any money or assets were transferred.

Consent under Terrorism Act

7.54 There are no provisions under the Terrorism Act for consent to be given within a specified period. Where firms have made a report to

NCIS under this Act, no related transaction or activity is allowed to proceed, until the firm has been contacted by NCIS or a law enforcement agency.

Tipping off, and prejudicing an investigation

POCA ss333, 342

7.55 POCA contains two separate sections creating offences of tipping off and prejudicing an investigation. These sections are similar and overlapping, but there are also significant differences between them. It is important for those working in the regulated sector to be aware of the provisions of both sections. The Terrorism Act contains similar offences.

POCA ss 333, 334
Terrorism Act, s 39(4)

7.56 Once an internal or external suspicion report has been made, it is a criminal offence for anyone to release information which is likely to prejudice an investigation. Reasonable enquiries of a customer, conducted in a tactful manner, regarding the background to a transaction or activity that is inconsistent with the normal pattern of activity is prudent practice, forms an integral part of KYC and monitoring, and should not give rise to tipping off.

POCA, ss 342(2), (3)
Terrorism Act s 39(2)

7.57 Where a confiscation investigation, a civil recovery investigation or a money laundering investigation is being, or is about to be, conducted, it is a criminal offence for anyone to release information which is likely to prejudice the investigation. It is also a criminal offence to falsify, conceal, destroy or otherwise dispose of documents which are relevant to the investigation (or to cause or permit these offences). It is, however, a defence if the person does not know or suspect that disclosure is likely to prejudice the investigation, or if the disclosure is made in compliance with other provisions of POCA, or similar enactments.

POCA, ss 335, 336

7.58 The fact that a transaction is notified to NCIS before the event, and NCIS does not refuse consent within seven working days following the day after disclosure is made, or a restraint order is not obtained, does not alter the position so far as 'tipping off' is concerned.

7.59 This means that a firm:

- cannot, at the time, tell a customer that a transaction is being delayed because a report is awaiting consent from NCIS;
- cannot later – unless law enforcement/NCIS agrees, or a court order is obtained permitting disclosure – tell a customer that a transaction or activity was delayed because a report had been made under POCA; and
- cannot tell the customer that law enforcement is conducting an investigation.

7.60 The case of Squirrell Ltd v National Westminster Bank Plc (2005) EWHC 664 (Ch) confirmed the application of these provisions. A copy of the judgement in this case is available at www.jmlsg.org.uk.

7.61 If a firm receives a complaint in these circumstances, it may be unable to provide a satisfactory explanation to the customer, who may then bring a complaint to the Financial Ombudsman Service (FOS). If a firm receives an approach from a FOS casehandler about such a case, the firm should contact a member of the FOS legal department immediately.

7.62 NCIS has confirmed that, in such cases, a firm may tell the FOS' legal department about a report to NCIS and the outcome, on the basis that the FOS will keep the information confidential (which they must do, to avoid any 'tipping off'). The FOS' legal department will then ensure that the case is handled appropriately in these difficult circumstances – liaising as necessary with NCIS. FOS' communications with the customer will still be in the name of a casehandler/ombudsman, so that the customer is not alerted.

Transactions following a disclosure

7.63 Firms must remain vigilant for any additional transactions by, or instructions from, any customer or account in respect of which a disclosure has been made, and should submit further disclosures, and consent applications, to NCIS, as appropriate.

POCA s339A

7.64 In the case of deposit-taking institutions alone, following the reporting of a suspicion, any subsequent transactions (including 'lifestyle' payments) involving the customer or account which was the subject of the original report may only proceed if it is for £250 or less; where the proposed transaction exceeds £250, permission from NCIS is required before it may proceed.

7.65 The significant practical difficulties involved in meeting the legal requirements set out in paragraph 7.64 are being discussed with the authorities. Further guidance on meeting these obligations will be provided once these discussions are satisfactorily completed. Firms should refer to the JMLSG website (www.jmlsg.org.uk) for such further guidance.

POCA, ss 337 (1), 338(4)
Terrorism Act s21B

7.66 The disclosure provisions within POCA and the Terrorism Act protect persons making SARs from any potential breaches of confidentiality, whether imposed under contract, statute (for example, the Data Protection Act), or common law. These provisions apply to those inside and outside the regulated sector, and include reports that are made voluntarily, in addition to reports made in order to fulfil reporting obligations.

7.67 NCIS' consent following a disclosure is given to the reporting institution solely in relation to the money laundering offences. Consent provides the staff involved with a defence against a charge of committing a money laundering offence under ss 327-329 of POCA. It is not intended to override normal commercial judgement, and a firm is not committed to continuing the relationship with the customer if such action would place the reporting institution at

commercial risk.

7.68 Whether to terminate a relationship is essentially a commercial decision, and firms must be free to make such judgements. However, in the circumstances envisaged here a firm should consider liaising with the law enforcement investigating officer to consider whether it is likely that termination would alert the customer or prejudice an investigation in any other way. If there is continuing suspicion about the customer or the transaction or activities, and there are funds which need to be returned to the customer at the end of the relationship, firms should ask NCIS for consent to repatriate the funds.

7.69 Where the firm knows that the funds in an account derive from criminal activity, or that they arise from fraudulent instructions, the account must be frozen. Where it is believed that the account holder may be involved in the fraudulent activity that is being reported, then the account may need to be frozen, but the need to avoid tipping off would have to be considered.

7.70 When an enquiry is under investigation, the investigating officer may contact the nominated officer to ensure that he has all the relevant information which supports the original disclosure. This contact may also include seeking supplementary information or documentation from the reporting firm and from other sources by way of a court order. The investigating officer will therefore work closely with the nominated officer who will usually receive direct feedback on the stage reached in the investigation. There may, however, be cases when the nominated officer cannot be informed of the state of the investigation, either because of the confidential nature of the enquiry, or because it is sub judice.

7.71 Where the firm does not wish to make the payment requested by a customer, it should notify NCIS of this fact and request them to identify any information that they are prepared to allow the firm to disclose to the court and to the customer in any proceedings brought by the customer to enforce payment. NCIS should be reminded that:

- the court may ask him to appear before it to justify his position if he refuses to consent to adequate disclosure; and
- the refusal to allow adequate disclosure is likely to make it apparent to the customer that the firm's reasons for refusing payment are due to a law enforcement investigation.

7.72 If the investigating officer is able to consent to the disclosure of adequate information to permit the firm to defend itself against any proceedings brought by the customer, that information may be shown to the court and to the customer without a tipping off offence being committed. In the event that the firm and the investigating officer cannot reach agreement on the information to be disclosed, an application can be made to the court for directions and/or an interim declaration.

7.73 In any proceedings that might be brought by the customer, the firm

may only disclose to the court and the other side such information as has been consented to by the investigating officer or the court.

Constructive trusts

7.74 The duty to report suspicious activity and to avoid tipping off could, in certain circumstances, lead to a potential conflict between the reporting firm's responsibilities under the criminal law and its obligations under the civil law, as a constructive trustee, to a victim of a fraud or other crimes.

7.75 A firm's liability as a constructive trustee under English law can arise when it either knows that the funds held by the firm do not belong to its customer, or is on notice that such funds may not belong to its customer. The firm will then take on the obligation of a constructive trustee for the rightful owner of the funds. If the firm pays the money away other than to the rightful owner, and it is deemed to have acted dishonestly in doing so, it may be held liable for knowingly assisting a breach of trust.

7.76 Having a suspicion that it considers necessary to report under the money laundering or terrorist financing legislation may, in certain circumstances, indicate that the firm knows that the funds do not belong to its customer, or is on notice that they may not belong to its customer. However, such suspicion may not itself be enough to cause a firm to become a constructive trustee. Case law suggests that a constructive trust will only arise when there is some evidence that the funds belong to someone other than the customer.

7.77 If, when making a suspicious activity report, a firm knows that the funds which are the subject of the report do not belong to its customer, or has doubts that they do, this fact, and details of the firm's proposed course of action, should form part of the report that is forwarded to NCIS.

7.78 If the customer wishes subsequently to withdraw or transfer the funds, the firm should, in the first instance, contact NCIS for consent. Consent from NCIS will, however, not necessarily protect the firm from the risk of committing a breach of constructive trust by transferring funds. In situations where the assistance of the court is necessary, it is open to a firm to apply to the court for directions as to whether the customer's request should be met. However, the powers of the court are discretionary, and should only be used in cases of real need. That said, it is unlikely that a firm acting upon the direction of a court would later be held to have acted dishonestly such as to incur liability for breach of constructive trust.

7.79 Although each case must be considered on its facts, the effective use of KYC information, and the identification of appropriate underlying beneficial owners, can help firms to guard against a potential constructive trust suit arising out of fraudulent misuse or misappropriation of funds.

7.80 It should be noted that constructive trust is not a concept recognised in Scots law.

Data Protection - Subject Access Requests, where a suspicion report has been made

7.81 Occasionally, a Subject Access Request under the Data Protection Act will include within its scope one or more money laundering/terrorist financing reports which have been submitted in relation to that customer. Although it might be instinctively assumed that to avoid tipping off there can be no question of ever including this information when responding to the customer, an automatic assumption to that effect must not be made, even though in practice it will only rarely be decided that it is appropriate to include it. However, all such requests must be carefully considered on their merits in line with the principles below.

7.82 The following guidance is drawn from guidance issued by HM Treasury in April 2002. This guidance – The UK's Anti-Money Laundering Legislation and the Data Protection Act 1998 – Guidance notes for the financial sector - is available at www.hm-treasury.gov.uk/documents/financial_services/fin_index.cfm.

Data Protection Act, s 7

7.83 On making a request in writing (a Subject Access Request) to a data controller (i.e. any organisation that holds personal data), an individual is normally entitled to:

- be informed whether the data controller is processing (which includes merely holding) his personal data; and if so
- be given a description of that data, the purposes for which they are being processed and to whom they are or may be disclosed; and
- have communicated to him in an intelligible form all the information that constitutes his personal data and any information available to the data controller as to the source of that data.

Data Protection Act, s29

7.84 Section 29 of the Data Protection Act provides that personal data are exempt from disclosure under section 7 of the Act in any case where the application of that provision would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders. However, even when relying on an exemption, data controllers (i.e., firms) should provide as much information as they can in response to a Subject Access Request.

7.85 Where a firm withholds a piece of information in reliance on the section 29 exemption, it is not obliged to tell the individual that any information has been withheld. The information in question can simply be omitted and no reference made to it when responding to the individual who has made the request.

7.86 To establish whether disclosure would be likely to prejudice an investigation or a potential investigation, firms should approach

NCIS for guidance; NCIS will usually discuss this with past or present investigating agencies/officers. This may also involve cases that are closed, but where related investigations may still be continuing.

7.87 Each Subject Access Request must be considered on its own merits in determining whether, in a particular case, the disclosure of a suspicion report is likely to prejudice an investigation and, consequently, constitute a tipping-off offence. In determining whether the section 29 exemption applies, it is legitimate to take account of the fact that although the disclosure does not, in itself, provide clear evidence of criminal conduct when viewed in isolation, it might ultimately form part of a larger jigsaw of evidence in relation to a particular crime. It is also legitimate to take account generally of the confidential nature of suspicious activity reports when considering whether or not the exemption under section 29 might apply.

7.88 In cases where the fact that a disclosure had been made had previously been reported in legal proceedings, or in a previous investigation, and the full contents of such a disclosure had been revealed, then it is less likely that the exemption under section 29 would apply. However, caution should be exercised when considering disclosures that have been made in legal proceedings for the purposes of the section 29 exemption, as often the disclosure will have been limited strictly to matters relevant to those proceedings, and other information contained in the original report may not have been revealed.

7.89 To guard against a tipping-off offence, nominated officers should ensure that no information relating to SARs is released to any person without the nominated officer's authorisation. Further consideration may need to be given to suspicion reports received internally that have not been submitted to NCIS. A record should be kept of the steps that have been taken in determining whether disclosure of a report would involve tipping off and/or the availability of the section 29 exemption.

Data Protection Act s 7(8)

7.90 Firms should bear in mind that there is a statutory deadline for responding to Subject Access Requests of 40 days from their receipt by the firm. The timing of enquiries to NCIS, or any other party, to obtain further information, or for guidance on whether disclosure would be likely to prejudice an investigation, should be made with this deadline in mind.

CHAPTER 8

STAFF AWARENESS, TRAINING AND ALERTNESS

Key points in this chapter

- **Relevant law/regulation**
  - Regulation 3 (1)
  - POCA ss 327-329, 330 (6),(7), 333, 334(2)
  - Terrorism Act ss 18, 21A
  - SYSC 3.2.6G(1) G
  - TC, Chapter 1
  - Financial sanctions legislation
- **Core obligations**
  - Relevant employees should be
    - made aware of the risks of money laundering and terrorist financing, the relevant legislation, and their obligations under that legislation
    - made aware of the identity and responsibilities of the firm's nominated officer and MLRO
    - trained in the firm's procedures and in how to recognise and deal with potential money laundering or terrorist financing transactions or activity
  - Staff training should be given at regular intervals, and details recorded
  - MLRO is responsible for oversight of the firm's compliance with its requirements in respect of staff training
  - The relevant director or senior manager has overall responsibility for the establishment and maintenance of effective training arrangements
- **Actions required, to be kept under regular review**
  - Provide appropriate training to make relevant employees aware of money laundering and terrorist financing issues, including how these crimes operate and how they might take place through the firm
  - Ensure that relevant employees are provided with information on, and understand, the legal position of the firm and of individual members of staff, and of changes to these legal positions
  - Consider providing relevant employees with case studies and examples related to the firm's business
  - Train relevant employees in how to operate a risk-based approach to AML/CFT

Why focus on staff awareness and training?

8.1 One of the most important controls over the prevention and detection of money laundering is to have staff who are alert to the risks of money laundering/terrorist financing and well trained in the identification of unusual activities or transactions which may prove to be suspicious.

8.2 The effective application of even the best designed control systems can be quickly compromised if the staff applying the systems are not adequately trained. The effectiveness of the training will therefore be important to the success of the firm's AML/CFT strategy.

8.3 It is essential that firms implement a clear and well articulated policy for ensuring that relevant employees are aware of their obligations in respect of the prevention of money laundering and terrorist financing

and for training them in the identification and reporting of anything that gives grounds for suspicion. This is especially important for staff who handle customer transactions or instructions. Temporary and contract staff carrying out such functions should also be covered by these training programmes.

POCA ss327-329, 334 (2) Terrorism Act ss18, 21A

8.4 Under POCA and the Terrorism Act, individual members of staff face criminal penalties if they are involved in money laundering or terrorist financing, or if they do not report their knowledge or suspicion of money laundering or terrorist financing where there are reasonable grounds for their knowing or suspecting such activity. It is important, therefore, that staff are made aware of these obligations, and are given training in how to discharge them.

General legal and regulatory obligations

TC 1.2.1 G

8.5 The FSA's Training and Competence Sourcebook (TC) contains high-level commitments for all FSA-regulated businesses and these provide an important background to the provision of money laundering awareness and training.

8.6 The firm's commitments to training and competence are that:

- its employees are competent;
- its employees remain competent for the work they do;
- its employees are appropriately supervised;
- its employees' competence is regularly reviewed;
- the level of competence is appropriate to the nature of the business.

Regulation 3 (1)(c)

8.7 The obligations on senior management and the firm in relation to staff awareness and staff training address each requirement separately. ML Regulations require firms to ensure, first, that relevant employees are made aware of the provisions of named pieces of relevant legislation (specifically, the ML Regulations, Part 7 of POCA and sections 18 and 21A of the Terrorism Act) and the obligations placed on staff and firms under these and, secondly, that they are given training in how to recognise and deal with transactions which may be related to money laundering or terrorist financing.

SYSC 3.2.6I(1) R

SYSC 3.2.6G(1) G

8.8 The FSA specifically requires the MLRO to have responsibility for ensuring that the firm's systems and controls include appropriate training for the firm's employees in relation to money laundering.

POCA, s330 (6) and (7)

8.9 Where a staff member is held to have had reasonable grounds for knowing or suspecting money laundering, but failed to make a disclosure, he will have a defence under POCA if he does not know or suspect, and has not been provided with AML training by his employer. No such defence is available under the Terrorism Act.

Regulation 3(1)(c)

8.10 Firms have an obligation under the ML Regulations to take appropriate measures in relation to staff training and awareness. A successful defence by a staff member under POCA may leave the firm open to

prosecution or regulatory sanction for not having adequate training and awareness arrangements. Firms should therefore not only obtain acknowledgement from the individual that they have received the necessary training, but should also take steps to assess its effectiveness.

Responsibilities of the firm, and its staff

Responsibilities of senior management

Regulation 3(1)

8.11 Senior management must be aware of their obligations under the ML Regulations to establish appropriate systems and procedures to forestall and prevent money laundering and terrorist financing. It is an offence not to have appropriate systems in place, whether or not money laundering or terrorist financing has taken place.

Regulation 3(1)(c)
SYSC 3.2.6H R
SYSC 3.2.6I R

8.12 The relevant director or senior manager has overall responsibility for the establishment and maintenance of effective training arrangements. The MLRO is responsible for oversight of the firm's compliance with its requirements in respect of training, including taking reasonable steps to ensure that the firm's systems and controls include appropriate training for employees in relation to money laundering. Awareness and training arrangements specifically for senior management, the MLRO and the nominated officer should therefore also be considered.

8.13 Firms should take reasonable steps to ensure that relevant employees are aware of:

- their responsibilities under the firm's arrangements for the prevention of money laundering and terrorist financing, including those for obtaining sufficient evidence of identity, recognising and reporting knowledge or suspicion of money laundering or terrorist financing;
- the identity and responsibilities of the nominated officer and the MLRO; and
- the potential effect on the firm, on its employees personally and on its clients, of any breach of that law.

8.14 The firm's approach to training should be built around ensuring that the content and frequency of training reflects the risk assessment of the products and services of the firm and the specific role of the individual.

Responsibilities of staff

8.15 Staff should be made aware of their personal responsibilities and those of the firm at the start of their employment. These responsibilities should be documented in such a way as to enable staff to refer to them as and when appropriate throughout their employment. In addition, selected or relevant employees should be given regular appropriate training in order to be aware of:

- the criminal law relating to money laundering and terrorist financing;
- the ML Regulations;

- the FSA Rules;
- industry guidance;
- the risks money laundering and terrorist financing pose to the business;
- the vulnerabilities of the firm's products and services; and
- the firm's policies and procedures in relation to the prevention of money laundering and terrorist financing.

8.16 Where staff move between jobs, or change responsibilities, their training needs may change. Ongoing training should be given at appropriate intervals to all relevant employees.

Legal obligations on staff

POCA, ss327 – 329, 330-332 Terrorism Act ss18, 21A

8.17 There are several sets of offences under POCA and the Terrorism Act which directly affect staff – the various offences of money laundering or terrorist financing, failure to report possible money laundering or terrorist financing, tipping off, and prejudicing an investigation.

POCA, ss327 – 329 Terrorism Act s18

8.18 The offences of involvement in money laundering or terrorist financing apply to all staff, whether or not the firm is in the regulated sector. This would include staff of general insurance firms and mortgage intermediaries. The offences have no particular application to those engaged in specific customer-related activities – that is, they also apply to back office staff.

POCA ss330-332 Terrorism Act s21A

8.19 The offence under POCA and the Terrorism Act of failing to report applies to staff in the regulated sector, and to all nominated officers, whether in the regulated sector or not. Although general insurance firms and mortgage intermediaries are not in the regulated sector, if they have opted to appoint a nominated officer, the obligations on nominated officers apply to these appointees.

POCA s333

8.20 Once a report has been made to the firm's nominated officer, it is an offence to make any further disclosure that is likely to prejudice an investigation.

Training in the firm's procedures

8.21 The firm should train staff, in particular, on how its products and services may be used as a vehicle for money laundering or terrorist financing, and in the firm's procedures for managing this risk. They will also need information on how the firm may itself be at risk of prosecution if it processes transactions without the consent of NCIS where a SAR has been made.

8.22 Relevant employees should be trained in what they need to know in order to carry out their particular role. Staff involved in customer acceptance, in customer servicing, or in settlement functions will need different training, tailored to their particular function. This may involve making them aware of the importance of the "know your customer" requirements for money laundering prevention purposes, and of the respective importance of customer ID procedures, obtaining additional KYC information and monitoring customer activity. The awareness raising and training in this respect should cover the need to

verify the identity of the customer, and circumstances when it should be necessary to obtain appropriate additional customer information in the context of the nature of the transaction or business relationship concerned.

8.23 Relevant employees should also be made aware of the particular circumstances of customers who present a higher risk of money laundering or terrorist financing, or who are financially excluded. Training should include how identity should be verified in such cases, what additional steps should be taken, and/or what local checks can be made.

Staff alertness to specific situations

8.24 Sufficient training will need to be given to all relevant employees to enable them to recognise when a transaction is unusual or suspicious, or when they should have reasonable grounds to know or suspect that money laundering or terrorist financing is taking place.

8.25 The set of circumstances giving rise to an unusual transaction or arrangement, and which may provide reasonable grounds for concluding that it is suspicious, will depend on the customer and the product or service in question. Illustrations of the type of situation that may be unusual, and which in certain circumstances might give rise to reasonable grounds for suspicion, are:

- transactions which have no apparent purpose, or which make no obvious economic sense (including where a person makes a loss against tax), or which involve apparently unnecessary complexity;
- the use of non-resident accounts, companies or structures in circumstances where the customer's needs do not appear to support such economic requirements;
- where the transaction being requested by the customer, or the size or pattern of transactions, is, without reasonable explanation, out of the ordinary range of services normally requested or is inconsistent with the experience of the firm in relation to the particular customer;
- dealing with customers not normally expected in that part of the business;
- transfers to and from high-risk jurisdictions, without reasonable explanation, which are not consistent with the customer's declared foreign business dealings or interests;
- where a series of transactions are structured just below a regulatory threshold;
- where a customer who has entered into a business relationship with the firm uses the relationship for a single transaction or for only a very short period of time;
- unnecessary routing of funds through third party accounts;
- unusual investment transactions without an apparently discernible

profitable motive.

8.26 Issues around the customer identification process that may raise concerns include such matters as the following:

- Has the customer refused, or appeared particularly reluctant, to provide the information requested without reasonable explanation?
- Do you understand the legal and corporate structure of the client entity, and its ownership and control, and does the structure appear to make sense?
- Is the staff member aware of any inconsistencies between locations and other information provided?
- Is the area of residence given consistent with other profile details, such as employment?
- Does an address appear vague or unusual – e.g., an accommodation agency, a professional 'registered office' or a trading address?
- Does it make sense for the customer to be opening the account or relationship in the jurisdiction that he is asking for?
- Is the information that the customer has provided consistent with the banking or other services or facilities that he is seeking?
- Does the supporting documentation add validity to the other information provided by the customer?
- Does the customer have other banking or financial relationships with the firm, and does the collected information on all these relationships appear consistent?
- Does the client want to conclude arrangements unusually urgently, against a promise to provide information at a later stage, which is not satisfactorily explained?
- Has the customer suggested changes to a proposed arrangement in order to avoid providing certain information?

8.27 Staff should also be on the lookout for such things as:

- sudden, substantial increases in cash deposits or levels of investment, without adequate explanation;
- transactions made through other banks or financial firms;
- regular large, or unexplained, transfers to and from countries known for money laundering, terrorism, corruption or drug trafficking;
- large numbers of electronic transfers into and out of the account;
- significant/unusual/inconsistent deposits by third parties; and
- reactivation of dormant account(s).

8.28 Staff awareness and training programmes may also include the nature of terrorism funding and terrorist activity, in order that staff are alert to customer transactions or activities that might be terrorist-related.

8.29 Examples of activity that might suggest to staff that there could be potential terrorist activity include:

- round sum deposits, followed by like-amount wire transfers;
- frequent international ATM activity;

- no known source of income;
- use of wire transfers and the internet to move funds to and from high-risk countries and geographic locations;
- frequent address changes;
- purchases of military items or technology; and
- media reports on suspected, arrested terrorists or groups.

8.30 It is important that staff are appropriately made aware of changing behaviour and practices amongst money launderers and those financing terrorism. As well as their regular series of publications on the typologies of financial crime, FATF's Guidance for Financial Institutions in Detecting Terrorist Financing issued in April 2002 contains an in-depth analysis of the methods used in the financing of terrorism and the types of financial activities constituting potential indicators of such activities. These documents are available from FATF's website www.fatf-gafi.org.

8.31 NCIS publishes a range of material on its website www.ncis.gov.uk, such as threat assessments and risk profiles, of which firms may wish to make their staff aware. The information on this website could usefully be incorporated into firms' training materials.

8.32 Illustrations, based on real cases, of how individuals and organisations might raise funds and use financial sector products and services for money laundering or to finance terrorism, are available on the JMLSG website, www.jmlsg.org.uk.

Staff based outside the UK

8.33 Where activities relating to UK business operations are undertaken by processing staff outside the UK, those staff must be made aware of and trained to follow the AML/CFT policies and procedures applicable to the UK operations. It is important that any local training and awareness obligations are also met, where relevant.

Training methods and assessment

8.34 There is no single solution when determining how to deliver training; a mix of training techniques may be appropriate. On-line learning systems can often provide an adequate solution for many employees, but there will be classes of employees for whom such an approach is not suitable. Focused classroom training for higher risk or minority areas can be more effective. Relevant videos always stimulate interest, but continually re-showing the same video may produce diminishing returns.

8.35 Procedures manuals, whether paper or intranet based, are useful in raising staff awareness and in supplementing more dedicated forms of training, but their main purpose is to provide ongoing reference and they are not generally written as training material.

8.36 Ongoing training should be given at appropriate intervals to all relevant employees. Particularly in larger firms, this may take the

form of a rolling programme.

8.37 Whatever the approach to training, it is vital to establish comprehensive records (see paragraph 9.20) to monitor who has been trained, when they received the training, the nature of the training given and its effectiveness.

CHAPTER 9

RECORD KEEPING

Key points in this chapter
➢ **Relevant law/regulation** ▪ Data Protection Act ▪ Regulation 3 ▪ Regulation 6 ▪ SYSC Chapter 3
➢ **Core obligations** ▪ Firms must retain: • copies of the evidence they obtained of a customer's identity, for five years after the end of the customer relationship • details of customer transactions for five years from the date of the transaction ▪ Firms should retain: • details of actions taken in respect of internal and external suspicion reports • details of information considered by the nominated officer in respect of an internal report where no external report is made
➢ **Actions required, to be kept under regular review** ▪ Firms should maintain appropriate systems for retaining records ▪ Firms should maintain appropriate systems for making records available when required, within the specified timescales

General legal and regulatory requirements

Regulation 3 (1)(a), Regulation 6

9.1 This chapter provides guidance on appropriate record keeping procedures that will meet a firm's obligations in respect of the prevention of money laundering and terrorist financing. There are general obligations on firms to maintain appropriate records and controls more widely in relation to their business; this guidance is not intended to replace or interpret such wider obligations.

9.2 Record keeping is an essential component of the audit trail that the ML Regulations and FSA Rules seek to establish in order to assist in any financial investigation and to ensure that criminal funds are kept out of the financial system, or if not, that they may be detected and confiscated by the authorities.

Regulation 6
SYSC 3.2.20R

9.3 Firms must retain records concerning customer identification and transactions as evidence of the work they have undertaken in complying with their legal and regulatory obligations, as well as for use as evidence in any investigation conducted by law enforcement. FSA-regulated firms must take reasonable care to make and keep adequate records appropriate to the scale, nature and complexity of their businesses.

Regulation 6 (5)

9.4 Where a firm has an appointed representative, it must ensure that the representative complies with the record keeping obligations under the ML Regulations. This principle would also apply where the record

keeping is delegated in any way to a third party (such as to an administrator or an introducer).

What records have to be kept?

9.5 The precise nature of the records required is not specified in the legal and regulatory regime. The objective is to ensure that a firm meets its obligations and that, in so far as is practicable, in any subsequent investigation the firm can provide the authorities with its section of the audit trail.

9.6 The firm's records should cover:

- Customer information
- Transactions
- Internal and external suspicion reports
- MLRO annual (and other) reports
- Information not acted upon
- Training and compliance monitoring
- Information about the effectiveness of training

Customer information

Regulation 6 (2)(a)

9.7 In relation to the evidence of a customer's identity, firms must keep the following records:

(i) a copy of the information dataset collected and verification evidence obtained; or

(ii) information as to where a copy of the evidence of identity may be obtained; or

(iii) when it is not reasonably practicable to comply with (i) or (ii), information enabling the evidence of identity to be re-obtained.

9.8 When a firm has concluded that it should treat a client as financially excluded for the purposes of customer identification, it should keep a record of the reasons for doing so.

9.9 A firm may often hold additional information in respect of a customer for the purposes of wider customer due diligence.

9.10 Where the individual presents himself to the firm, or at one of its branches, he may produce the necessary identity proof(s), for the firm to take and retain copies. In circumstances (such as where verification is carried out at a customer's home and photocopying facilities are not available) where it would not be possible to take a copy of the identity proof, a record should be made of the type of document and its number, date and place of issue, so that, if necessary, the document may be re-obtained from its source of issue.

Regulation 6 (3)

9.11 Records of identification evidence must be kept for a period of at least five years after the relationship with the customer has ended. The date the relationship with the customer ends is the date:

- a one-off transaction, or the last in a series of linked transactions, is carried out; or
- the business relationship ended, i.e. the closing of the account or accounts.

9.12 Where documents verifying the identity of a customer are held in one part of a group, they do not need to be held in duplicate form in another. The records do, however, need to be accessible to the nominated officer and the MLRO and to all areas that have contact with the customer, where these areas seek to rely on this evidence, or where they may be called upon by law enforcement to produce them.

9.13 When an introducing branch or subsidiary ceases to trade or have a business relationship with a customer, as long as his relationship with other group members continues, particular care needs to be taken to retain, or hand over, the appropriate customer records. Similar arrangements need to be made if a company holding relevant records ceases to be part of the group. This will also be an issue if the record keeping has been delegated to a third party.

Transactions

Regulation 6 (2)(b)

9.14 All transactions carried out on behalf of or with a customer in the course of relevant business must be recorded within the firm's records. Transaction records in support of entries in the accounts, in whatever form they are used, e.g. credit/debit slips, cheques, should be maintained in a form from which a satisfactory audit trail may be compiled where necessary, and which may establish a financial profile of any suspect account or customer.

Regulation 6 (4)

9.15 Records of all transactions relating to a customer must be retained for a period of five years from the date of the transaction.

9.16 In the case of managers of investment funds or issuers of electronic money, where there may be no business relationship as defined in the ML Regulations, but the customer may nevertheless carry out further one-off transactions in the future, it is recommended that all records be kept for five years after the investment has been fully sold or funds disbursed.

Internal and external reports

9.17 A firm should make and retain:

- records of actions taken under the internal and external reporting requirements; and
- when the nominated officer has considered information or other material concerning possible money laundering, but has not made a report to NCIS, a record of the other material that was considered.

9.18 In addition, copies of any SARs made to NCIS should be retained.

9.19 Records of all internal and external reports should be retained for five years from the date the report was made.

Other

9.20 A firm's records should include:

(a) in relation to training:

- dates AML training was given;
- the nature of the training;
- the names of the staff who received training; and
- the results of the tests undertaken by staff, where appropriate.

(b) in relation to compliance monitoring -

- reports by the MLRO to senior management; and
- records of consideration of those reports and of any action taken as a consequence.

Form in which records have to be kept

9.21 Most firms have standard procedures which they keep under review, and will seek to reduce the volume and density of records which have to be stored, whilst still complying with statutory requirements. Retention may therefore be:

- by way of original documents;
- by way of photocopies of original documents;
- on microfiche;
- in scanned form;
- in computerised or electronic form.

9.22 The record retention requirements are the same, regardless of the format in which they are kept, or whether the transaction was undertaken by paper or electronic means.

9.23 Firms involved in mergers, take-overs or internal reorganisations need to ensure that records of identity verification and transactions are readily retrievable for the required periods when rationalising computer systems and physical storage arrangements.

Location

9.24 The ML Regulations do not state where relevant records should be kept, but the overriding objective is for firms to be able to retrieve relevant information without undue delay.

9.25 Where identification records are held outside the UK, it is the responsibility of the UK firm to ensure that the records available do in fact meet UK requirements. No secrecy or data protection legislation should restrict access to the records either by the UK firm freely on request, or by UK law enforcement agencies under court order or relevant mutual assistance procedures. If it is found that such restrictions exist, copies of the underlying records of identity should, wherever possible, be sought and retained within the UK.

9.26 Firms should take account of the scope of AML/CFT legislation in

other countries, and should ensure that group records kept in other countries that are needed to comply with UK legislation are retained for the required period.

9.27 Records relating to ongoing investigations should, where possible, be retained until the relevant law enforcement agency has confirmed that the case has been closed. However, if a firm has not been advised of an ongoing investigation within five years of the disclosure being made, the records may be destroyed in the normal course of the firm's records management policy.

9.28 There is tension between the provisions of the ML Regulations and data protection legislation; the nominated officer and the MLRO must have due regard to both sets of obligations.

9.29 When setting document retention policy, financial sector businesses must weigh the statutory requirements and the needs of the investigating authorities against normal commercial considerations. When original vouchers are used for account entry, and are not returned to the customer or his agent, it is of assistance to the law enforcement agencies if these original documents are kept for at least one year to assist in forensic analysis. This can also provide evidence for firms when conducting their own internal investigations. However, this is not a requirement of the AML legislation and there is no other statutory requirement in the UK that would require the retention of these original documents.

Sanctions and penalties

Regulation 3

9.30 Where the record keeping obligations under the ML Regulations are not observed, a firm or person is open to prosecution, including imprisonment for up to two years and/or a fine, or regulatory censure.

GLOSSARY OF TERMS

Term/expression	Meaning
Approved person	A person in relation to whom the FSA has given its approval under s 59 of FSMA for the performance of a controlled function. [FSA Glossary of definitions].
Applicant for business	Any natural or legal person seeking to form a business relationship, or carry out a one-off transaction, with another person acting in the course of relevant business carried on by that other person in the United Kingdom.
Appropriate person	Someone in a position of responsibility, who knows, and is known by, a customer, and may reasonably confirm the customer's identity. It is not possible to give a definitive list of such persons, but the following may assist firms in determining who is appropriate in any particular case: ➢ The Passport Office has published a list of those who may countersign passport applications: see www.ukpa.gov.uk/passport_countersign.asp ➢ Others might include members of a local authority, staff of a higher or further education establishment, or a hostel manager.
Bank of England Sanctions Notices and News Releases	Notices issued by the Bank of England advising firms of additions to the UN Consolidated List maintained under Security Council resolution 1390 (2002) and to the list of persons and entities subject to EC Regulation 2580/2001.
Basel CDD paper	Basel Committee Customer Due Diligence paper, published in October 2001.
Basel Consolidated KYC Risk Management Paper	Basel Committee paper on Consolidated KYC Risk Management, published in October 2004.
Basel Committee	Basel Committee on Banking Supervision.
Beneficial owner(s)	The natural person(s) who ultimately owns or controls the customer and/or the legal entity on whose behalf a transaction or activity is being conducted.
Controlled function	A function relating to the carrying on of a regulated activity by a firm which is specified under s 59 of FSMA, in FSA's table of controlled functions.
Comparable jurisdiction	A jurisdiction (other than an EEA state) whose law contains comparable provisions to those contained in the EU Money Laundering Directive [see JMLSG website www.jmlsg.org.uk].
Criminal property	Property which constitutes a person's benefit from criminal conduct or which represents such a benefit (in whole or part and

	whether directly or indirectly), and the alleged offender knows or suspects that the property constitutes or represents such a benefit. [POCA s 340 (3)]
Criminal conduct	Conduct which constitutes an offence in any part of the United Kingdom, or would constitute an offence in any part of the United Kingdom if it occurred there. [POCA s 340 (2)]
Customer	In relation to an FSA-regulated firm, a customer is a person who is using, or may be contemplating using, any of the services provided by the firm. As noted in paragraph 5.2.3, this is not the definition of customer that applies in SYSC. [FSMA, s 59 (11)]
EU Money Laundering Directives	The First Money Laundering Directive, adopted in 1991 (91/308/EEC), was designed to harmonise the various national laws relating to money laundering, and thus avoid the potential for regulatory arbitrage. The Directive required anti money laundering systems and controls – principally in relation to customer identification, record keeping and reporting suspicious transactions - to be in place in firms that carried on specified financial business. A Second Money Laundering Directive, adopted in 2001 (2001/97/EC), widened the scope of predicate offences, and extended the application of the First Directive to a range of non-financial activities and professions.
EC Sanctions Regulation	Regulation 2580/2001, on specific restrictive measures directed against certain persons and entities with a view to combating terrorism.
FATF Recommendations	A series of Forty Recommendations on the structural, supervisory and operational procedures that countries should have in place to combat money laundering, issued by the FATF. The Forty Recommendations were originally published in 1990, revised in 1996, and last revised in October 2004. The FATF Forty Recommendations have been recognised by the International Monetary Fund and the World Bank as the international standards for combating money laundering.
FATF Special Recommendations	FATF issued a series of Special Recommendations on Terrorist Financing in October 2001, and October 2004. The FATF Special Recommendations have been recognised by the International Monetary Fund and the World Bank as the international standards for combating the financing of terrorism.
Financial services business	Business that is covered in Regulation 2(2)(a) – (e) of the ML Regulations.
FSA-regulated firm	A firm holding permission from the FSA under FSMA, Part IV, to carry on certain of the activities listed in FSMA, Schedule 2.

Government-issued	Issued by a central government department or by a local government authority or body.
Guidance Paper 5	Guidance Paper No 5: Guidance paper on anti-money laundering and combating the financing of terrorism, issued by IAIS in October 2004.
Identification	Ascertaining the name of, and other relevant information about, an applicant for business.
IOSCO Principles paper	IOSCO paper 'Principles on Client Identification and Beneficial Ownership for the Securities Industry', published May 2004.
Mind and management	Those individuals who, individually or collectively, exercise practical control over a non-personal entity.
ML Regulations	The Money Laundering Regulations 2003 [SI 2003/3075].
Money laundering	An act which: ➢ constitutes an offence under ss 327, 328 or 329 of POCA or ➢ constitutes an attempt, conspiracy or incitement to commit such an offence or ➢ constitutes aiding, abetting, counselling or procuring the commission of such an offence or ➢ would constitute an offence specified above if done in the United Kingdom. [POCA, s 340 (11)] A person also commits an offence of money laundering if he enters into or becomes concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property: ➢ by concealment; ➢ by removal from the jurisdiction; ➢ by transfer to nominees; or ➢ in any other way. [Terrorism Act, s 18]
Money service operator	A person who carries on the business of a bureau de change, transmitting money (or any representation of monetary value) by any means or cashing cheques that are made payable to customers. [ML Regulation 2 (1)]
Nominated officer	A person in a firm or organisation nominated by the firm or organisation to receive disclosures under Regulation 7 and/or s 330 of POCA from others within the firm or organisation who know or suspect that a person is engaged in money laundering. Similar provisions apply under the Terrorism Act.
One-off transaction	Any transaction other than one carried out in the course of an existing business relationship. [ML Regulation 2]

Politically exposed persons	Natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons. [3 MLD, Article 3 (8)]
Regulated Activities Order	Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (SI 2001/544).
Regulated activity	Activities set out in the Regulated Activities Order, made under s 22 and Schedule 2 of FSMA.
Regulated sector	Persons and firms which carry on relevant business,which is business subject to the ML Regulations. [ML Regulation 2(2)]
Relevant business	Business that is covered in Regulation 2 (2) of the ML Regulations.
Senior management	The directors and senior managers (or equivalent) of a firm who are responsible, either individually or collectively, for management and supervision of the firm's business.
Senior manager	An individual, other than a director (or equivalent), who is employed by the firm, and to whom the Board (or equivalent) or a member of the Board, has given responsibility, either alone or jointly with others, for management and supervision.
Terrorism Act	Terrorism Act 2000, as amended by the Anti-terrorism, Crime and Security Act 2001.
Terrorist property	➢ Money or other property which is likely to be used for the purposes of terrorism (including any resources of a proscribed organisation); or ➢ Proceeds of the commission of acts of terrorism; or ➢ Proceeds of acts carried out for the purposes of terrorism "Proceeds of an act" includes a reference to any property which wholly or partly, and directly or indirectly, represents the proceeds of the act (including payments or other rewards in connection with its commission). "Resources" includes any money or other property which is applied or made available, or is to be applied or made available, for use by the organisation. [Terrorism Act, s 14]
Tipping off	A tipping-off offence is committed if a person knows or suspects that a disclosure falling under POCA ss 337 or 338 has been made, and he makes a disclosure which is likely to prejudice any investigation which may be conducted following the disclosure under s 337 or s 338. [POCA, s 333]

Verification	Verifying the identity of a customer, by reference to reliable, independent source documents, data or information.
Wolfsberg Group	An association of twelve global banks, which aims to develop financial services industry standards, and related products, for Know Your Customer, Anti-Money Laundering and Counter Terrorist Financing policies.
Wolfsberg Principles	These are contained in four documents: ➢ Global Anti-Money Laundering Guidelines for Private Banking, published by the Wolfsberg Group in October 2000, and revised in May 2002. ➢ Statement on the Suppression of the Financing of Terrorism, published in January 2002. ➢ Anti-Money Laundering Principles for Correspondent Banking, published in November 2002. ➢ Statement on Monitoring, Screening and Searching, published in September 2003.

Abbreviation	
ACPO	Association of Chief Police Officers
AML	Anti-money laundering
CDD	Basel Committee Customer Due Diligence paper, published in October 2001
CFT	Combating the financing of terrorism
DfES	Department for Education and Skills
DWP	Department of Work and Pensions
FATF	Financial Action Task Force, an intergovernmental body whose purpose is to develop and promote broad AML/CFT standards, both at national and international levels
FSA	Financial Services Authority, the UK regulator of the financial services industry
FSMA	Financial Services and Markets Act 2000
HMT	Her Majesty's Treasury
IAIS	International Association of Insurance Supervisors
IOSCO	International Organisation of Securities Commissions
MLRO	Money Laundering Reporting Officer
NCIS	National Criminal Intelligence Service, the UK's financial intelligence unit.
POCA	Proceeds of Crime Act 2002
SAR	Suspicious activity report
SOCPA	Serious Organised Crime and Police Act 2005
SYSC	FSA Sourcebook: Senior Management Arrangements, Systems and Controls

APPENDIX I

ANTI-MONEY LAUNDERING RESPONSIBILITIES IN THE UK

UK Government	Law Enforcement, other investigating bodies and prosecutors	Regulator	Industry
Home Office: • UK primary legislation (Proceeds of Crime Act 2002, Terrorism Act 2000 and Anti-terrorism, Crime and Security Act 2001) • Police strategy and resourcing • Asset recovery strategy • Chairs (jointly with HM Treasury) Money Laundering Advisory Committee (MLAC), a forum for key stakeholders to coordinate the AML regime and review its efficiency and effectiveness **HM Treasury** • Represents UK in EU and FATF • Implements EU Directives, principally through the Money Laundering Regulations • Approves industry guidance under POCA, Terrorism Act and Money Laundering Regulations • Chairs (jointly with Home Office) Money Laundering Advisory Committee (MLAC), a forum for key stakeholders to coordinate the AML regime and review its efficiency and effectiveness • Implements the UK's financial sanctions regime	**Serious Organised Crime Agency** will bring together : • National Crime Squad • NCIS • HMRC investigative branches • Parts of the Home Office Immigration Service **National Criminal Intelligence Service (NCIS)** • UK's financial intelligence unit receives suspicious activity reports (about money laundering and terrorist financing) and sends cleared intelligence to law enforcement agencies for investigation • Assesses organised crime threats **Police** • 52 forces in the UK • Investigate crime, money laundering and terrorism **HM Revenue and Customs** • Investigates money laundering, drug trafficking and certain tax offences • Licenses money service businesses and dealers in high value goods **Assets Recovery Agency** • Powers under POCA to recover the proceeds of crime through criminal, civil, or tax recovery processes • Supports law enforcement agencies • Trains financial investigators	**Financial Services Authority** • UK's financial regulator • Statutory objectives (under Financial Services and Markets Act 2000) include reduction of financial crime • Approves persons to perform "controlled functions" (including money laundering reporting officer function) • Makes, supervises and enforces, amongst other things, rules on money laundering • Power to prosecute firms under the Money Laundering Regulations (except in Scotland)	**Joint Money Laundering Steering Group** • Industry body made up of 16 financial sector trade bodies • Produces guidance on compliance with legal and regulatory requirements and good practice

	The Revenue and Customs Prosecutions Office • Prosecutes money laundering, drug trafficking and certain tax offences investigated by HMRC **Crown Prosecution Service** • Prosecutes crime, money laundering and terrorism offences in England and Wales **Procurator Fiscal** • Prosecutes crime, money laundering and terrorism offences in Scotland **Public Prosecution Service of Northern Ireland** • Prosecutes crime, money laundering and terrorism offences in Northern Ireland **Bank of England** • Administers the UK's financial sanctions regime, on behalf of HM Treasury		

APPENDIX II

SUMMARY OF UK LEGISLATION

Proceeds of Crime Act 2002[1] (as amended)

1. The Proceeds of Crime Act 2002 (POCA) consolidates and extends the existing UK legislation regarding money laundering. The legislation covers all crimes and any dealing in criminal property, with no exceptions and no de minimis. POCA:

    - establishes the Assets Recovery Agency[2] (ARA), to conduct an investigation[3] to discover whether a person holds criminal assets and to recover the assets in question.

    - creates five investigative powers for the law enforcement agencies:
        - a production order[4]
        - a search and seizure warrant[5]
        - a disclosure order[6]
        - a customer information order[7]
        - an account monitoring order[8]

    - establishes the following criminal offences:

        - a criminal offence[9] to acquire, use, possess, conceal, disguise, convert, transfer or remove criminal property from the jurisdiction, or to enter into or become concerned in an arrangement to facilitate the acquisition, retention, use or control of criminal property by another person

        - a criminal offence[10] for persons working in the regulated sector of failing to make a report where they have knowledge or suspicion of money laundering, or reasonable grounds for having knowledge or suspicion, that another person is laundering the proceeds of any criminal conduct, as soon as is reasonably practicable after the information came to their attention in the course of their regulated business activities

            Note: There are no provisions governing materiality or de minimis thresholds for having to report under POCA (although for deposit-taking firms, a transaction under £250 may be made without consent under certain circumstances – see paragraph 7.64).

        - a criminal offence[11] for anyone to take any action likely to prejudice an investigation by informing (e.g., tipping off) the person who is the subject of a suspicion report, or anybody else, that a disclosure has been made to a

[1] 2002 ch 29
[2] section 1
[3] section 341(2)
[4] section 345
[5] section 352
[6] section 357
[7] section 363
[8] section 370 – see also Terrorism Act s38A
[9] sections 327 - 329
[10] sections 330 and 331
[11] section 333

nominated officer or to NCIS, or that the police or customs authorities are carrying out or intending to carry out a money laundering investigation.

- a criminal offence[12] of destroying or disposing of documents which are relevant to an investigation.

- a criminal offence[13] by a firm of failing to comply with a requirement imposed on it under a customer information order, or in knowingly or recklessly making a statement in purported compliance with a customer information order that is false or misleading in a material particular.

- sets out maximum penalties:

  - for the offence of money laundering of 14 years' imprisonment and/or an unlimited fine.

    Note: An offence is not committed if a person reports the property involved to the National Criminal Intelligence Service (NCIS) or under approved internal arrangements, either before the prohibited act is carried out, or as soon afterwards as is reasonably practicable.

  - for failing to make a report of suspected money laundering, or for "tipping off", of five years' imprisonment and/or an unlimited fine.

  - for destroying or disposing of relevant documents of five years' imprisonment and/or an unlimited fine.

Terrorism Act 2000[14], and the Anti-terrorism, Crime and Security Act 2001[15]

2. The Terrorism Act establishes a series of offences related to involvement in arrangements for facilitating, raising or using funds for terrorism purposes. The Act:

   - makes[16] it a criminal offence for any person not to report the existence of terrorist property where there are reasonable grounds for knowing or suspecting the existence of terrorist property

   - makes it a criminal offence[17] for anyone to take any action likely to prejudice an investigation by informing (i.e. tipping off) the person who is the subject of a suspicion report, or anybody else, that a disclosure has been made to a nominated officer or to NCIS, or that the police or customs authorities are carrying out or intending to carry out a terrorist financing investigation

   - grants[18] a power to the law enforcement agencies to make an account monitoring order, similar in scope to that introduced under POCA

[12] section 341(2)(b)
[13] section 366
[14] 2000 ch 11
[15] 2001 ch 24
[16] section 21A
[17] section 39
[18] section 38A and Schedule 6A

- sets out the following penalties:
    - the maximum penalty for failure to report under the circumstances set out above is five years' imprisonment, and/or a fine.
    - the maximum penalty for the offence of actual money laundering is 14 years' imprisonment, and/or a fine.

3. A number of organisations have been proscribed under the Terrorism Act. The definition of terrorist property, involvement with which is an offence, includes resources of a proscribed organisation.

4. The Anti-terrorism, Crime and Security Act 2001 gives the authorities power to seize terrorist cash, to freeze terrorist assets and to direct firms in the regulated sector to provide the authorities with specified information on customers and their (terrorism-related) activities.

Money Laundering Regulations 2003[19]

5. The Money Laundering Regulations 2003 prescribe arrangements which must be in place within firms carrying on relevant business, to forestall and prevent their being used for money laundering.

6. The ML Regulations apply[20], inter alia, to:
    - The regulated activities of all financial sector firms, i.e.:
        - banks, building societies and other credit institutions;
        - individuals and firms engaging in regulated investment activities under FSMA;
        - issuers of electronic money;
        - insurance companies undertaking long-term life business, including the life business of Lloyd's of London;
    - Bureaux de change, cheque encashment centres and money transmission services (money service businesses);
    - The National Savings Bank;
    - Corporate service providers, company formation agents, trust companies and trust service providers or managers;
    - Casinos;
    - Dealers in high-value goods (including auctioneers) who accept payment in cash of €15,000 or more (either single or linked transactions);
    - Lawyers and accountants, when undertaking relevant business.

7. Persons carrying on relevant business under the ML Regulations are required to establish and maintain appropriate systems and controls, to forestall and prevent the firm being used in connection with money laundering, covering:
    - internal controls and communication

[19] SI 2003/3075
[20] Regulation 2

- identification procedures
- recognition of suspicious transactions and reporting procedures
- awareness raising and training of employees
- record keeping

8. The FSA may[21] institute proceedings (other than in Scotland) for offences under prescribed regulations relating to money laundering. This power is not limited to firms or persons regulated by the FSA. Whether a breach of the ML Regulations has occurred is not dependent on whether money laundering has taken place: firms may be sanctioned for not having adequate AML/CFT systems. Failure to comply with any of the requirements of the ML Regulations constitutes an offence punishable by a maximum of two years' imprisonment, or a fine, or both.

FSA-regulated firms – the FSA Handbook

9. FSMA gives the FSA a statutory objective[22] to reduce financial crime. In considering this objective, the FSA is required[23] to have regard to the desirability of firms:

    - Being aware of the risk of their businesses being used in connection with the commission of financial crime;
    - Taking appropriate measures to prevent financial crime, facilitate its detection and monitor its incidence;
    - Devoting adequate resources to that prevention, detection and monitoring.

10. Firms may only engage in a regulated activity[24] in the UK if it is an authorised or exempt person. A person can become an authorised person as a result of: (a) being given a "permission" by the FSA under Part IV of FSMA (known as a "Part IV permission"); or (b) by qualifying for authorisation under FSMA itself. As an example of the latter, an EEA firm establishing a branch in, or providing cross-border services into, the UK can qualify for authorisation under FSMA Schedule 3 and, as a result, be given a permission; although such firms are, generally, authorised by their home state regulator, they are regulated by the FSA in connection with the regulated activities carried on in the UK.

11. A firm may only carry on regulated business in accordance with its permission. A firm with a Part IV permission may apply to the FSA to vary its permission, add or remove regulated activities, to limit these activities (for example, the types of client with or for whom the firm may carry on an activity) or to vary the requirements on the firm itself. Before giving or varying a Part IV permission, the FSA must ensure that the person/firm will satisfy and continue to satisfy the threshold conditions in relation to all of the regulated activities for which he has or will have permission. If a firm is failing, or is likely to fail, to satisfy the threshold conditions, the FSA may vary or cancel a firm's permission.

12. Threshold condition 5 (Suitability) requires the firm to satisfy the FSA that it is "fit and proper" to have Part IV permission having regard to all the circumstances, including its connection with other persons, the range and nature of its proposed (or current) regulated activities and the overall need to be satisfied that its affairs are and will continue to be conducted soundly and prudently. Hence, the FSA "will consider whether a firm is ready, willing and organised to comply, on a continuing basis, with the requirements and standards under the regulatory system which apply to

[21] FSMA, s 402(1)(b)

[22] FSMA s 6. This is defined as "reducing the extent to which it is possible for a business carried on by a regulated person … to be used for a purpose connected with financial crime".

[23] FSMA s 6(2)

[24] FSMA s22, Schedule 2, and the Regulated Activities Order. These activities are substantially the same as set out in Regulation 2 (2)(a).

the firm, or will apply to the firm, if it is granted Part IV permission, or a variation of its permission". The FSA will also have regard to all relevant matters, whether arising in the UK or elsewhere. In particular, the FSA will consider whether a firm "has in place systems and controls against money laundering of the sort described in SYSC 3.2.6 R to SYSC 3.2.6J G". (COND 2.5.7G)

13. The FSA Handbook of rules and guidance contains high level standards that apply, with some exceptions, to all FSA-regulated firms, (for example, the FSA Principles for Businesses, COND and SYSC) and to all approved persons (for example, the Statements of Principle and Code of Practice for Approved Persons). SYSC sets out particular rules relating to senior management responsibilities, and for systems and controls processes. Some of these rules focus on the management and control of risk[25], and specifically require appropriate systems and controls over the management of money laundering risk[26].

14. In addition to prosecution powers under the Regulations, the FSA has a wide range of enforcement powers against authorised persons and approved persons for breaches of its Rules.

[25] SYSC 3.2.6 R
[26] SYSC 3.2.6G G