The Joint Money Laundering Steering Group

Prevention of money laundering/ combating terrorist financing

2011 REVIEW VERSION

GUIDANCE FOR THE UK FINANCIAL SECTOR
PART I

Amended: December 2011

Draftsman/Editor: David Swanney

Contents

Chapter 5 Customer due diligence

Chapter 6 Suspicious activities, reporting and data protection

Chapter 7 Staff awareness, training and alertness

Chapter 8 Record keeping

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 current Regulations being those of 2007. 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 anti-money laundering/countering terrorist financing (AML/CTF) 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/CTF 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/CTF 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/CTF 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. 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, is at www.jmlsg.org.uk/other-helpful-material/case-studies.

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 establish adequate and appropriate policies and procedures in place to forestall and prevent 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)..

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/CTF 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/CTF. 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.

The content of the guidance

21. This guidance 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 sets out a standard approach to the identification and verification of customers, separating out basic identity from other aspects of customer due diligence measures, as well as giving guidance on the obligation to monitor customer activity.

22. 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/CTF framework.

23. The guidance provided by the JMLSG is in a number of 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. [Part III provides additional guidance on a number of specific areas of activity.]

24. Part I comprises eight 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.

25. 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 the application of CDD measures (Chapter 4);
    - helping a firm have confidence that it has properly carried out its CDD obligations, including monitoring customer transactions and activity (Chapter 5);
    - the identification and reporting of suspicious activity (Chapter 6);
    - staff awareness, training and alertness (Chapter 7);
    - record keeping (Chapter 8).

26. Parts II and III 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

27. 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.

28. The FSA Handbook also confirms that the FSA will have regard to whether a firm has followed relevant provisions of this guidance when:

- Considering whether to take action against an FSA-regulated firm in respect of a breach of the relevant provisions in SYSC (see SYSC 3.2, SYSC 5.3, and DEPP 6.2.3); and
- Considering whether to prosecute a breach of the Money Laundering Regulations (see EG 12.1).

29. The guidance therefore 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 this guidance, and the rationale for so doing, should be documented, and firms will have to stand prepared to justify departures, for example to the FSA.

Who are the members of JMLSG?

30. The members of JMLSG are:

Asset Based Finance Association (ABFA)
Association of British Credit Unions (ABCUL)
Association of British Insurers (ABI)
Association for Financial Markets in Europe (AFME)
Association of Financial Mutuals (AFM)
Association of Foreign Banks (AFB)
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)
Tax Incentivised Savings Association (TISA)
Wholesale Market Brokers' Association (WMBA)

OVERVIEW OF CONTENTS

The anti-money laundering/counter terrorist financing (AML/CTF) regime in the UK is delivered through several discrete pieces of legislation[1], which collectively impose a number of obligations on firms and their senior management:

- To apply Customer Due Diligence (CDD) measures (to identify/verify customers and to understand the nature and purpose of the proposed relationship)
- To maintain appropriate systems and controls for AML/CTF purposes
- To monitor customer transactions and activities
- To report suspicious activity, both internally and, if appropriate, externally
- To keep appropriate records, and train staff
- To comply with the UK financial sanctions regime

Part I is the core guidance to firms in the financial sector, with generic application.

Part II comprises sector-specific additional material, which draws out specific considerations that are relevant to each sector given the specific products and services they offer and must be read in conjunction with the main guidance set out in Part I.

Part III provides additional guidance in relation to a number of specific areas, including compliance with financial sanctions.

Part I

Chapter 1 - Essential reading for senior management (pages 19 – 28)

- Gives an overview of the context of AML/CTF in the UK and more widely, and the place of Guidance in assisting the implementation of UK legal and regulatory obligations in practice

- Outlines the responsibilities and obligations that rest on senior management as part of their general responsibility for running the firm

- Stresses the importance of senior management taking responsibility for effectively managing the money laundering and terrorist financing risks faced by the firm's businesses

- Refers to the requirement that they must appoint a director or senior manager to take responsibility for AML/CTF across the firm

Chapter 2 – internal controls (pages 29 – 31)

- Outlines the obligations on firms under the Money Laundering Regulations to establish and maintain appropriate controls against the risk of financial crime

- Areas where controls are specifically required are referenced forward to other, more detailed text within the Guidance:

[1] These include the Money Laundering Regulations 2007, the Proceeds of Crime Act 2002, the Terrorism Act 2000, the Terrorist Asset-freezing etc Act 2010 and the Counter-terrorism Act 2008

- Risk assessment and management (Chapter 4)
- Customer due diligence and ongoing monitoring (Chapter 5)
- Record keeping (Chapter 8)
- Reporting of suspicions (Chapter 6)
- Internal; communication of policies (which includes staff awareness and training) (Chapter 7)
- Monitoring and management of compliance with the firm's policies and procedures (Chapter 3 – para 3.27)

Chapter 3 – responsibilities of the nominated officer/MLRO (pages 32 – 37)

- Notes the requirement that the MLRO must be of sufficient seniority within the firm, and should have adequate resources available to carry out the role

- Refers to the nominated officer's *personal* responsibility for considering internal suspicion reports, and for deciding whether an external SAR should be made

- Refers to the requirement that the MLRO make regular reports to senior management on the operation of the firm's AML/CTF procedures, and on any improvements that are needed

Chapter 4 – how to establish a risk-based approach (pages 38 – 45)

- Discusses the management of the risk of being used for financial crime in the context of senior management's general approach to managing other risks faced by the firm

- Summarises how a risk-based approach might be established, through

  - Identifying and assessing the risks faced by the firm (giving some suggested questions that senior management may ask themselves)
  - Designing and implementing controls to manage and mitigate the risks
  - Monitoring and improving the effectiveness of the firm's controls
  - Recording appropriately what has been done and why

- Notes that risk management is dynamic, and is generally a continuous process rather than a one-time exercise

Chapter 5 – customer due diligence (pages 46 – 128)

- The key chapter in this Part of the Guidance, setting out the way in which customer due diligence should be approached

- Describes what customer due diligence and ongoing monitoring are, and why these are necessary **(section 5.1, pages 40 – 48)**

- Discusses the timing of applying CDD (including cases where exceptions from the general requirement are permitted), and what to do where CDD measures cannot be applied **(section 5.2, pages 48 – 61)**

- In the main section **(section 5.3),** discusses the minimum requirements for CDD measures, in relation to customers and beneficial owners generally, and more specifically in relation to the identification and verification of the various types of customers that firms will encounter:

  - Personal customers, including personal representatives and attorneys **(pages 61-70)**
  - Regulated financial services firms **(pages 71-72)**
  - Other firms subject to the Money Laundering Regulations **(pages 72-73)**
  - Other corporate customers **(pages 73-74)**

    - Companies listed on regulated markets **(pages 74-75)**
    - Other publicly listed companies **(page 75)**
    - Private and unlisted companies **(pages 75-78)**
  - Partnerships and unincorporated bodies **(pages 78-80)**
  - Public sector bodies, governments, state-owned companies and supra-nationals, other than sovereign wealth funds **(pages 80-81)**
  - Sovereign wealth funds **(pages 81-85)**
  - Pension schemes **(pages 85-86)**
  - Charities, church bodies and places of worship **(pages 86-89)**
  - Other trusts and foundations **(pages 89-92)**
  - Clubs and societies **(pages 93-94)**

- The guidance refers to the provisions in the legislation under which **simplified due diligence** (SDD) may be applied **(pages 94-96).**

- Conversely, the guidance also refers to the provisions in the legislation under which **enhanced due diligence** (EDD) *must* be applied **(pages 96-100),** including non fact-to-face business and when dealing with Politically Exposed Persons.

- The guidance addresses situations where more than one firm is dealing with the same customer, and **situations where one firm may rely on another, or on group associates,** to carry out CDD **(pages 101-107).**

- Guidance is given on **monitoring,** what it is and how it may be manual or automated **(pages 107-111).**

Chapter 6 – reporting suspicions (pages 129-146)

- This section discusses what is meant by 'knowledge' and 'suspicion', and by 'reasonable grounds to know or suspect' **(pages 131-133).**

- It goes on to give guidance on

  - Internal reporting **(pages 133-134)**
  - Evaluation and determination by nominated officer **(pages 134-135)**
  - External reporting **(pages 135-137)**
  - Consent **(pages 137-146)**
  - Tipping off, and prejudicing an investigation **(pages146-142)**
  - Transactions following a disclosure **(pages142-144)**
  - Related data protection issues **(pages 144-146)**

Chapter 7 – Staff awareness, training and alertness (pages 147-153)

- This section discusses the firm's obligations to employ appropriately trained and qualified staff **(pages 140-141)**

- The section gives guidance on discharging the responsibilities on the firm and on its staff **(pages 149-150)**

- The section also gives examples of situations where the alertness of staff is important **(pages 150-153)** and training methods **(page 153)**

Chapter 8 – Record keeping (pages 1454-158)

- This section discusses the obligations on firms to retain appropriate records **(page 154)** and gives guidance on what records should be kept **(pages 155-157),** and the form in which records might be retained **(pages 157-158).**

Glossary – pages 159-164

- The Glossary defines many of the terms used in the Guidance

Appendices – pages 165-173

- I – this Appendix (pages 165-166) summarises the distribution of responsibilities amongst the competent authorities for developing and enforcing AML/CTF legislation in the UK

- II – the Appendix (pages 167-173) summarises the provisions of various relevant legislation and regulation. It is not a substitute for reading the complete legislative or regulatory text.

Parts II and III

The sectoral guidance is incomplete on its own and must be read in conjunction with the main guidance set out in Part I.

Part II provides additional guidance in relation to 21 different sectors within the financial sector:

1	Retail banking
2	Credit cards, etc
3	Electronic money
4	Credit unions
5	Wealth management
6	Financial advisers
7	Life assurance, and life-related pensions and investment products
7A	General insurers
8	Non-life providers of investment fund products
9	Discretionary and advisory investment management
10	Execution-only stockbrokers
11	Motor finance
12	Asset finance
13	Private equity
14	Corporate finance
15	Trade finance
16	Correspondent banking
17	Syndicated lending
18	Wholesale markets
19	Name-passing brokers in inter-professional markets
20	Brokerage services to funds
21	Invoice finance

Part III provides additional guidance in relation to a number of specific areas:

1. Transparency in electronic payments (Wire transfers)

    - Covering the obligations of payment service providers under the EU Regulation implementing FATF Special Regulation VII.

2. Equivalent jurisdictions

- Providing assistance to firms in the assessment of equivalence of EEA and third countries for the purposes of reliance and simplified due diligence.

3. Equivalent markets

   - Providing assistance to firms in determining what constitutes an "equivalent market" for the purposes of applying simplified due diligence to listed companies.

4. Compliance with the UK financial sanctions regime

   - Providing guidance on compliance with the UK financial sanctions regime, including the screening of customers against the UK consolidated list of sanctions targets and the freezing of assets and reporting in the event of a match.

5. Directions under the Counter-Terrorism Act 2008, Schedule 7

   - Offering further guidance on compliance with directions that may be issued under the CTA.

CHAPTER 1

SENIOR MANAGEMENT RESPONSIBILITY

- **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
  - Third Money Laundering Directive 2005/60/EC
  - Implementing Measures Directive 2006/70/EC
- **EU Regulations**
  - EC Regulation 2580/2001
  - EC Regulation 1781/2006 (the Wire Transfer Regulation)
- **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 2007
  - Financial Sanctions
    - HM Treasury Sanctions Notices and News Releases
  - Regulatory regime
    - FSA Handbook –APER, COND, DEPP, PRIN, and SYSC
  - Industry guidance
- **Other matters**
  - Extra-territoriality of some overseas jurisdictions' regimes
- **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,
6.1.1 R
6.3.1 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. Senior management must be aware of the level of money laundering risk the firm is exposed to and take a view whether the firm is equipped to mitigate that risk effectively; this implies that decisions on entering or maintaining high-risk business relationships must be escalated to senior management. That said, provided the assessment of the risks has been approached in a considered way, the selection of risk mitigation procedures is appropriate, all the relevant decisions are properly recorded, and the firm's procedures are followed and applied effectively, the risk of censure should be small.

International pressure to have effective AML/CTF 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 on Money Laundering 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 CTF. The text of these Recommendations is available at www.fatf-gafi.org.

1.7 Separate from the development of FATF's Recommendations, an EU Directive is targeted at money laundering prevention, and has been implemented in the UK mainly through the Money Laundering Regulations 2007.

1.8 Internationally, the FATF Forty Recommendations, the Basel CDD paper (www.bis.org), IAIS Guidance Paper 5 (www.iais.org) and the IOSCO Principles paper (www.iosco.org) 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/CTF 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, HM Treasury issues sanctions notices whenever a new name is added to the list, or when any details are amended.

1.10 Some international groupings, official or informal, publish material that may be useful as context and background in informing firms' approaches to AML/TF. These groupings include Transparency International (www.transparency.org.uk) and the Wolfsberg Group (www.wolfsberg-principles.com).

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/CTF 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 2007;
- Counter-terrorism Act 2008, Schedule 7
- HM Treasury 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.

Regulation 3 (1)

1.15 The ML Regulations apply to a range of specified firms undertaking business in the UK. POCA and the Terrorism Act consolidated, updated and reformed the scope of UK AML/CTF 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.

UKAnti-money laundering and terrorist finance strategy, 28 February 2007

1.16 Firms should be aware of the UK's strategy document *The financial challenge to crime and terrorism*, issued jointly by HM Treasury, Home Office, SOCA and the Foreign Office (available at http://webarchive.nationalarchives.gov.uk/+/http://www.hm-treasury.gov.uk/media/C/B/financialchallenge_crime_280207.pdf which sets out why it is important to combat money laundering and terrorist financing. The strategy document notes that the Government's objectives are to use financial measures to:

- **deter** crime and terrorism in the first place – by increasing the risk and lowering the reward faced by perpetrators;
- **detect** the criminal or terrorist abuse of the financial system; and
- **disrupt** criminal and terrorist activity – to save lives and hold the guilty to account.

1.17 In order to deliver these objectives successfully, the government believes action in this area must be underpinned by the three key organising principles that were first set out in the 2004 AML Strategy (see www.hm-treasury.gov.uk/media/D57/97/D579755E-BCDC-D4B3-19632628BD485787.pdf):

- **effectiveness** – making maximum impact on the criminal and terrorist threat:
  - build knowledge of criminal and terrorist threats to drive continuous improvement
  - make the best use of the financial tools we have, by making sure that all stakeholders make the maximum use of the opportunities provided by financial tools, including those to recover criminal assets
- **proportionality** – so that the benefits of intervention are justified and that they outweigh the costs:
  - entrench the risk-based approach
  - reduce the burdens on citizens and business created by crime and security measures to the minimum required to protect their security
- **engagement** – so that all stakeholders in government and the private sector, at home and abroad, work collaboratively in partnership:
  - work collaboratively across the AML/CTF community, including to share data to reduce harm
  - engage international partners to deliver a global solution to a global problem

General legal and regulatory obligations

Regulation 20
POCA ss327-330
Terrorism Act ss18, 21A

1.18 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 Appendix II.

FSMA s 6
SYSC

1.19 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 responsibilities and obligations are summarised in Appendix II. The FSA has also issued a publication "Financial Crime: A Guide for Firms", which provides practical assistance and information for firms on actions they can take to counter the risk that they might be used to further financial crime.

Obligations on all firms

Regulations 20 and 45(1)

1.20 The ML Regulations place a general obligation on firms within its scope to establish adequate and appropriate policies and procedures to prevent money laundering. Failure to comply with this obligation risks a prison term of up to two years and/or a fine.

Regulation 47

1.21 In addition to imposing liability on firms, the ML Regulations impose criminal liability on certain individuals in firms subject to the ML Regulations. Where the firm is a body corporate, an officer of that body corporate (i.e., a director, manager, secretary, chief executive, member of the committee of management, or a person purporting to act in such a capacity), who consents or connives in the commission of an offence by the firm, or that offence (by the firm) is attributable to any neglect on his part, himself commits a criminal offence and may be prosecuted. Similarly, where the firm is partnership, a partner 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 to be prosecuted for the offence. A similar rule applies to officers of unincorporated associations.

POCA ss 327-330
Terrorism Act s 21A
Regulation 21

1.22 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 all relevant employees are made aware of the law relating to money laundering and terrorist finance, and are regularly 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

1.23 A number of the financial sector firms regulated by the FSA are so-called 'common platform' firms, because they are subject both to MiFID and to the Capital Requirements Directive. The FSA Rules relating to systems and controls to prevent firms being used in connection with the commission of financial crime are in two parts: those which apply to most firms, set out in SYSC 6.1.1, and those which apply to non common platform firms, set out in SYSC 3.2.6. To avoid confusing the vast

majority of firms by including a multitude of references to SYSC 3.2.6, this guidance is constructed in terms of following the requirements of SYSC 6.1.1; non common platform firms should follow this guidance, interpreting it as referring as necessary to the relevant parts of SYSC 3.2.6.

FSMA, s 6 (2) (a)
FSMA, s 6 (2) (b)
SYSC 2.1.1 R, 2.1.3 R, 6.1.1 R, 6.3.7(G)

1.24 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 6.3.8 R

1.25 In FSA-regulated firms (but see paragraph 1.35 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 6.3.9 R

1.26 In FSA-regulated firms (but see paragraph 1.35 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 1.25); in firms where he is not, he will be directly responsible to someone who is.

SYSC 6.3.8 R
SYSC 6.3.9 R

1.27 Senior management of FSA-regulated firms must:

- 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/CTF systems and controls;
- appoint an appropriately qualified senior member of the firm's staff as the MLRO (see Chapter 3); and
- provide direction to, and oversight of the firm's AML/CTF strategy.

1.28 Although the FSA Rule referred to in paragraph 1.26 requires overall responsibility for AML/CTF systems and controls to be allocated to a single individual, in practice this may often be difficult to achieve, especially in larger firms. As a practical matter, therefore, firms may allocate this responsibility among a number of individuals, provided the division of responsibilities is clear.

1.29 The relationship between the MLRO and the director/senior manager allocated overall responsibility for the establishment and maintenance of the firm's AML/CTF systems (where they are not the same person) is one of the keys to a successful AML/CTF regime. It is important that this relationship is clearly defined and documented, so that each knows the extent of his, and the other's, role and day to day responsibilities.

SYSC 6.3.7(2) G

1.30 At least once in each calendar year, an FSA-regulated firm should 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.

1.31 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 3.2.6 R, 6.3.9 (2) R
FSMA s 6 (2) (c)

1.32 Those FSA-regulated firms required to appoint an MLRO are specifically required to provide the MLRO with adequate resources. All firms, whether or not regulated by the FSA for AML purposes, must apply adequate resources to counter the risk that they may be used for the purposes of financial crime. This includes systems and controls to prevent ML/TF. The level of resource should reflect the size, complexity and geographical spread of the firm's customer and product base.

1.33 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.

1.34 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 1.1A.1, 3.2.6 R

1.35 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. Guidance for general insurance firms is given in Part II, sector 7A: *General insurers*.

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

1.36 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 SOCA, and appropriate consent for the transaction or activity obtained. Certain of these firms may also be subject to the provisions of Schedule 7 to the Counter-Terrorism Act 2008 – see Part III, section 5, especially paragraph 5.11.

POCA s 332
Terrorism Act ss 19, 21

1.37 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 6).

Relationship between money laundering, terrorist financing and other financial crime

1.38 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.

1.39 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.

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

SYSC 3.1.1 R, 3.2.6 R 6.1.1 R 6.3.1 R

1.40 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 6.3.7 (3) G

1.41 For FSA-regulated firms (but see paragraph 1.35 for general insurance firms and mortgage intermediaries) SYSC 6.3.7 (3) G says that a firm should produce "appropriate 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/CTF 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/CTF policy will focus the minds of staff on the need to be constantly aware of such risks, and how they are to be managed.

1.42 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.

1.43 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

1.44 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 2.7-2.11), the firm must put in place a group AML/CTF strategy.

Regulation 15 (1)

1.45 A group policy must ensure that all non-EEA branches and subsidiaries carry out CDD measures, and keep records, 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.

Regulation 20(5)

1.46 Firms must communicate their policies and procedures established to prevent activities related to money laundering and terrorist financing to branches and subsidiaries located outside the UK.

Regulation 15(2)

1.47 Where the law of a non-EEA state does not permit the application of such equivalent measures, the firm must inform the FSA accordingly, and take additional measures to handle effectively the risk of money laundering or terrorist financing.

1.48 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 SOCA (see paragraph 6.25).

Extra-territoriality of some overseas jurisdictions' regimes

1.49 Where a firm has a listing, or activities in, or linked to, certain overseas jurisdictions, whether through a branch, subsidiary, associated company or correspondent banking relationship, or where a firm deals in another jurisdiction's currency, there is a risk that the application of that jurisdiction's AML/CTF and financial sanctions regimes may apply to the non-domestic activities of the firm. Senior management should take advice on the extent to which the firm's activities may be affected in this way.

CHAPTER 2

INTERNAL CONTROLS

➢ **Relevant law/regulation** ▪ FSMA s 6 ▪ Regulations 20, 21 ▪ SYSC Chapters 2, 3, 3A, 6
➢ **Core obligations** ▪ Firms must establish and maintain adequate and appropriate policies and procedures to forestall and prevent operations relating to 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 adequate and appropriate policies and 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 20(1)
SYSC 3, 6

2.1 There is a requirement for firms to establish and maintain appropriate and risk-based policies and procedures in order to prevent operations related to money laundering or terrorist financing. 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

Regulations 20, 21

2.3 There are specific requirements under the ML Regulations for the firm to establish adequate and appropriate policies and procedures relating to: internal control; risk assessment and management (see Chapter 4); customer due diligence and ongoing monitoring (see Chapter 5); record keeping (see Chapter 8); reporting of suspicions (see Chapter 6); the monitoring and management of compliance with such policies and procedures (see paragraph 3.27); and the internal communication of such policies and procedures (which includes staff awareness and training) (see Chapter 7). 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 3.1.1 R

2.4 FSA-regulated firms are required to have systems and controls appropriate to their business. Specifically, those systems and controls

SYSC 3.1.2 G
SYSC 6.1.1 R
SYSC 6.1.2R

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 6.3.1 R

2.5 An FSA-regulated firm must ensure that these systems and controls:

- enable it to identity, assess, monitor and manage money laundering risk; and
- are comprehensive and proportionate to the nature, scale and complexity of its activities.

SYSC 6.3.7 G
SYSC 6.3.8 R
SYSC 6.3.9 R

2.6 An FSA-regulated firm's systems and controls (but see paragraph 1.35 for general insurance firms and mortgage intermediaries) are required to cover senior management accountability, including allocation to a director or senior manager of 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. The systems and controls should also cover:

- 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 3.2.4 G
SYSC 13.9

2.7 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 in the interests of the firm to ensure that outsourcing does not result in reduced standards or requirements being applied. In all cases, the firm should have regard to the FSA's guidance on outsourcing.

SYSC 3.2.4 G
SYSC 13.9

2.8 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/CTF systems, controls and procedures, and that those policies and procedures are kept up to date to reflect changes in UK requirements.

2.9 Where UK operational activities are undertaken by staff in other jurisdictions (for example, overseas call centres), those staff should be subject to the AML/CTF 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.

2.10 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/CTF regulations and reporting requirements. Any conflicts between the UK and local AML/CTF requirements, where meeting local requirements would result in a lower standard than in the UK, should be resolved in favour of the UK.

2.11 In some circumstances, the outsourcing of functions can actually lead to increased risk - for example, outsourcing to businesses in jurisdictions with less stringent AML/CTF requirements than in the UK. All financial services businesses that outsource functions and activities should therefore assess any possible AML/CTF 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)

- **Relevant law/regulation**
  - Regulation 20
  - PRIN, Principle 11
  - APER, Chapters 2 and 4
  - APER, Principles 4 and 7
  - SYSC, Chapter 6
  - 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 AML systems and controls
- **Actions required, to be kept under regular review**
  - Senior management to ensure the MLRO has:
    - active support of senior management
    - adequate resources
    - independence of action
    - access to information
    - 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 20(2)(d) 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 disclosures under Part 7 of POCA and Part 3 of the Terrorism Act, deciding whether these should be reported to SOCA, and, if appropriate, making such external reports.

SYSC 1.1A.1 SYSC 3.2.6R

3.2 As noted in paragraph 1.35, general insurance firms and mortgage intermediaries are not covered by the ML Regulations, s 330 of POCA, s 21A of the Terrorism Act, or the provisions of SYSC relating specifically to money laundering. They are, however, regulated by the FSA and may be subject to the certain disclosure obligations in POCA and the Terrorism Act. 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 ss 337 and 338 of POCA and s 19 of 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 6.3.9 R

3.4 In the case of FSA-regulated firms, other than sole traders with no employees 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 6.3.9(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/CTF 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 6.3.10 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 6.3.9 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 6.3.9 R
SYSC 6.3.10 G

3.9 In FSA-regulated firms, the MLRO is responsible for the oversight of all aspects of the firm's AML/CTF 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 1.25). 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 6.3.9(1) R
SYSC 6.3.10 G

3.10 Along with the Director/Senior Manager appointed by the Board (see paragraph 1.25), 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.

3.11 As noted in paragraph 1.29, the relationship between the MLRO and the director(s)/senior manager(s) allocated overall responsibility for the establishment and maintenance of the firm's AML/CTF systems is one of the keys to a successful AML/CTF regime. It is important that this relationship is clearly defined and documented, so that each knows the extent of his, and the other's, role and day to day responsibilities.

SYSC 6.3.9(2)R

3.12 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 SOCA, 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 SOCA on any question of whether to proceed with a transaction in the circumstances.

SYSC 6.3.9 (2)R

3.13 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.

3.14 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/CTF 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

3.15 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.

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

Internal and external reports

Regulation 20(2)(d)
POCA s 330

3.17 A firm must require that anyone in the firm to whom information or other matter comes in the course of business as a result of which they know or suspect, or have reasonable grounds for knowing or suspecting, that a person is engaged in money laundering or terrorist financing complies with Part 7 of POCA or Part 3 of the Terrorism Act (as the case may be). This includes staff having an obligation to make an internal report to the nominated officer as soon as is reasonably practicable after the information or other matter comes to them.

3.18 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.

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

3.20 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 beneficial owner, 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).

3.21 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 20(2)(d) POCA s 331

3.22 If the nominated officer (or appointed alternate) concludes that the internal report does give rise to knowledge or suspicion of money laundering or terrorist financing, he must make a report to SOCA as soon as is practicable after he makes this determination. The nominated officer (or appointed alternate)'s decision in this regard must be his own, and should not be subject to the direction or approval of other parties within the firm.

3.23 Guidance on reviewing internal reports, and reporting as appropriate to SOCA, is set out in Chapter 6.

National and international findings in respect of countries and jurisdictions

3.24 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.

3.25 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, SOCA periodically produces intelligence assessments, which are forwarded to the MLROs of the relevant sectors for internal dissemination only. No SOCA material is published through an open source.

3.26 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.

Monitoring effectiveness of money laundering controls

SYSC 6.3.3 R
SYSC 6.3.9(1) R
SYSC 6.3.10 G
Regulation 20(1)(f)

3.27 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/CTF 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 6.3.7(2) G

3.28 At least annually the senior management of an FSA-regulated firm should 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.

3.29 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.

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

3.31 The MLRO will wish to bring to the attention of senior management areas where the operation of AML/CTF controls should be improved, and proposals for making appropriate improvements. The progress of any significant remedial programmes will also be reported to senior management.

3.32 In addition, the MLRO should report on the outcome of any relevant quality assurance or internal audit reviews of the firm's AML/CTF processes, as well as the outcome of any review of the firm's risk assessment procedures (see paragraph 4.34).

3.33 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.

3.34 In December 2006, after discussion with the FSA, JMLSG issued a template suggesting a suitable presentation and content framework for a working paper underpinning the production of the MLRO Annual Report. [see www.jmlsg.org.uk]

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

3.36 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

➢ **Relevant law/regulation** ▪ Regulation 7(3)(a) ▪ SYSC 3.1.2 G, 6.1.1 R, 6.3.1-3, 6.3.6 ➢ **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 ▪ Determine appropriate CDD measures on a risk-sensitive basis, depending on the type of customer, business relationship, product or transaction ▪ Take into account situations which by their nature can present a higher risk of money laundering or terrorist financing; these specifically include where the customer has not been physically present for identification purposes; correspondent banking relationships; and business relationships and occasional transactions with PEPs
➢ **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.

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 and any underlying beneficial owners*;
  - 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.

* In this Chapter, references to 'customer' should be taken to include beneficial owner, where appropriate.

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 at www.fsa.gov.uk/pubs/other/money_laundering/jmslg.pdf.

A risk-based approach

SYSC 6.3.1 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/CTF 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/CTF. 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 customer 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 at www.jmlsg.org.uk.

SYSC 6.3.6 G

4.15 In identifying its money laundering risk an FSA-regulated firm should consider a range of factors, including

- its customer, product and activity profiles;
- its distribution channels;
- the complexity and volume of its transactions;
- its processes and systems; and
- its operating environment.

4.16 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 meeting the definition of a PEP (see paragraphs 5.5.18ff);
  - Customers (not necessarily PEPs) 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, or which are associated with higher levels of corruption (e.g., arms dealing).
  - Customers engaged in industries that might relate to proliferation activities[2]

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

Regulation 20(2)(a)

  - Where there is no commercial rationale for the customer buying the product he seeks;
  - Requests for a complex or unusually large transaction which has no apparent economic or lawful purpose;
  - 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 customers who are not private individuals 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:
  - Occasional transactions (see paragraph 5.3.6) v business relationships (see paragraph 5.3.5);
  - 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

[2] A working definition of proliferation is the transfer and export of nuclear, chemical or biological weapons; their means of delivery and related materials. [FATF Proliferation Financing Report, 18 June 2008.]

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?

4.17 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).

4.18 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.

4.19 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

4.20 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.

Regulation 7(3)(a)

4.21 As regards money laundering and terrorist financing, managing and mitigating the risks will involve measures to verify the customer's identity; collecting additional 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 can use customer verification procedures carried out by other firms. Firms must determine the extent of their CDD measures on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction.

4.22 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.

4.23 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 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.

4.24 Where a customer is assessed as carrying a higher risk, then depending on the product sought, it will be necessary 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 5.5.

4.25 In order to be able to identify customer transactions or activity that may be suspicious, it is necessary to monitor such transactions or activity in some way. Guidance on monitoring customer transactions and activity is given in section 5.7. 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.

4.26 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.

4.27 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 7 – Staff awareness, training and alertness).

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

SYSC 6.3.3 R

4.28 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

4.29 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 6.3.3 R

4.30 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 must therefore ensure that their risk management processes for managing money laundering and terrorist financing risks are kept under regular review.

4.31 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.

4.32 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.

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

4.34 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 3.28 to 3.36).

CHAPTER 5

CUSTOMER DUE DILIGENCE

- **Relevant UK law/regulation**
  - Regulations 5-9, 11-17, 18
  - POCA ss 330 – 331, 334(2), 342
  - Counter-terrorism Act 2008, Schedule 7
  - Financial sanctions legislation
- **Customers that may not be dealt with**
  - Regulation 18 – HM Treasury powers to prohibit firms from forming, or to require them to terminate, relationships with customers situated in a given country to which the FATF has applied counter-measures
  - UN Sanctions resolutions 1267 (1999), 1373 (2001), 1333 (2002), 1390 (2002) and 1617 (2005)
  - EC Regulation 2580/2001, 881/2002 (as amended), 423/2007 and 1110/2008
  - Terrorism Act, 2000, Sch 2
  - Terrorism (United Nations Measures) Orders 2006 and 2009
  - Al-Qa'ida and Taliban (United Nations Measures) Order 2006
  - HM Treasury Sanctions Notices and News Releases
- **Regulatory regime**
  - SYSC 6.1.1 R, 6.3.7(5) G
- **Other material pointing to good practice**
  - FATF Recommendations
  - FATF Guidance on the risk-based approach: High level principles and procedures
  - Basel CDD paper
  - IAIS Guidance Paper 5
  - IOSCO Principles paper
  - Basel Consolidated KYC Risk Management Paper

- **Core obligations**
  - Must carry out prescribed CDD measures for all customers not covered by exemptions
  - Must have systems to deal with identification issues in relation to those who cannot produce the standard evidence
  - Must apply enhanced due diligence to take account of the greater potential for money laundering in higher risk cases, specifically when the customer is not physically present when being identified, and in respect of PEPs and correspondent banking
  - 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 keeping customer information up to date

5.1 Meaning of customer due diligence measures and ongoing monitoring

5.1.1 The ML Regulations 2007 specify CDD measures that are required to be carried out, and the timing, as well as actions required if CDD measures are not carried out. The Regulations then describe customers and products in respect of which no, or limited, CDD measures are required (referred to as 'Simplified Due Diligence'), and those customers and circumstances where enhanced due diligence is required. Provision for reliance on other regulated firms in the carrying out of CDD measures are then set out.

5.1.2 Schedule 7 to the Counter-terrorism Act 2008 gives HM Treasury power to require firms, in particular circumstances, to carry out enhanced CDD and

monitoring.

5.1.3 This chapter therefore gives guidance on the following:

- The meaning of CDD measures (5.1.5 – 5.1.14)
- Timing of, and non-compliance with, CDD measures (5.2.1 – 5.2.13)
- Application of CDD measures (section 5.3)
- Simplified due diligence (section 5.4)
- Enhanced due diligence (section 5.5)
- Reliance on third parties and multipartite relationships (section 5.6)
- Monitoring customer activity (section 5.7)
- Directions under the Counter-Terrorism Act 2008 (section 5.8)

Regulation 7(3)(a) and 8(3)

5.1.4 Firms must determine the extent of their CDD measures and ongoing monitoring on a risk-sensitive basis, depending on the type of customer, business relationship, product or transaction. They must be able to demonstrate to their supervisory authority that the extent of their CDD measures and monitoring is appropriate in view of the risks of money laundering and terrorist financing.

What is customer due diligence?

Regulation 5(1)

5.1.5 The CDD measures that must be carried out involve:

(a) identifying the customer, and verifying his identity (see paragraphs 5.3.2ff**);**
(b) identifying the beneficial owner, where relevant, and verifying his identity (see paragraphs 5.3.8ff)**;** and
(c) obtaining information on the purpose and intended nature of the business relationship (see paragraphs 5.3.21ff**)**.

Regulation 5(b)

5.1.6 Where the customer is a legal person (such as a company) or a legal arrangement (such as a trust), part of the obligation on firms to identify any beneficial owner of the customer means firms taking measures to understand the ownership and control structure of the customer.

5.1.7 Working out who is a beneficial owner may not be a straightforward matter. Different rules apply to different forms of entity (see paragraphs 5.3.8ff).

Regulations 13 and 14

5.1.8 For some particular customers, products or transactions, simplified due diligence (SDD) may be applied; in the case of higher risk situations, and specifically in relation to customers who are not physically present when their identities are verified, correspondent banking and PEPs, enhanced due diligence (EDD) measures must be applied on a risk sensitive basis. For

- guidance on applying SDD see section 5.4
- guidance on applying EDD see section 5.5

What is ongoing monitoring?

Regulation 8

5.1.9 Firms must conduct ongoing monitoring of the business relationship with their customers (see paragraphs 5.7.1ff). This is a separate, but related, obligation from the requirement to apply CDD measures.

Why is it necessary to apply CDD measures and conduct ongoing monitoring?

Regulations 7 and 8
POCA, ss 327-334
Terrorism Act s 21A

5.1.10 The CDD and monitoring obligations on firms under legislation and regulation are designed to make it more difficult for the financial services industry to be used for money laundering or terrorist financing.

5.1.11 Firms also need to know who their customers are 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.

5.1.12 Firms therefore need to carry out customer due diligence, and monitoring, 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.

5.1.13 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 nature 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.

Other material, pointing to good practice

5.1.14 FATF, the Basel Committee, IAIS and IOSCO have issued recommendations on the steps that should be taken to identify customers. FATF has also published guidance on high level principles and procedures on the risk-based approach. 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: www.fatf-gafi.org; www.bis.org; www.iaisweb.org; www.iosco.org. Where relevant, firms are encouraged to use these websites to keep up to date with developing industry guidance from these bodies. The private sector Wolfsberg Group has also issued relevant material, see www.wolfsberg-principles.com.

5.2 Timing of, and non compliance with, CDD measures

Regulation 7

5.2.1 A firm must apply CDD measures when it does any of the following:
(a) establishes a business relationship;
(b) carries out an occasional transaction;
(c) suspects money laundering or terrorist financing; or
(d) doubts the veracity of documents, data or information previously obtained for the purpose of identification or verification.

Timing of verification

Regulation 9(2)

5.2.2 **General rule**: The verification of the identity of the customer and, where applicable, the beneficial owner, must, subject to the exceptions referred to below, take place before the establishment of a business relationship or the carrying out of an occasional transaction.

Regulation 9(4)

5.2.3 **Exception for life assurance:** The verification of the identity of the beneficiary under a life assurance policy may take place after the business relationship has been established provided that it takes place at or before the time of payout or at or before the time the beneficiary exercises a right vested under the policy. [See Part II, sector 7, paragraph 7.31 for further guidance.]

Regulation 9(5)

5.2.4 **Exception when opening a bank account:** The verification of the identity of a bank account holder may take place after the bank account has been opened, provided that there are adequate safeguards in place to ensure that

(a) the account is not closed
(b) transactions are not carried out by or on behalf of the account holder (including any payment from the account to the account holder)

before verification has been completed.

Regulation 9(3)

5.2.5 **Exception if necessary not to interrupt normal business and there is little risk:** In any other case, verification of the identity of the customer, and where there is one, the beneficial owner, may be completed during the establishment of a business relationship if

(a) this is necessary not to interrupt the normal conduct of business and
(b) there is little risk of money laundering or terrorist financing occurring

provided that the verification is completed as soon as practicable after the initial contact.

Requirement to cease transactions, etc

Regulation 11(1)

5.2.6 Where a firm is unable to apply CDD measures in relation to a customer, the firm

(a) must not carry out a transaction with or for the customer through a bank account;
(b) must not establish a business relationship or carry out an occasional transaction with the customer;
(c) must terminate any existing business relationship with the customer;
(d) must consider whether it ought to be making a report to SOCA, in accordance with its obligations under POCA and the Terrorism Act.

5.2.7 Firms should always consider whether an inability to apply CDD measures is caused by the customer not possessing the 'right' documents or information. In this case, the firm should consider whether there are any other ways of being reasonably satisfied as to the customer's identity. In either case, the firm should consider whether there are any circumstances which give grounds for making a report.

5.2.8 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 SOCA (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.

5.2.9 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 return the funds to the source from which they came. Returning the funds in such a circumstance is part of the process of terminating the relationship; it is closing the account, rather than carrying out a transaction with the customer through a bank account.

Electronic transfer of funds

EC Regulation 1781/2006

5.2.10 To implement FATF Special Recommendation VII, the EU adopted Regulation 1781/2006, which came into force on 1 January 2007, and is directly applicable in all member states. The Recommendation requires that payment services providers (PSPs) must include certain information in electronic funds transfers and ensure that the information is verified. The core requirement is that the payer's name, address and account number are included in the transfer, but there are a number of permitted exemptions, concessions and variations. For guidance on how to meet the obligations under the Regulation, see Part II, Specialist Guidance A: *Wire transfers*.

5.2.11 The Regulation includes (among others) the following definitions:

- 'Payer' means either a natural or legal person who holds an account and allows a transfer of funds from that account.
- 'Payment service provider' means a natural or legal person whose business includes the provision of transfer of funds services.
- 'Intermediary payment service provider' means a payment service provider, neither of the payer nor of the payee, that participates in the execution of transfers of funds.

5.2.12 Accordingly, a financial sector business needs to consider which role it is fulfilling when it is involved in a payment chain. For example, a bank or building society effecting an electronic funds transfer on the direct instructions of a customer to the debit of that customer's account will clearly be a PSP whether it undertakes the payment itself (when it must provide its customer's details as the payer), or via an intermediary PSP. In the latter case it must provide the required information on its customer to the intermediary PSP including when it inputs the payment through an electronic banking product supplied by the intermediary PSP.

5.2.13 In other circumstances when a financial sector business, whether independent of the PSP or a specialist function within the same group, passes the transaction through an account in its own name, it may reasonably consider itself under the above definitions as the payer, rather than the PSP, even though the transaction relates ultimately to a customer, e.g., mortgages, documentary credits, insurance claims, financial markets trades. In these cases, if XYZ is the name of the financial sector business initiating the transfer as a customer of the PSP, XYZ can input its own name if using an

electronic banking product. There is nothing in the Regulation to prevent including the name of the underlying client elsewhere in the transfer, if XYZ wishes to do so.

5.3 Application of CDD measures

Regulation 5(1)

5.3.1 Applying CDD measures involves several steps. The firm is required to verify the identity of customers and, where applicable, beneficial owners. Information on the purpose and intended nature of the business relationship must also be obtained.

Identification and verification of the customer

5.3.2 The firm *identifies* the customer by obtaining a range of information about him. The *verification* of the identity consists of the firm verifying some of this information against documents, data or information obtained from a reliable and independent source.

5.3.3 The term 'customer' is not defined in the ML Regulations, and its meaning has to be inferred from the definitions of 'business relationship' and 'occasional transaction', the context in which it is used in the ML Regulations, and its everyday dictionary meaning. It should be noted that for AML/CTF purposes, a 'customer' may be wider than the FSA Glossary definition of 'customer'.

5.3.4 In general, the customer will be the party, or parties, with whom the business relationship is established, or for whom the transaction is carried out. Where, however, there are several parties to a transaction, not all will necessarily be customers. Further, more specific, guidance for relevant sectors is given in Part II. Section 5.6 is also relevant in this context.

Regulation 2(1)

5.3.5 A "business relationship" is defined in the ML Regulations as a business, professional or commercial relationship between a firm and a customer, which is expected by the firm when contact is established to have an element of duration. A relationship need not involve the firm in an actual transaction; giving advice may often constitute establishing a business relationship.

Regulation 2(1)

5.3.6 An "occasional transaction" means a 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), amounting to €15,000 or more, whether the transaction is carried out in a single operation or several operations which appear to be linked.

5.3.7 The factors linking transactions to assess whether there is a business relationship are inherent in the characteristics of the transactions – 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 situations that do not otherwise give rise to a business relationship, a three-month period for linking transactions might be appropriate, assuming this is not a regular occurrence.

Identification and verification of a beneficial owner

Regulations 6, 5(b)

5.3.8 A beneficial owner is normally an individual who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted. In respect of private individuals the customer himself is the beneficial owner, unless there are features of the transaction, or surrounding circumstances, that indicate otherwise. Therefore, there is no requirement on firms to make proactive searches for beneficial owners in such cases, but they should make appropriate enquiries where it appears that the customer is not acting on his own behalf.

Regulation 6

5.3.9 The ML Regulations define beneficial owners as individuals either owning or controlling more than 25% of body corporates or partnerships (or at least 25% of trusts) or otherwise owning or controlling the customer. These individuals must be identified, and risk-based and adequate measures must be taken to verify their identities.

5.3.10 Where an individual is required to be *identified* as a beneficial owner in the circumstances outlined in paragraph 5.3.8, where a customer who is a private individual is fronting for another individual who is the beneficial owner, the firm should obtain the same information about that beneficial owner as it would for a customer. For identifying beneficial owners of customers other than private individuals see paragraphs 5.3.115 onwards.

Regulation 5(a) and (b)

5.3.11 The *verification* requirements under the ML Regulations are, however, different as between a customer and a beneficial owner. The identity of a customer must be verified on the basis of documents, data or information obtained from a reliable and independent source. The obligation to verify the identity of a beneficial owner is for the firm to take risk-based and adequate measures so that it is satisfied that it knows who the beneficial owner is. It is up to each firm to consider whether it is appropriate, in light of the money laundering or terrorist financing risk associated with the business relationship, to make use of records of beneficial owners in the public domain (if any exist), ask their customers for relevant data, require evidence of the beneficial owner's identity on the basis of documents, data or information obtained from a reliable and independent source or obtain the information otherwise.

5.3.12 In low risk situations, therefore, it may be reasonable for the firm to confirm the beneficial owner's identity based on information supplied by the customer. This could include information provided by the customer (including trustees or other representatives whose identities have been verified) as to their identity, and confirmation that they are known to the customer. While this may be provided orally or in writing, any information received orally should be recorded in written form by the firm.

Regulation 6(3)(b)

5.3.13 In some trusts and similar arrangements, instead of being an individual, the beneficial owner may be a class of persons who may benefit from the trust (see paragraphs 5.3.246ff). Where only a class of persons is required to be identified, it is sufficient for the firm to ascertain and name the scope of the class. It is not necessary to identify every individual member of the class.

Existing customers

Regulations 7(2), 16(4)

5.3.14 Firms must apply CDD measures at appropriate times to its existing customers on a risk-sensitive basis. Firms must also apply CDD measures to any anonymous accounts or passbooks before they are used. The obligation

to report suspicions of money laundering, or terrorist financing, however, applies in respect of *all* the firm's customers, as does the UK financial sanctions regime (see paragraphs 5.3.41-5.3.63).

5.3.15 As risk dictates, therefore, firms must take steps to ensure that they hold appropriate information to demonstrate that they are satisfied that they know all their customers. Where the identity of an existing customer has already been verified to a previously applicable standard then, in the absence of circumstances indicating the contrary, the risk is likely to be low. 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 6.1.1 R

5.3.16 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/CTF – 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

5.3.17 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.

5.3.18 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

5.3.19 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 the identities of its customers have been verified.

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.

5.3.20 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.

Nature and purpose of proposed business relationship

Regulation 5(c)

5.3.21 A firm must understand the purpose and intended nature of the business relationship or transaction to assess whether the proposed business relationship is in line with the firm's expectation and to provide the firm with a meaningful basis for ongoing monitoring. In some instances this will be self-evident, but in many cases the firm may have to obtain information in this regard.

5.3.22 Depending on the firm's risk assessment of the situation, information that might be relevant may include some or all of the following:

- 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;
- the origin of the initial and ongoing source(s) of wealth and funds (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.

Keeping information up to date

Regulation 8(2)(b)

5.3.23 Where information is held about customers, it must, 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 (unless doubts arise as to the veracity or adequacy of the evidence previously obtained for the purposes of customer identification); as risk dictates, however, firms must take steps to ensure that they hold appropriate up-to-date information on 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.

5.3.24 Although keeping customer information up-to-date is required under the ML Regulations, this is also a requirement of the Data Protection Act in respect of personal data.

Characteristics and evidence of identity

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

5.3.26 The identity of a customer who is not a private individual is a combination of its constitution, its business, and its legal and ownership structure.

5.3.27 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 assurances from persons or organisations that have dealt with the customer for some time.

Regulation 5(3)(a)

5.3.28 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 must 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.

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

Documentary evidence

5.3.30 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 equivalent legislation; then
- those issued by other organisations.

5.3.31 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.

5.3.32 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

5.3.33 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/CTF 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.

5.3.34 External electronic databases are accessible directly by firms, or through independent third party organisations. The size of the electronic 'footprint' (see paragraph 5.3.25) 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

5.3.35 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.

5.3.36 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.

5.3.37 Negative information includes lists of individuals known to have committed fraud, including identity fraud, and registers of deceased persons. Checking against such information may be necessary to mitigate against impersonation fraud.

5.3.38 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

5.3.39 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.

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

Persons firms should not accept as customers

5.3.41 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 comprehensive freeze of funds and economic resources, together with a prohibition on making funds or economic resources available to the designated target. A Consolidated List of all targets to whom financial sanctions apply is maintained by HM Treasury, and includes all individuals and entities that are subject to financial sanctions in the UK. This list is at: www.hm-treasury.gov.uk/financialsanctions.

5.3.42 The obligations under the UK financial sanctions regime apply to all firms, and not just to banks. The Consolidated List includes all the names of designated persons under UN and EC sanctions regimes which have effect in the UK. Firms will not normally have any obligation under UK law to have regard to lists issued by other organisations or authorities in other countries, although a firm doing business in other countries will need to be aware of the scope and focus of relevant financial sanctions regimes in those countries. The other websites referred to below may contain useful background information, but the purpose of the HM Treasury list is to draw together in one place all the names of designated persons for the various sanctions regimes effective in the UK. 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 HM Treasury 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.

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

5.3.44 The HM Treasury 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 HM Treasury, and links to other useful websites. HM Treasury may also be contacted direct to provide guidance and to assist with any concerns regarding the implementation of financial sanctions:

Asset Freezing Unit
HM Treasury
1 Horse Guards Road
LONDON SW1A 2HQ
Tel: +44 (0) 20 7270 5454
Email: assetfreezingunit@hm-treasury.gov.uk

5.3.45 An asset freeze works by way of a prohibition against dealing with the funds or economic resources of a designated person. It is also prohibited to make funds or economic resources (and in relation to designated terrorists, financial services) available, directly or indirectly, to or for the benefit of targets on the list maintained by HM Treasury. Firms therefore need to have an appropriate means of monitoring payment instructions to ensure that the prohibitions are not breached. A breach could involve the making of payments to or for the benefit of designated persons, whether or not the payment is made direct to the designated person, through an intermediary or in a manner which is for the benefit of the designated person.

5.3.46 HM Treasury can licence exceptions to the prohibitions to enable frozen funds and economic resources to be unfrozen and to allow payments to be made to or for the benefit of a designated person. A firm seeking such a licence should write to the Asset Freezing Unit at the address set out in paragraph 5.3.44.

5.3.47 If a firm breaches a sanctions prohibition, it is likely to have committed a criminal offence. 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/code_for_crown_prosecutors/index.html

5.3.48 To reduce the risk of breaching 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.

5.3.49 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.

5.3.50 Where a firm freezes funds under financial sanctions legislation, or where it has suspicions of terrorist financing, it must make a report to HM Treasury, and/or to SOCA. Guidance on such reporting is given in paragraphs 6.33 to 6.42.

Terrorism

UNSCR 1373 (2001)

5.3.51 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)

5.3.52 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)

5.3.53 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)

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

5.3.55 The texts of the EC Regulations referred to in paragraphs 5.3.53 and 5.3.54, and the lists of persons targeted, are available at http://ec.europa.eu/external_relations/cfsp/sanctions/docs/measures_en.pdf As noted above, names of persons and entities on the EU list will be included in the Consolidated List maintained by HM Treasury.

2010 c38 Al-Qa'ida and Taliban (United Nations Measures) Order 2006

5.3.56 The UK has implemented UNSCR 1373 and its successor resolutions under the Terrorist Asset-Freezing etc Act 2010 (which replaced the Terrorism (United Nations Measures) Order 2006 and the Terrorism (United Nations Measures) Order 2009), and UNSCR 1267 and its successor resolutions under the Al-Qa'ida and the Taliban (United Nations Measures) Order 2006.

2010 c38

5.3.57 Acting under the Terrorist Asset-Freezing etc Act 2010, where HM Treasury has reasonable grounds for suspecting that the person is or may be a person who commits, attempts to commit, facilitates or participates in the commission of acts of terrorism, it can designate that person for the purposes of the financial sanctions. This might result in the addition of a name to the HM Treasury list that might not appear on the equivalent UN

or EU lists. HM Treasury also has certain designation powers under the Al-Qa'ida and Taliban (United Nations Measures) Order 2006.

Terrorism Act Sch 2

5.3.58 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 HM Treasury.

5.3.59 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

5.3.60 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

5.3.61 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, http://ec.europa.eu/external_relations/cfsp/sanctions/docs/measures_en.pdf

5.3.62 In most cases, EC Regulations directly apply to give effect to those sanctions regimes. In addition, the UK implements or enforces 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 in these sanctions regimes apply in respect of funds and economic resources in the same manner as those in the terrorism sanctions. Where relevant, any specific individuals and entities subject to such targeted countries/regimes will be included on the HM Treasury Consolidated List. Details of the UK regime is available at http://www.hm-treasury.gov.uk/fin_sanctions_index.htm.

Regulation 18 CTA 2008, Schedule 7

5.3.63 HM Treasury may direct that a firm may not enter into a business relationship, carry out an occasional transaction, or proceed further with a business relationship or occasional transaction, in relation to a person who is based or incorporated in a non EEA state to which the FATF has decided to apply counter-measures. Details of any such HM Treasury directions will be found at www.hm-treasury.gov.uk or www.jmlsg.org.uk. Guidance on complying with directions issued by HM Treasury under CTA 2008, Schedule 7 is given in Part III, section 5.

5.3.64 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.berr.gov.uk/whatwedo/europeandtrade/strategic-export-control/index.html

Shell banks and anonymous accounts

Regulation 16 (1), (2), (5)

5.3.65 Firms must not enter into, or continue, a correspondent banking relationship with a shell bank. Firms must take appropriate measures to ensure that it does not enter into or continue a correspondent naming relationship with a bank that is known to permit its accounts to be used by a shell bank. A shell bank is an entity incorporated in a jurisdiction where it has no physical presence involving meaningful decision-making and management, and which is not part of a financial conglomerate.

Regulation 16 (3), (4)

5.3.66 Firms carrying on business in the UK must not set up an anonymous account or an anonymous passbook for any new or existing customer. All firms carrying on business in the UK must apply CDD measures to all existing anonymous accounts and passbooks before such accounts or passbooks are used in any way.

5.3.67 Firms should pay special attention to any money laundering or terrorist financing threat that may arise from products or transactions that may favour anonymity and take measures, if needed, to prevent their use for money laundering or terrorist financing purposes.

Private individuals

General

5.3.68 Paragraphs 5.3.70 to 5.3.82 refer to the standard identification requirement for customers who are private individuals; paragraphs 5.3.83 to 5.3.114 provide further guidance on steps that may be applied as part of a risk-based approach.

5.3.69 Depending on the circumstances relating to the customer, the product and the nature and purpose of the proposed relationship, firms may also need to apply the following guidance to identifying, and verifying the identity of, beneficial owners, and to other relevant individuals associated with the relationship or transaction (but see paragraphs 5.3.11 and 5.3.12).

Obtain standard evidence

Identification

5.3.70 The firm should obtain the following information in relation to the private individual:

- full name
- residential address
- date of birth

Verification

5.3.71 Verification of the information obtained must be based on reliable and independent sources – which might either be 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

5.3.72 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.

5.3.73 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.

5.3.74 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
- 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, a regulated utility company, or another FSA-regulated firm in the UK financial services sector, or in an equivalent 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 an equivalent jurisdiction (but not ones printed off the internet) ➢ Utility bills (but not ones printed off the internet)

5.3.75 The examples of other documents are intended to support a customer's address, and so it is likely that they will have been delivered to the customer through the post, rather than being accessed by him across the internet.

5.3.76 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).

5.3.77 In practical terms, this means that, for face-to-face verification, production of a valid passport or photocard driving licence (so long as the photograph is in date[3]) should enable most individuals to meet the identification requirement for AML/CTF 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 5.3.98 to 5.3.114).

5.3.78 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. Examples of sources of information include CIFAS, the Fraud Advisory Panel and the Serious

[3] It should be noted that as well as a general expiry date for UK driving licences, the photograph has a separate expiry date (10 years from first issue). Northern Ireland driving licences have a single expiry date, which is ten years from date of issue.

Fraud Office. Commercial software is also available that checks the algorithms used to generate passport numbers. This can be used to check the validity of passports of any country that issues machine-readable passports.

Electronic verification

5.3.79 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 5.3.39 and 5.3.40, that provide a reasonable assurance that the customer is who he says he is.

5.3.80 As well as requiring a commercial agency used for electronic verification to meet the criteria set out in paragraphs 5.3.39 and 5.3.40, 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 5.3.35-5.3.38, and cumulatively meet the standard level of confirmation set out above.

5.3.81 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 5.3.82.

Mitigation of impersonation risk

5.3.82 Where identity is verified electronically, or copy documents are used, 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 may include:

- 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 an equivalent jurisdiction;
- verifying additional aspects of the customer's identity, or of his electronic 'footprint' (see paragraph 5.3.25);
- 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;

- other card or account activation procedures;

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

Other considerations

5.3.83 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.

5.3.84 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.

5.3.85 For higher risk customers, the need to have additional information needs to be balanced against the possibility of instituting enhanced monitoring (see sections 5.5 and 5.7).

Executors and personal representatives

Regulation 6(8)

5.3.86 In the case of an estate of a deceased person in the course of administration, the beneficial owner is

- in England and Wales, the executor, original or by representation, or administrator for the time being of a deceased person; and
- in Scotland, the executor for the purposes of the Executors (Scotland) Act 1900[4].

In circumstances where an account is opened or taken over by executors or administrators 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 those personal representatives. 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, or to an appropriate professional register.

Court of Protection orders and court-appointed deputies

2005, c 9
SI 2007/1253

5.3.87 Under the Mental Capacity Act 2005 (and related Regulations), the Court of Protection will be able to make an order concerning a single decision in cases where a one-off decision is required regarding someone who lacks capacity. The Court can also appoint a deputy or deputies (previously referred to as receivers) where it is satisfied that a series of decisions needs to be made for a person who lacks capacity.

5.3.88 Firms may accept the court documents appointing the deputy, or concerning a single act, as evidence of identity of the person appointed. While the subject of such an order should be regarded as the beneficial owner, their identity may also be verified by reference to the court documents.

Attorneys

5.3.89 When a person deals with assets under a power of attorney, that person is also a customer of the firm. Consequently, the identity of holders of powers of attorney should be verified, in addition to that of the donor.

5.3.90 Where the donor of a power of attorney has capacity, and therefore has control, he remains the owner of the funds, and is the customer. Other than where he is an existing customer of the firm, therefore, his identity must be verified. In many cases, these customers may not possess the standard identity documents referred to in paragraphs 5.3.74ff, and firms may have to accept some of the documents referred to in paragraph 5.3.104.

[4] 1900 c.55. Sections 6 and 7 were amended by the Succession (Scotland) Act 1964 (c.41)

5.3.91 In circumstances where he has lost capacity, the donor no longer has control of the property, but his identity should be verified as the beneficial owner. When an Enduring Power of Attorney is registered with the Court of Protection, the firm will know that the donor has lost, or is losing, capacity. A Lasting Power of Attorney cannot be used until it has been registered, but, subject to any restrictions, this may be done at any time, and while the donor is still able to manage their affairs. Therefore, the firm will not necessarily know whether or not the donor has lost capacity. Where the firm is satisfied that the donor has lost capacity it should verify his identity as a beneficial owner.

Source of funds as evidence

5.3.92 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 an equivalent 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.

5.3.93 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. Part II, sector 3: *Electronic Money* includes guidance on accepting the funding instrument used to load a purse as a form of initial verification in low risk situations, subject to compensating monitoring controls and turnover limits, and establishing that the customer has rightful control over the instrument.

5.3.94 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 customers themselves, on a face-to-face basis where identity can be confirmed.

5.3.95 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.

5.3.96 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.

5.3.97 Part II, sector 8: *Non-life providers of investment fund products* provides additional guidance to investment fund managers in respect of customers whose identity may not need to be verified until the time of redemption.

Customers who cannot provide the standard evidence

5.3.98 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/partners 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 6.3.7 (5) G Promoting Financial Inclusion, December 2004

5.3.99 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.

5.3.100 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.

5.3.101 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 private individuals set out in paragraphs 5.3.70 to 5.3.97 cannot reasonably be applied.

5.3.102 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 5.3.104 to 5.3.114.

5.3.103 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

5.3.104 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

5.3.105 Guidance on dealing with customers who lack capacity to manage their affairs, such as the mentally incapacitated, or people with learning difficulties, covering Powers of Attorney; Receivership (or short) order; and Appointeeship, are set out in a BBA leaflet, "Banking for people who lack capacity to make decisions", which can be obtained from the British Bankers' Association at www.bba.org.uk. (see also paragraphs 5.3.87 – 5.3.91)

Gender reassignment

5.3.106 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

5.3.107 When opening accounts for students or other young people, the standard identification requirement should be followed as far as possible (see paragraphs 5.3.70 – 5.3.97). 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 UK Border Agency website http://www.bia.homeoffice.gov.uk/employers/points/ sponsoringmigrants/registerofsponsors/ and Part II, sector 1: *Retail banking*, Annex 1-I). 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. UCAS also maintain a database of students who have confirmed places at a University/Higher Education establishment, which is accessible on subscription (see www.ucasmedia.co.uk/).

5.3.108 All international students, other than those from EEA countries or Switzerland, undergo rigorous checks by the immigration services at home and abroad in order to be satisfied as to their identity and bona fides before they are given leave to enter or remain in the UK as a student or prospective student. Applicants must meet the requirements of the Student Immigration Rules and must provide documentation which demonstrates that they intend to study, and have been accepted, on a course of study at a bona fide institution. This includes the provision of a course admission letter from the education institution. If they cannot provide the documents they will not be given leave to enter or remain in the UK.

5.3.109 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

5.3.110 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.

5.3.111 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.

5.3.112 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 enhanced due diligence (see section 5.5) or monitoring (see section 5.7) 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.

5.3.113 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 section 5.7). 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.

5.3.114 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.

Customers other than private individuals

5.3.115 Depending on the nature of the entity, a relationship or transaction with a customer who is not a private individual may be entered into in the customer's own name, or in that of specific individuals or other entities on its behalf. 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 5(b)

5.3.116 In deciding who the beneficial owner is in relation to a customer who is not a private individual, the firm's objective must be to know who has ownership or 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. Verifying the identity of the beneficial owner(s) will be carried out on a risk-based approach, following the guidance in paragraphs 5.3.11 and 5.3.12, 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.

5.3.117 Firms also have obligations under the UK financial sanctions regime (see Part III, section 4: *Compliance with the UK financial sanctions regime)* which require the collection of information in relation to trustees, directors or equivalent (see Part III, paragraphs 4.51 – 4.52). In determining the information to be collected, therefore, firms should take account of their information needs in relation to sanctions compliance.

5.3.118 Certain other information about the entity 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 should be verified. 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 5.5).

Regulation 14(1(b) and (4)

5.3.119 Where an entity is known to be linked to a PEP (perhaps through a directorship or shareholding), or to a jurisdiction assessed as carrying a higher money laundering/terrorist financing risk, it is likely that this will put the entity into a higher risk category, and that enhanced due diligence measures should therefore be applied (see sections 5.5 and 5.7).

5.3.120 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.

5.3.121 This section provides guidance on verifying the identity of a range of non-

personal entities, as follows:

- Regulated financial services firms subject to the ML Regulations (or equivalent) (paragraphs 5.3.122 to 5.3.126)
- Other firms subject to the ML Regulations (or equivalent) (paragraphs 5.3.127 to 5.3.130)
- Corporate customers (other than regulated firms) (paragraphs 5.3.131 to 5.3.162)
- Partnerships and unincorporated businesses (paragraphs 5.3.163 to 5.3.177)
- Public sector bodies, governments, state-owned companies and supranationals (paragraphs 5.3.178 to 5.3.191)
- Sovereign Wealth Funds (paragraphs 5.3.192-5.3.215)
- Pension schemes (paragraphs 5.3.216 to 5.3.225)
- Charities, church bodies and places of worship (paragraphs 5.3.226 to 5.3.245)
- Other trusts and foundations (paragraphs 5.3.246 to 5.3.269)
- Clubs and societies (paragraphs 5.3.270 to 5.3.278)

Regulated financial services firms subject to the ML Regulations (or equivalent)

Regulation 13(2)

5.3.122 In respect of other financial services firms (including their nominee or trustee subsidiaries) which are subject to the ML Regulations or equivalent, and which are regulated in the UK by the FSA, or in the EU or an equivalent jurisdiction, by an equivalent regulator, simplified due diligence may be applied (see section 5.4).

Regulation 13(1)

5.3.123 Firms must, however, have reasonable grounds for believing that the customer qualifies for the treatment in paragraph 5.3.122.

5.3.124 Having reasonable grounds might involve:

- checking with the home country central bank or relevant supervisory body; or
- checking with another office, subsidiary, branch or correspondent bank in the same country; or
- checking with a regulated correspondent bank of the overseas institution; or
- obtaining from the relevant institution evidence of its licence or authorisation to conduct financial and/or banking business.

To assist firms, a list of the regulatory authorities in EU and FATF member states is available at www.jmlsg.org.uk.

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

5.3.126 Firms should take appropriate steps to be reasonably satisfied that the person they are dealing with is properly authorised by the customer.

Other firms that are subject to the ML Regulations (or equivalent)

5.3.127 Customers which are subject to the ML Regulations or equivalent, but which are not regulated in the UK, the EU or an equivalent jurisdiction as a financial services business, should be treated, for AML/CTF purposes, according to their legal form: for example, as private companies, in accordance with the guidance set out in paragraphs 5.3.149 to 5.3.162; 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 professional individuals are acting in their personal capacity, for example, as trustees, their identity should normally be verified as for any other private individual.

5.3.128 Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer.

5.3.129 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.

Regulation 13(4)

5.3.130 Independent legal professionals that are subject to the ML Regulations, or from third countries where they are subject to equivalent requirements (and are supervised for compliance with those requirements), and which hold client money in pooled accounts (whether in a bank account or through a securities holding), are obliged to verify the identities of their clients. Financial services firms with which such client accounts are held are not required to identify the beneficial owners of such funds, provided that the information on the identity of the beneficial owner is available, on request, to the firm. As a practical matter, firms may reasonably apply a similar approach to such client accounts which only contain the funds of a single beneficial owner. Similarly, firms may reasonably apply this approach to pooled accounts maintained by landlords or property managers in respect of tenants' service charges or security deposits.

Corporate customers (other than regulated firms)

5.3.131 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.

Regulation 20(2)(a)

5.3.132 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.

5.3.133 Control over companies may be exercised through a direct shareholding or through intermediate holding companies. 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 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.

Regulation 5(c)

5.3.134 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 must obtain sufficient additional information on the nature of the company's business, and the reasons for seeking the product or service.

Regulation 6(1)

5.3.135 In the case of a body corporate the beneficial owner includes any individual who:

- as respects any body other than a company listed on a regulated market, ultimately owns or controls (whether through direct or indirect ownership or control, including through bearer share holdings) more than 25% of the shares or voting rights in the body; or
- as respects any body corporate, otherwise exercises control over the management of the body.

5.3.136 Directors of a body corporate do not fall under the definition of beneficial owner, as in the capacity of director they do not have an ownership interest in the body, nor do they control the voting rights in the body, nor do they exercise control over management in the sense of being able to control the composition and/or voting of the board of directors.

5.3.137 Paragraphs 5.3.138 – 5.3.141 refer to the standard evidence for corporate customers, and paragraphs 5.3.142 – 5.3.148 provide further supplementary guidance on steps that may be applied as part of a risk-based approach.

Obtain standard evidence

5.3.138 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 or unlisted companies:

- names of all directors (or equivalent)
- names of individuals who own or control over 25% of its shares or voting rights
- names of any individual(s) who otherwise exercise control over the management of the company

5.3.139 The firm should verify the existence of the corporate from:

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

or a search of the relevant company registry

or a copy of the company's Certificate of Incorporation

5.3.140 Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer.

5.3.141 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.

Companies listed on regulated markets (EEA or equivalent)

5.3.142 Corporate customers whose securities are admitted to trading on a regulated market in an EEA state or one in an equivalent jurisdiction are publicly owned and generally accountable.

Regulation 13(3)

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

- a company which is listed on a regulated market (within the meaning of MiFID) in the EEA, or on a non-EEA market that is subject to specified disclosure obligations; or
- a majority-owned and consolidated subsidiary of such a listed company

simplified due diligence may be applied (see section 5.4).

Regulation 2(1)

5.3.144 Specified disclosure obligations are disclosure requirements consistent with specified articles of:

- The Prospectus directive [2003/71/EC]
- The Transparency Obligations directive [2004/109/EC]
- The Market Abuse directive[2003/6/EC]

Regulations 2(1) and 13(3)

5.3.145 If a regulated market is located within the EEA 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. If the market is outside the EEA, but is one which subjects companies whose securities are admitted to trading to disclosure obligations which are contained in international standards and are equivalent to the specified disclosure obligation in the EU, similar treatment is permitted. For companies listed outside the EEA on markets, which do not qualify for SDD, the standard verification requirement for private and unlisted companies should be applied.

5.3.146 The European Commission maintains a list of regulated markets within the EU at ec.europa.eu/internal_market/securities/isd/mifid_en.htm. Firms should note that AIM is not a regulated market under MiFID. However, due diligence requirements at admission and ongoing disclosure requirements on AIM are broadly similar to those of regulated markets. A firm may, therefore, under its risk-based approach, regard the due diligence process for admission to AIM as giving equivalent comfort as to the identity of the company under consideration.

Other publicly listed or quoted companies

5.3.147 Companies that are listed on a regulated market that is not equivalent and thus not eligible for SDD are still subject to some degree of accountability and transparency. As part of their risk-based approach, therefore, firms may have regard to the listing conditions that apply in the relevant jurisdiction and the level of transparency and accountability to which the company is subject in determining the level of checks required and the extent to which the customer should be treated as a private company (see paragraphs 5.3.149 - 5.3.162).

5.3.148 In applying the risk based approach, firms may take into account the potentially lower risk presented by companies whose shares are traded as this makes them less likely to be established for money laundering purposes. However, the firm should, for markets that allow listed companies to have dominant shareholders (especially where they are also directors), ensure that such cases are examined more closely.

Private and unlisted companies

5.3.149 Unlike publicly quoted companies, the activities of private or unlisted 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.

5.3.150 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. Where a higher risk of money laundering is associated with the business relationship, however, EDD (and enhanced monitoring) must be applied.

5.3.151 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.

5.3.152 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.

5.3.153 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 other 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.

5.3.154 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

5.3.155 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 private individuals (paragraphs 5.3.68 to 5.3.114). 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. Firms may, of course, already be required to identify a particular director as a beneficial owner if the director owns or controls more than 25% of the company's shares or voting rights (see paragraph 5.3.135).

Beneficial owners

Regulation 6(1)
Regulation 5(b)

5.3.156 As part of the standard evidence, the firm will know the names of all individual beneficial owners owning or controlling more than 25% of the company's shares or voting rights, (even where these interests are held indirectly) or who otherwise exercise control over the management of the company. , The firm must take risk based and adequate measures to verify the identity of those individuals (see paragraphs 5.3.11 and 5.3.12).

Signatories

5.3.157 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.

Other considerations

5.3.158 Unless their securities are admitted to trading in a regulated market in an EEA state, corporate customers that are subject to statutory licensing and regulation of their industry (for example, energy, telecommunications) do not qualify for simplified due diligence. Under its risk-based approach, however, a firm may feel that, provided that it is confirmed by a reliable and independent source, imposition of regulatory obligations on such a firm gives an equivalent level of confidence in the company's public accountability. Therefore, evidence that the corporate customer is subject to the licensing and prudential regulatory regime of a statutory regulator in the EU (e.g., OFGEM, OFWAT, OFCOM or an EU equivalent), will satisfy the firm's obligation to verify the identity of such a customer.

Regulation 14(1)(b)

5.3.159 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 must, on a risk-sensitive basis, apply enhanced due diligence measures. For example, the firm will need to decide whether it should require additional identity information to be provided and/or verified (see sections 5.6 and 5.7).

5.3.160 Higher risk corporate customers may also 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.

Bearer shares

5.3.161 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.

5.3.162 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.

Partnerships and unincorporated bodies

5.3.163 Partnerships and unincorporated businesses, although principally operated by individuals, or groups of individuals, are different from private individuals 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.

Regulation 6(2)

5.3.164 The beneficial owner of a partnership is any individual who ultimately is entitled to or controls (whether the entitlement or control is direct or indirect) more than a 25% share of the capital or profits of the partnership, or more than 25% of the voting rights in the partnership, or who otherwise exercise control over the management of the partnership.

Obtain standard evidence

5.3.165 The firm should obtain the following in relation to the partnership or unincorporated association:

- full name
- business address
- names of all partners/principals who exercise control over the management of the partnership
- names of individuals who own or control over 25% of its capital or profit, or of its voting rights

5.3.166 Given the wide range of partnerships and unincorporated businesses, in terms of size, reputation and numbers of partners/principals, firms need to make an assessment of where a particular partnership or business lies on the associated risk spectrum.

5.3.167 The firm's obligation is to verify the identity of the customer using evidence from a reliable and independent source. 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, confirmation of the customer's membership of a relevant professional or trade association is likely to be able to provide such reliable and independent evidence. This does not obviate the need to verify the identity of the partnership's beneficial owners.

5.3.168 As part of the standard evidence, the firm will know the names of all individual beneficial owners owning or controlling more than 25% of the partnership's capital or profit, or its voting rights or who otherwise exercise control over the management of the partnership. The firm must take risk based and adequate measures to verify the identity of those individuals (see paragraphs 5.3.11 and 5.3.12).

5.3.169 Other partnerships and unincorporated businesses will have a lower profile, and will generally comprise a much smaller number of partners/principals. In verifying the identity of such customers, firms should primarily have regard to the number of partner/principals. Where these are relatively few, the customer should be treated as a collection of private individuals, and

follow the guidance set out in paragraphs 5.3.70 – 5.3.114; where numbers are larger, the firm should decide whether it should continue to regard the customer as a collection of private individuals, or whether it can be satisfied with evidence of membership of a relevant professional or trade association. In either circumstance, there is likely to be a need to see the partnership deed (or other evidence in the case of sole traders or other unincorporated businesses), to be satisfied that the entity exists, unless an entry in an appropriate national register may be checked.

5.3.170 For identification purposes, Scottish partnerships and limited liability partnerships should be treated as corporate customers. For limited partnerships, the identity of general partners should be verified whilst other partners should be treated as beneficial owners.

5.3.171 Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer.

5.3.172 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.

Other considerations

5.3.173 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, companies listed on a regulated market.

5.3.174 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 5.3.92 to 5.3.96 should be followed. This does not obviate the need to verify the identity of beneficial owners, where these exist.

5.3.175 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, additional precautions should be taken.

5.3.176 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 owners

5.3.177 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 as customers. 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; other partners/owners must be

verified as beneficial owners, following the guidance in paragraphs 5.3.11 and 5.3.12.

Public sector bodies, governments, state-owned companies and supranationals (other than sovereign wealth funds)

5.3.178 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 state supported schools, colleges, universities and NHS trusts.

Regulation 13(5)

5.3.179 Only simplified due diligence (see section 5.4) is required in respect of public authorities in the UK.

Regulation 13(6)
Schedule 2, Paragraph 2

5.3.180 Only simplified due diligence (see section 5.4) is required in respect of non-UK public authorities which meet the following criteria:

- the customer has been entrusted with public functions pursuant to the Treaty on the European Union, the Treaties on the European Communities or Community secondary legislation;
- the customer's identity is publicly available, transparent and certain;
- the activities of the customer and its accounting practices are transparent; and
- either the customer is accountable to a Community institution or to the authorities of an EEA state, or otherwise appropriate check and balance procedures exist ensuring control of the customer's activity.

Regulation 13(1)

5.3.181 Firms must, however, have reasonable grounds for believing that the customer qualifies for the treatment in paragraphs 5.3.179 or 5.3.180.

Obtain standard evidence

5.3.182 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)

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

5.3.184 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.

5.3.185 Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer.

Signatories

5.3.186 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

5.3.187 State supported schools, colleges and universities should be treated as public sector bodies, in accordance with the guidance set out in paragraphs 5.3.177 to 5.3.185. The UK Border Agency maintains a register of sponsors [www.bia.homeoffice.gov.uk/employers/points/sponsoringmigrants/registerofsponsors/], which may assist firms in verifying the existence of such customers. The register of sponsors lists all organisations that the UK Border Agency has approved to employ migrants or sponsor migrant students.

5.3.188 For independent schools and colleges, firms should refer to the guidance given at paragraph 5.3.241.

Other considerations

5.3.189 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.

5.3.190 The guidance in paragraphs 5.3.178 to 5.3.188 should be applied to overseas entities, as appropriate to the firm's assessment of the risk that such entities present.

5.3.191 Many governmental, supranational and state-owned organisations will be managed and controlled by individuals who may qualify as PEPs (see paragraphs 5.5.18 to 5.5.30). Firms need to be aware of the increased likelihood of the existence of such individuals in the case of such customers, and deal with them appropriately, having regard to the risk that the funds of such entities may be used for improper purposes.

Sovereign wealth funds

5.3.192 Sovereign wealth funds (SWFs) are defined[5] as special purpose investment funds or arrangements, owned by the general (i.e., national) government. Created by the general government for macroeconomic purposes, SWFs

[5] International Working Group of Sovereign Wealth Funds *www.iwg-swf.org*

hold, manage, or administer assets to achieve financial objectives, and employ a set of investment strategies which include investing in foreign financial assets.

5.3.193 Typically, SWFs are established from balance of payments surpluses, proceeds raised from privatisations or revenues from natural resources exports. They are managed to meet specific investment objectives, perhaps for a specific future need. Increasingly in recent years, SWFs have looked to employ third party institutions to assist in the management their assets.

5.3.194 Notwithstanding the different forms that SWFs can take, a large proportion of them are participants in the International Working Group of Sovereign Wealth Funds (IWG).

5.3.195 The IWG was established in May 2008 to develop a common set of voluntary principles ("the Santiago Principles") in order to promote a clearer understanding of SWFs through better transparency of their governance and operation. A list of the IWG's member funds, and the counties in which they are established, can be found at Appendix II to the Santiago Principles at: www.iwg-swf.org/pubs/eng/santiagoprinciples.pdf. Further countries, plus the OECD and the World Bank, participate as permanent observers. The International Monetary Fund provides both a co-chair of the IWG and its secretariat.

5.3.196 A general concern exists that SWFs are capable of being used to meet political, rather than purely financial objectives, by acquiring controlling interests in strategically important industries or destabilising economies. For this reason, understanding the nature of purpose of the SWF and the relationship or transaction is a key AML/CTF control and important to the reputation of the firm. Firms should be alert to activities that might give rise to an asset freezing order where UK interests are at stake.

5.3.197 The firm should consider the international reputation of the country and/or SWF concerned (see the Transparency International website www.transparency.org for some helpful resources), before entering into a relationship with the fund. Moreover, financial sanctions may be in force against a country that operates an SWF and must be observed irrespective of whether or not the country is a member of the IWG.

5.3.198 SWFs are unlikely to qualify for simplified due diligence.

Nature and legal form

5.3.199 SWFs are constituted in a variety of ways. Usually, however, they take one of the following forms:

- pool of assets managed by the Ministry of Finance or Central Bank;
- government-owned corporation;
- independent corporation established by statute

This means that CDD must be tailored according to the nature of the SWF. A fundamental feature, however, is that the beneficial owner of a SWF is the government concerned.

Obtain standard evidence

5.3.200 The standard evidence outlined below is founded on an SWF's participation in the IWG and the close involvement with that body of the OECD, IMF and World Bank. Without the comfort of IWG membership, the firm should undertake normal identity verification measures according to the legal form of the SWF.

5.3.201 The following information should be obtained about the identity of the SWF and its officers:

- Full name of the SWF
- Address of the SWF
- Name of the national government
- Names of directors/ trustees (or equivalent)

5.3.202 The objectives in terms of identification are to establish that the SWF exists, that it is owned and controlled by a government and that the individuals with whom the firm has contact in connection with establishing the relationship are bona fide representatives of the fund.

5.3.203 For the purposes of establishing that an SWF exists, reference should normally be made to Appendix II to the Santiago Principles (see paragraph 5.3.195), to confirm that it is represented on the IWG as a full or observer member. Additional steps will be required if the fund is not an IWG member.

5.3.204 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 and take steps to be reasonably satisfied that the person(s) the firm is dealing with is properly authorised by the SWF.

5.3.205 To supplement the measures described in paragraph 5.3.204 and assist with the verification of the individuals that represent the fund, a copy of the constitutional documentation should be obtained, including evidence of its establishment or appointment as an SWF and the authority of those individuals to bind the fund or appoint others to do so. Information in the public domain from reputable and independent sources (e.g., news items, international conference programmes etc.) may also be used as additional evidence of an individual's connection with the fund.

5.3.206 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. Particular care should be exercised if there is a change of government to ensure that the firm is clear as to the individuals authorised to act for the SWF.

Beneficial ownership

5.3.207 SWFs are created to manage the wealth or financial resources at national level so there will be no natural person that has any beneficial interest. The constitutional documents should make this clear.

Nature and purpose

5.3.208 Given the concern that surrounds SWFs (see paragraph 5.3.196), and the fact that those who control them and perhaps the firm's mandate are likely in many cases to be PEPs, the firm needs to consider the nature and purpose of various aspects, including:

- the purpose of the SWF
- the purpose of the relationship with the firm
- the acceptability of any PEPs that may be involved; and
- on an ongoing basis, the reasons for withdrawals from the portfolio

5.3.209 Each firm's processes should take into account any PEP involvement with a SWF, and, on a risk-assessed basis, require a person from senior management and independent from the officer sponsoring the relationship to approve the establishment of the relationship. For higher risk relationships, the firm's compliance (or MLRO) function should also satisfy itself that the risks are acceptable.

5.3.210 The purpose of the SWF should be evident from its constitutional documentation and elsewhere. Note that one of Santiago Principles (GAPP 2) is that the purpose of the fund should be clearly defined and publicly disclosed.

5.3.211 The reasons for using the firm's services need to be understood. For example, investment management mandates are likely to be similar to other institutional mandates and should be questioned if they are unusually focused towards particular sectors, having regard (if appropriate) to the fact that the firm may be managing a specific tranche of the overall fund.

5.3.212 Given the specific nature of SWFs, attention should be given to withdrawals to ensure that the reasons are consistent with the legitimate objectives of the fund and that any payment instructions are appropriate in that context. If the firm has suspicions concerning the motives of the fund, it should make Suspicious Activity Report to SOCA.

5.3.213 Monitoring should be conducted to identify changes to the objectives of the fund and its status in relation to the IWG.

Other considerations

5.3.214 When formulating a risk based approach to SWFs, and particularly when considering those based in countries with higher levels of corruption, firms should take into account the fact that some IWG member funds may not have fully implemented the Santiago Principles and that observers will not necessarily implement them at all and should factor such variations into their additional enquiries.

5.3.215 If a country is not a member of the IWG or does not subscribe to the Santiago Principles, it may be more difficult to obtain information about its constitution and objectives. In these circumstances, the firm must determine what further information, if any, it requires, bearing in mind the need to apply a risk-based approach. For example the firm should understand there may be increased risk that the origins of the fund are

corrupt or the funds' purpose constitutes a potential threat in connection with terrorism or economic manipulation.

Pension schemes

5.3.216 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 register with HMRC in order to achieve tax-exempt status. Most have to register with the Pensions Regulator. Generally, evidence of registration with HMRC or the Pensions Regulator will be sufficient to meet identification and verification obligations in respect of most UK pension schemes.

Regulation 13(7)(c)

5.3.217 In respect of a pension, superannuation or similar scheme which provides retirement benefits for employees, where contributions are made by an employer or by way of deduction from an employee's wages and the scheme rules do not permit the assignment of a member's interest under the scheme [other than in two cases set out in Regulation 13(7)(c)], simplified due diligence may be applied (see section 5.4).

5.3.218 For such a scheme, therefore, the firm need only satisfy itself that the customer qualifies for simplified due diligence in this way.

Regulation 6(5)(b)(ii)

5.3.219 For a scheme that takes the form of a trust, an individual does not qualify as a beneficial owner through having control solely as a result of discretion delegated to him under s 34 of the Pensions Act 1995.

Obtain standard evidence

5.3.220 Where a pension scheme does not meet the criteria in paragraph 5.3.216, and therefore does not qualify for simplified due diligence, but has HMRC or Pensions Regulator registration, a firm's identification and verification obligations may be met by confirming the scheme's registration, as described in paragraph 5.3.216.

5.3.221 Where a firm is unable to confirm the scheme's HMRC or Pension Regulator registration, a pension scheme should be treated for AML/CTF purposes according to its legal form and standard evidence obtained.

Signatories

5.3.222 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.

Other considerations

5.3.223 Following a risk-based approach, the identity of the principal employer may need to be verified in accordance with the guidance given for

companies in paragraphs 5.3.131 to 5.3.162 and the source of funding recorded to ensure that a complete audit trail exists if the employer is wound up.

Payment of benefits

5.3.224 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.)

5.3.225 Where individual members of an occupational pension scheme are to be given personal investment advice, their identities must be verified. However, where the identity of the trustees and principal employer have been satisfactorily verified (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

5.3.226 Charities have their status because of their purposes, and can take a number of legal forms. Some may be companies limited by guarantee, or incorporated by Royal Charter or by Act of Parliament; some may take the form of trusts; others may be unincorporated associations.

5.3.227 If the charity is an incorporated entity (or otherwise has legal personality), firms should verify its identity following the guidance in paragraphs 5.3.131ff. The charity itself is the firm's customer, for practical purposes represented by the trustees who give instruction to the firm.

5.3.228 If the charity takes the form of a trust, it has no legal personality and its trustees have control and management over its affairs. Although those trustees who enter into the business relationship with the firm, in their capacity as trustees of that particular charitable trust, are the firm's customers, where there is a large number of trustees the firm may take a risk-based approach to determining on how many, and which, the firm must carry out full CDD measures; the identities of the other trustees would be verified as beneficial owners. (see paragraphs 5.3.246ff.)

5.3.229 If the charity takes the form of an unincorporated association, it also has no legal personality. Its officers, or members of its governing body, are then the firm's customers, on whom the firm must carry out full CDD measures. (see paragraphs 5.3.270ff.)

5.3.230 Any trustees of a charitable trust who are not the firm's customers will be beneficial owners, because they exercise control over the charity's property. In exceptional cases, another individual may exercise control. Examples include a receiver appointed to manage the affairs of the charity, or a settlor who retains significant powers over the trust property.

5.3.231 For the vast majority of charities, either there will be no individual who is a beneficial owner (apart from the trustees) within the meaning of the ML

Regulations, or at most a class of persons who stand to benefit from the charity's objects must be identified. These persons will be self-evident from a review of the charity's objects in its constitution or the extract from the Register of Charities.

5.3.232 Examples of charities where classes of persons can be identified include charities that relieve poverty, famine or homelessness, educate individuals or alleviate sickness, disability or age. In these cases, a broad description of the class of persons who stand to benefit is sufficient so that the firm understands who the persons are who benefit. Examples of classes might be:

- 'Victims of the Asian Tsunami'
- 'Homeless persons in London'
- 'Deaf and blind people'
- 'Children in the village of Ambridge'

In other charities, no individuals benefit directly from the charity's objects. Examples include charities for the benefit of animals, wildlife or flora, or the conservation or preservation of buildings, habitats or environment.

5.3.233 Neither the Charity Commissioners, nor judges of courts (who may exercise powers over charities) fall within the definition of controllers for these purposes.

Obtain standard evidence

5.3.234 The firm should obtain the following in relation to the charity or church body:

- Full name and address
- Nature of body's activities and objects
- Names of all trustees (or equivalent)
- Names or classes of beneficiaries

5.3.235 The existence of the charity can be verified from a number of different sources, depending on whether the charity is registered or not, a place of worship or an independent school or college.

Registered charities – England and Wales, and Scotland

5.3.236 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.

5.3.237 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 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

5.3.238 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 5.3.138 to 5.3.146, if they are limited by guarantee, and for clubs and societies, those in paragraphs 5.3.270 to 5.3.278. Verification of the charitable status can normally be obtained through HMRC.

Church bodies and places of worship

Charities (exception from Registration) Regulations 1996

Registered Places of Worship Act 1855

5.3.239 Certain church bodies are excepted by law from registering as charities and may not therefore have a registered number. For tax purposes, however, they may notify HMRC of their charitable status; verification of their status may be met by having sight of HMRC's confirmation of the church's application for charitable status. The identity of individual churches may be verified through the headquarters or regional organisation of the denomination, or religion. Places of worship may apply for a certified building of worship from the General Register Office (GRO). Their identity may be verified by reference to a copy of the GRO registration, or examination of the GRO register.

Unregistered charities or church bodies

5.3.240 Other than those covered by paragraph 5.3.239, 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 5.3.149 to 5.3.157, for trusts, as set out in paragraphs 5.3.246 to 5.3.269, or for clubs and societies, as set out in paragraphs 5.3.270 to 5.3.278. 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.

Independent schools and colleges

5.3.241 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 5.3.149 to 5.3.157.

5.3.242 Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer.

Other considerations

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

5.3.244 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.

5.3.245 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 at 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 at www.jmlsg.org.uk.

Other trusts and foundations

5.3.246 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/CTF 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, areas of activity and nature of business being conducted, present.

5.3.247 For trusts or foundations that have no legal personality, those trustees (or equivalent) who enter into the business relationship with the firm, in their capacity as trustees of the particular trust or foundation, are the firm's customers on whom the firm must carry out full CDD measures. Following a risk-based approach, in the case of a large, well known and accountable organisation firms may limit the trustees considered customers to those who give instructions to the firm. Other trustees will be verified as beneficial owners, following the guidance in paragraphs 5.3.11 and 5.3.12.

5.3.248 Most trusts are not separate legal persons, and for AML/CTF purposes should be identified as described in paragraphs 5.3.254 to 5.3.256.

Regulation 6(3), (4)

5.3.249 The beneficial owner of a trust is defined by reference to three categories of individual:

- any individual who is entitled to a specified interest (that is, a vested, not a contingent, interest) in at least 25% of the capital of the trust property
- as respects any trust other than one which is set up or operates entirely for the benefit of individuals with such specified interests, the class of persons in whose main interest the trust is set up or operates
- any individual who has control over the trust.

Regulation 6(4)

5.3.250 The trustees of a trust will be beneficial owners, as they will exercise control over the trust property. In exceptional cases, another individual may exercise control, such as a trust protector, or a settlor who retains significant powers over the trust property.

5.3.251 For the vast majority of trusts, either there will be clearly identified beneficiaries (who are beneficial owners within the meaning of the ML Regulations), or a class of beneficiaries. These persons will be self-evident from a review of the trust's constitution.

5.3.252 In some trusts, no individuals may benefit directly; examples include trusts for the benefit of animals, wildlife or flora, or the conservation or preservation of buildings, habitats or environment.

Regulation 6(6)

5.3.253 In the case of a legal arrangement that is not a trust, the beneficial owner means

- where the individuals who benefit from the entity or arrangement have been determined, any individual who benefits from at least 25% of the property of the entity or arrangement;
- where the individuals who benefit from the entity or arrangement have yet to be determined, the class of persons in whose main interest the entity or arrangement is set up or operates;
- any individual who exercise control over at least 25% of the property of the entity or arrangement.

Obtain standard evidence

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

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

Regulation 4(1)(b)

5.3.255 The identity of the trust must be verified using reliable and independent documents, data or information. This may require sight of relevant extracts from the trust deed, or reference to an appropriate register in the country of establishment. The firm must take measures to understand the ownership and control structure of the customer.

5.3.256 Although those trustees who enter into the business relationship with the firm, in their capacity as trustees of that particular trust, are the firm's customers, where there is a large number of trustees the firm may take a risk-based approach to determining on how many, and which, the firm must carry out full CDD measures; the identities of the other trustees would be verified as beneficial owners. (see paragraphs 5.3.246ff.)

5.3.257 Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer.

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.

Beneficial owners

Regulation 4(1)(b)

5.3.258 The firm must verify the identities of the trustees (or equivalent) as beneficial owners, if not already identified as customers of the firm. The identities of other beneficial owners, either individuals or a class, as appropriate, must also be verified (see paragraphs 5.3.11 and 5.3.12).

5.3.259 Where a trustee is itself a regulated entity (or a nominee company owned and controlled by a regulated entity), or a company listed on a regulated market, or other type of entity, the identification and verification procedures that should be carried out should reflect the standard approach for such an entity.

Other considerations

5.3.260 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.

5.3.261 For situations 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.

5.3.262 Where a situation is assessed as carrying a higher risk of money laundering or terrorist financing, the firm may need to carry out a higher level of verification. Information that might be appropriate to ascertain for higher risk situations includes:

- Donor/settlor/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)

5.3.263 Following its assessment of the money laundering risk presented by the trust, the firm may decide to verify the identity of the settlor(s).

Non-UK trusts and foundations

5.3.264 The guidance in paragraphs 5.3.246 to 5.3.263 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.

5.3.265 A foundation ("Stiftung") is described in the FATF October 2006 *Report*

on the Misuse of Corporate Vehicles as follows:

"A foundation (based on the Roman law *universitas rerum)* is the civil law equivalent to a common law trust in that it may be used for similar purposes. A foundation traditionally requires property dedicated to a particular purpose. Typically the income derived from the principal assets (as opposed to the assets themselves) is used to fulfil the statutory purpose. A foundation is a legal entity and as such may engage in and conduct business. A foundation is controlled by a board of directors and has no owners. In most jurisdictions a foundation's purpose must be public. However there are jurisdictions in which foundations may be created for private purposes. Normally, foundations are highly regulated and transparent."

5.3.266 Foundations feature in a number of EEA member state and other civil law jurisdictions including, notably, Liechtenstein and Panama. The term is also used in the UK and USA in a looser sense, usually to refer to a charitable organisation of some sort.

5.3.267 The nature of a civil law foundation should normally be well understood by firms, or their subsidiaries or branches, operating in the jurisdiction under whose laws the foundation has been set up. Where a foundation seeks banking or other financial services outside its home jurisdiction, firms will need to be satisfied that there are legitimate reasons for doing so and to establish the statutory requirements within the specific home jurisdiction for setting up a foundation. So far as possible, comparable information should be obtained as indicated in paragraph 5.3.254 for trusts, including the identity of the founder and beneficiaries (who may include the founder), whose identity should be verified as necessary on similar risk-based principles.

5.3.268 Where the founder's identity is withheld, firms will need to exercise caution and have regard to the standing of any intermediary and the extent of assurances that may be obtained from them to disclose information on any parties concerned with the foundation in response to judicial demand in the firm's own jurisdiction. Liechtenstein foundations, for example, are generally established on a fiduciary basis through a licensed trust company to preserve the anonymity of the founder, but the trust companies are themselves subject to AML laws.

5.3.269 Whilst firms may conclude on the basis of their due diligence that the request for facilities is acceptable, they should bear in mind that terms like 'foundation', 'stiftung', 'anstalt' are liable to be hijacked by prime bank instrument fraudsters to add spurious credibility to bogus investment schemes.

Clubs and societies

5.3.270 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.

5.3.271 For the vast majority of clubs and societies, either there will be no individual who is a beneficial owner within the meaning of the ML Regulations, or at most a class of persons who stand to benefit from the club or society's objects must be identified. These persons will be self-evident from a review of the club or society's objects in its constitution.

Obtain standard evidence

5.3.272 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

5.3.273 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.

5.3.274 Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer.

5.3.275 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.

Other considerations

5.3.276 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 5.3.92 to 5.3.96 should be followed. This does not obviate the need to verify the identity of beneficial owners, where these exist.

5.3.277 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.

5.3.278 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 section 5.7).

5.4 Simplified due diligence

Regulation 13(1) and 7(3)(b)

5.4.1 Simplified due diligence means not having to apply CDD measures. In practice, this means not having to verify the customer's identity, or, where relevant, that of a beneficial owner, nor having to obtain information on the purpose or intended nature of the business relationship. It is, however, still necessary to conduct ongoing monitoring of the business relationship. Firms must have reasonable grounds for believing that the customer, transaction or product relating to such transaction falls within one of the categories set out in the Regulations, and may have to demonstrate this to their supervisory authority. Clearly, for operating purposes, the firm will nevertheless need to maintain a base of information about the customer.

Regulation 13

5.4.2 Simplified due diligence may be applied to::

(i) certain other regulated firms in the financial sector (see paragraph 5.3.122)
(ii) companies listed on a regulated market (see paragraph 5.3.142)
(iii) beneficial owners of pooled accounts held by notaries or independent legal professionals (see paragraph 5.3.130)
(iv) UK public authorities (see paragraph 5.3.179)
(v) Community institutions (see paragraph 5.3.180)
(vi) certain life assurance and e-money products (see Part II, sectors 7 and 3)
(vii) certain pension funds (see paragraphs 5.4.4 and 5.3.216ff)
(viii) certain low risk products (see paragraph 5.4.5)
(ix) Child Trust Funds and Junior ISAs (see paragraphs 5.4.6 - 5.4.8)

Regulation 7(1) (c) (d)

5.4.3 There is no exemption from the obligation to verify identity where the firm knows or suspects that a proposed relationship or occasional transaction involves money laundering or terrorist financing, or where there are doubts about the veracity or accuracy of documents, data or information previously obtained for the purposes of customer verification.

Regulation 13(7)(c)

5.4.4 Simplified due diligence may be applied to pension, superannuation or similar schemes which provide retirement benefits to employees, where contributions are made by an employer or by way of deduction from an employee's wages and the scheme rules do not permit the assignment of a member's interest under the scheme.

Regulation13(8) and Schedule 2,paragraph 3

5.4.5 Simplified due diligence may be applied to low risk products which meet specified criteria set out in the ML Regulations. These criteria, which are cumulative, are:

(i) the product has a written contractual base;

(ii) any related transactions are carried out through an account of the customer with a bank which is subject to the money laundering directive, or a bank in an equivalent jurisdiction;

(iii) the product or related transaction is not anonymous and its nature is such that it allows for the timely application of CDD measures where there is a suspicion of money laundering or terrorist financing;

(iv) the product is within the following maximum threshold:

a. in the case of insurance policies or savings products of a similar nature, the annual premium is no more than €1,000 or there is a single premium of no more than €2,500;
b. in the case of products which are related to the financing of physical assets where the legal and beneficial title of the assets is not transferred to the customer until the termination of the contractual relationship (whether the transaction is carried out in a single operation or in several operations which appear to be linked) the annual payments do not exceed €15,000;
c. in all other cases, the maximum threshold is €15,000.

(v) the benefits of the product or related transaction cannot be realised for the benefit of third parties, except in the case of death, disablement, survival to a predetermined advanced age, or similar events;

(vi) in the case of products or related transactions allowing for the investment of funds in financial assets or claims, including insurance or other kinds of contingent claims:

a. the benefits of the product or related transaction are only realisable in the long term;
b. the product or related transaction cannot be used as collateral;
c. during the contractual relationship, no accelerated payments are made, surrender clauses used or early termination takes place.

Regulation 13(8), (9), (10)

5.4.6 Firms need to decide whether particular products meet the criteria for simplified due diligence. In respect of Child Trust Funds and Junior ISAs, no CDD measures need be carried out. Other products in respect of which no CDD measures need be carried out may be designated from time to time by HM Treasury, by amendment of the ML Regulations.

5.4.7 In respect of Junior ISAs, simplified due diligence may be applied. Firms will, however, in due course need to verify identity at the point the child reaches 18 years and becomes entitled to the funds, or at the next 'trigger' event thereafter (unless the child's identity has by then already been verified for the purposes of some other relationship).

5.4.8 With Junior ISAs, the child is able to manage the account from the age of 16, in which case the firm might choose to undertake customer due diligence at that stage in order to avoid delaying any transaction the child should wish to undertake on reaching 18, when the account becomes a 'full' ISA. It is recommended that firms indicate in their product literature etc. what their policy will be when, for example, the child reaches 16 or 18.

Regulations 5 and 8
POCA s330 (2)(b)
Terrorism Act s 21A

5.4.9 An exemption from the basic verification obligation does not extend to the obligation to conduct ongoing monitoring of the business relationship, or to the duty to report knowledge or suspicion of money laundering or terrorist financing.

5.5 Enhanced due diligence

Regulation 14 (1)

5.5.1 A firm must apply EDD measures on a risk-sensitive basis in any situation which by its nature can present a higher risk of money laundering or terrorist financing. As part of this, a firm may conclude, under its risk-based approach, that the information it has collected as part of the customer due diligence process (see section 5.3) is insufficient in relation to the money laundering or terrorist financing risk, and that it must obtain additional information about a particular customer, the customer's beneficial owner, where applicable, and the purpose and intended nature of the business relationship.

5.5.2 As a part of a risk-based approach, therefore, firms should hold sufficient information about the circumstances and business of their customers and, where applicable, their customers' beneficial owners, 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.

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

5.5.4 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.

5.5.5 A firm should hold a fuller set of information in respect of those business relationships it assessed as carrying a higher money laundering or terrorist financing risk, or where the customer is seeking a product or service that carries a higher risk of being used for money laundering or terrorist financing purposes.

5.5.6 When someone becomes a new customer, or applies for a new product or service, or where there are indications that the risk associated with an existing business relationship might have increased, the firm should, depending on the nature of the product or service for which they are applying, request information as to the customer's residential status, employment details, income, and other sources of income, in order to decide whether to accept the application or continue with the relationship. The firm should also consider whether or not there is a need to enhance its activity monitoring in respect of the relationship. A firm should have a clear policy regarding the escalation of decisions to senior management concerning the acceptance or continuation of high-risk business relationships.

5.5.7 The availability and use of other financial information held is important for reducing the additional costs of collecting customer due diligence information and can help increase a firm's understanding of the risk associated with the business relationship. Where appropriate and practical, therefore, and where there are no data protection restrictions, firms should take reasonable steps to ensure that where they have customer due diligence information in one part of the business, they are able to link it to information in another.

5.5.8 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.

Regulation 14

5.5.9 The ML Regulations prescribe three specific types of relationship in respect of which EDD measures must be applied. These are:

- where the customer has not been physically present for identification purposes (see paragraphs 5.5.10ff);
- in respect of a correspondent banking relationship (see Part II, sector 16: *Correspondent banking*);
- in respect of a business relationship or occasional transaction with a PEP (see paragraphs 5.5.18ff).

Non face-to-face identification and verification

5.5.10 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.

5.5.11 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.

Regulation 14(2)

5.5.12 Where the customer has not been physically present for identification purposes, a firm must take specific and adequate measures to compensate for the higher risk, for example by applying one or more of the following measures:

(a) ensuring that the customer's identity is established by additional documents, data or information;
(b) supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a financial services firm in the UK, EU or an equivalent jurisdiction;
(c) ensuring that the first payment of the operation is carried out through an account opened in the customer's name with a bank.

5.5.13 Further guidance on the measures that should be applied to non face-to-face customers in different industry sectors is given in Part II of this Guidance.

5.5.14 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.

5.5.15 Additional measures would also 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.

5.5.16 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 5.3.79 -5.3.81), or by reference to documents (see paragraphs 5.3.72 – 5.3.78).

5.5.17 Non face-to-face identification and verification carries an inherent risk of impersonation fraud, and firms should follow the guidance in paragraph 5.3.82 to mitigate this risk.

Politically exposed persons (PEPs)

5.5.18 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 may make 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 does, however, put the customer, or the beneficial owner, into a higher risk category.

Regulation 14(4), (5), (6)

5.5.19 A PEP is defined as "an individual who is or has, at any time in the preceding year, been entrusted with prominent public functions and an immediate family member, or a known close associate, of such a person". This definition only applies to those holding such a position in a state outside the UK, or in a Community institution or an international body.

5.5.20 Although under the definition of a PEP an individual ceases to be so regarded after he has left office for one year, firms are encouraged to apply a risk-based approach in determining whether they should cease carrying out appropriately enhanced monitoring of his transactions or activity at the end of this period. In many cases, a longer period might be appropriate, in order to ensure that the higher risks associated with the individual's previous position have adequately abated.

Regulation, Sch, 2, paras 4 (1)(a),(b) and (c)

5.5.21 Public functions exercised at levels lower than national should normally not be considered prominent. However, when their political exposure is comparable to that of similar positions at national level, for example, a senior official at state level in a federal system, firms should consider, on a risk-based approach, whether persons exercising those public functions should be considered as PEPs. Prominent public functions include:

- heads of state, heads of government, ministers and deputy or assistant ministers;
- members of parliaments;
- members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not generally subject to further appeal, except in exceptional circumstances;
- members of courts of auditors or of the boards of central banks;
- ambassadors, charges d'affaires and high-ranking officers in the armed forces; and (other than in respect of relevant positions at Community and international level)
- members of the administrative, management or supervisory boards of State-owned enterprises.

These categories do not include middle-ranking or more junior officials.

Regulation Sch 2, paras 4(1)(d) and (2)

5.5.22 Immediate family members include:

- a spouse;
- a partner (including a person who is considered by his national law as equivalent to a spouse);
- children and their spouses or partners; and
- parents.

Regulation Sch 2, para 4(1)(e)

5.5.23 Persons known to be close associates include:

- any individual who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with a person who is a PEP; and
- any individual who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of a person who is a PEP.

Regulation 14(6)and

5.5.24 For the purpose of deciding whether a person is a known close associate of

20(2)(c)

a PEP, the firm need only have regard to any information which is in its possession, or which is publicly known. Having to obtain knowledge of such a relationship does not presuppose an active research by the firm.

Regulation 14(4)

5.5.25 Firms are required, 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 a business relationship with such a customer;
- take adequate measures to establish the source of wealth and source of funds which are involved in the business relationship or occasional transaction; and
- conduct enhanced ongoing monitoring of the business relationship.

Risk-based procedures

5.5.26 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 or not the firm needs to screen all customers for this purpose. In the context of this risk analysis, it would be appropriate if the firm's resources were focused in particular on products and transactions that are characterised by a high risk of money laundering.

5.5.27 Establishing whether individuals 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. The IMF, World Bank and some non-governmental organisations also publish relevant reports. 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 an adequate risk mitigation tool.

Regulation 14(4)(b)

5.5.28 It is for each firm to decide the steps it takes to determine whether a PEP is seeking to establish a business relationship for legitimate reasons. Firms should, in any case, take adequate and meaningful measures to establish the source of funds and source of wealth. Firms may wish to refer to information sources such as asset and income declarations, which some jurisdictions expect certain senior public officials to file and which often include information about an official's source of wealth and current business interests. Firms should note that not all declarations are publicly available and that a PEP customer may have legitimate reasons for not providing a copy. Firms should also be aware that some jurisdictions impose restrictions on their PEPs' ability to hold foreign bank accounts or to hold other office or paid employment.

Senior management approval

5.5.29 Obtaining approval from senior management for establishing a business relationship does not necessarily mean obtaining approval from the Board

of directors (or equivalent body), but from a higher level of authority from the person seeking such approval. As risk dictates, firms should escalate decisions to more senior management levels.

On-going monitoring

5.5.30 Guidance on the on-going monitoring of the business relationship is given in section 5.7. Firms should remember that new and existing customers may not initially meet the definition of a PEP, but may subsequently become one during the course of a business relationship. 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. When an existing customer is identified as a PEP, EDD must be applied to that customer.

5.6 Multipartite relationships, including reliance on third parties

5.6.1 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.

5.6.2 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/CTF obligations, and as to the extent to which it can rely upon or otherwise 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.

5.6.3 In other cases, a customer may be an existing customer of another regulated firm in the same group. Guidance on meeting AML/CTF obligations in such a relationship is given in paragraphs 5.6.26 to 5.6.29.

Reliance on third parties

Regulation 17

5.6.4 The ML Regulations expressly permit a firm to rely on another person to apply any or all of the CDD measures, provided that the other person is listed in Regulation 17(2), and that consent to being relied on has been given (see paragraph 5.6.8). The relying firm, however, retains responsibility for any failure to comply with a requirement of the Regulations, as this responsibility cannot be delegated.

5.6.5 For example:

- where a firm (firm A) enters into a business relationship with, or undertakes an occasional transaction for, the underlying customer of another firm (firm B), for example by accepting instructions from the customer (given through Firm B); or
- firm A and firm B both act for the same customer in respect of a transaction (e.g., firm A as executing broker and firm B as clearing broker),

firm A may rely on firm B to carry out CDD measures, while remaining ultimately liable for compliance with the ML Regulations.

Regulation 17(2)(a),(b) and (5)

5.6.6 In this context, Firm B must be:

(1) a person who carries on business in the UK who is
  (a) an FSA-authorised credit or financial institution (excluding a money service business) (see also paragraph 5.6.7 below); or
  (b) an auditor, insolvency practitioner, external accountant, tax adviser or independent legal professional, who is supervised for the purposes of the Regulations by one of the bodies listed in Part 1 of Schedule 3 to the ML Regulations;

Regulation 17(2)(c) and (5)

(2) a person who carries on business in another EEA State who is:
  (a) a credit or financial institution (excluding a money service business), an auditor, insolvency practitioner, external accountant, tax adviser or other independent legal professional;
  (b) subject to mandatory professional registration recognised by law; and
  (c) supervised for compliance with the requirements laid down in the Money Laundering Directive in accordance with section 2 of Chapter V of that directive;

Regulation 17(2)(d) and (5)

(3) a person carrying on business in a non-EEA State who is
  (a) a credit or financial institution (excluding a money service business), an auditor, insolvency practitioner, external accountant, tax adviser or other independent legal professional;
  (b) subject to mandatory professional registration recognised by law; and
  (c) subject to requirements equivalent to those laid down in the Money Laundering Directive; and
  (d) supervised for compliance with those requirements in a manner equivalent to section 2 of Chapter V of the Money Laundering Directive.

5.6.7 In practice, appointed representatives of FSA-authorised credit or financial institutions (see sub-paragraph (1)(a) above) may be regarded as extensions of their FSA-authorised principal firms, and reliance may be placed upon them accordingly for the purposes of Regulation 17.

Consent to be relied upon

5.6.8 The ML Regulations do not define how consent must be evidenced. Ordinarily, 'consent' means an acceptance of some form of proposal by one party from another – this may be written or oral, express or implied.

Written acknowledgement that a firm is being relied on makes its relationship with the firm relying on it clear. On the other hand, it is not necessary for a firm to give an express indication that it is being relied on, and it may be inferred from their conduct; for example - dealing with a firm after receipt of that firm's terms of business which indicate reliance; silence where it has been indicated that this would be taken as acknowledgement of reliance; participation in a tri-partite arrangement, based on a market practice that has reliance as an integral part of its framework.

5.6.9 In order to satisfy the purpose behind Regulation 17(1)(a), a firm may wish to consider providing a firm being relied on with notification of the reliance. The notification should specify that the firm intends to rely on the third party firm for the purposes of Regulation 17(1)(a). Such a notification can be delivered in a number of ways. For example, where one firm is introducing a client to another firm, the issue of reliance can be raised during the introduction process, and may form part of the formal agreement with the intermediary. Similarly, where the relying and relied upon firms are party to tripartite agreement with a client, the notification may be communicated during exchange of documents. Where a relationship exists between the parties it is likely that such a notification plus some form of acceptance (see paragraph 5.6.8) should be sufficient for the purposes of establishing consent.

5.6.10 Where there is no contractual or commercial relationship between the relying and relied on firms it is less likely that consent can be assumed from the silence of the firm being relied on. In such circumstances firms may wish to seek an express agreement to reliance. This does not need to take the form of a legal agreement and a simple indication of consent (e.g., by e-mail) should suffice.

Basis of reliance

5.6.11 For one firm to rely on verification carried out by another firm, the verification that the firm being relied upon has carried out must have been based at least on the standard level of customer verification. It is not permissible to rely on SDD carried out, or any other exceptional form of verification, such as the use of source of funds as evidence of identity.

5.6.12 Firms may also only rely on verification actually carried out by the firm being relied upon. A firm that has been relied on to verify a customer's identity may not 'pass on' verification carried out for it by another firm.

Regulation 2(9), Schedule 1

5.6.13 Under the ML Regulations, the FSA has been given the additional responsibility for supervising the AML/CTF systems and controls in Annex I Financial Institutions. Such businesses are not authorised by the FSA, may not therefore be relied on to carry out CDD measures on behalf of other firms until such time as this is permitted under the ML Regulations.

5.6.14 Whether a firm wishes to place reliance on a third party will be part of the firm's risk-based assessment, which, in addition to confirming the third party's regulated status, may include consideration of matters such as:

- its public disciplinary record, 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 other firm'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 firm to be relied upon.

5.6.15 The assessment as to whether or not a firm should accept confirmation from a third party that appropriate CDD measures have been carried out on a customer will be risk-based, and cannot be based simply on a single factor.

5.6.16 In practice, the firm relying on the confirmation of a third party needs to know:

- the identity of the customer or beneficial owner whose identity is being verified;
- the level of CDD that has been carried out; and
- confirmation of the third party's understanding of his obligation to make available, on request, copies of the verification data, documents or other information.

In order to standardise the process of firms confirming to one another that appropriate CDD measures have been carried out on customers, guidance is given in paragraphs 5.6.30 to 5.6.33 below on the use of pro-forma confirmations containing the above information.

5.6.17 The third party 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 does not wish to rely upon the third party, then the firm must carry out its own CDD measures on the customer.

5.6.18 For a firm to confirm that it has carried out CDD measures in respect of a customer is a serious matter. A firm must not give a confirmation on the basis of a generalised assumption that the firm's systems have operated effectively. There has to be awareness that the appropriate steps have in fact been taken in respect of the customer that is the subject of the confirmation.

Regulation 19(5)

5.6.19 A firm which carries on business in the UK and is relied on by another person must, within the period of five years beginning on the date on which it is relied on, if requested by the firm relying on it

- as soon as reasonably practicable make available to the firm which is relying on it any information about the customer (and any beneficial owner) which the third party obtained when applying CDD measures; and
- as soon as reasonably practicable forward to the firm which is relying on it relevant copies of any identification and verification data and other relevant documents on the identity of the customer (and any beneficial owner) which the third party obtained when applying those measures

Regulation 19(6)

5.6.20 A firm which relies on a firm situated outside the UK to apply CDD

measures must take steps to ensure that the firm on which it relies will, within the period of five years beginning on the date on which the third party is relied on, if requested, comply with the obligations set out in paragraph 5.6.19.

5.6.21 The personal information supplied by the customer as part of a third party's customer identification procedures will generally be set out in the form that the relying firm will require to be completed, and this information will therefore be provided to that firm.

Regulation 19 (4), (5) and (6)

5.6.22 A request to forward copies of any identification and verification data and other relevant documents on the identity of the customer or beneficial owner obtained when applying CDD measures, if made, would normally be as part of a firm's risk-based customer acceptance procedures. However, the firm giving the confirmation must be prepared to provide these data or other relevant documents throughout the five year period for which it has an obligation under the Regulations to retain them.

5.6.23 Where a firm makes such a request, and it is not met, the firm will need to take account of that fact in its assessment of the third party in question, and of the ability to rely on the third party in the future.

5.6.24 A firm must also document the steps taken to confirm that the firm relied upon satisfies the requirements in Regulation 17(2). This is particularly important where the firm relied upon is situated outside the EEA.

5.6.25 Part of the firm's AML/CTF policy statement should address the circumstances where reliance may be placed on other firms and how the firm will assess whether the other firm satisfies the definition of third party in Regulation 17(2) (see paragraph 5.6.6).

Group introductions

5.6.26 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.

5.6.27 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/CTF standards in the UK, the EU or an equivalent jurisdiction; and
- the group entity that carried out the CDD measures can be relied upon as a third party under Regulation 17(2).

5.6.28 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, on request, from the UK.

5.6.29 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/CTF

standards in the EU, or in an equivalent 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 17 (2)

5.6.30 Whilst a firm may be able to place reliance on another party to apply all or part of the CDD measures under Regulation 17(2) (see paragraph 5.6.4), it may still wish to receive, as part of its risk-based procedures, a written confirmation from the third party, not least to evidence consent. This may also be the case, for example, when a firm is unlikely to have an ongoing relationship with the third party. Confirmations can be particularly helpful when dealing with third parties located outside of the UK, where it is necessary to confirm that the relevant records will be available (see 5.6.19).

5.6.31 The provision of a confirmation certificate implies consent to be relied upon, in accordance with paragraph 5.6.7.

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

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

Situations which are not reliance

(i) One firm acting solely as introducer

5.6.34 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.*

5.6.35 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 (see paragraphs 5.6.36 – 5.6.37).

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

5.6.36 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.

5.6.37 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.

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

5.6.38 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 an equivalent 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 "equivalent jurisdictions" is given at www.jmlsg.org.uk.

Regulation 13(2)

5.6.39 Depending on jurisdiction, where the customer is an intermediary carrying on appropriately regulated business, and is acting on behalf of another, there is no obligation on the product provider to carry out CDD measures on the customer, or on the underlying party (see paragraph 5.3.203).

5.6.40 Where a firm cannot apply simplified due diligence to the intermediary (see paragraphs 5.4.1ff), the product/service provider is obliged to carry out CDD measures on the intermediary and, as the intermediary acts for another, on the underlying customer.

5.6.41 Where the firm takes instruction from the underlying customer, or where the firm acts on the underlying customer's behalf (e.g., as a custodian) the firm then has an obligation to carry out CDD measures in respect of that customer, although the reliance provisions (see paragraphs 5.6.4ff) may be applied.

5.6.42 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/CTF 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.

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

5.7 Monitoring customer activity

The requirement to monitor customers' activities

Regulation 8

5.7.1 Firms must conduct ongoing monitoring of the business relationship with their customers. Ongoing monitoring of a business relationship includes:

- Scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the firm's knowledge of the customer, his business and risk profile;
- Ensuring that the documents, data or information held by the firm are kept up to date.

5.7.2 Monitoring customer activity helps identify unusual activity. If unusual activities cannot be rationally explained, they may involve money laundering or terrorist financing. Monitoring customer activity and transactions that take place throughout a relationship helps firms know their customers, assist them to assess risk and provides greater assurance that the firm is not being used for the purposes of financial crime.

What is monitoring?

5.7.3 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.

5.7.4 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.

5.7.5 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.

5.7.6 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.

5.7.7 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.

5.7.8 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

5.7.9 Some financial services business typically involves transactions with customers about whom the firm 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 firm 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.

5.7.10 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.

5.7.11 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.

Regulation 14(1)

5.7.12 Higher risk accounts and customer relationships require enhanced ongoing monitoring. This will generally mean more frequent or intensive monitoring.

Manual or automated?

5.7.13 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.

5.7.14 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).

5.7.15 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.

5.7.16 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.

5.7.17 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.

5.7.18 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?

5.7.19 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.

5.7.20 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.

5.7.21 Monitoring also involves keeping information held about customers up to date, as far as reasonably possible. Guidance on this is given at paragraphs 5.3.23 - 5.3.24.

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 who have been subject to Simplified Due Diligence under the Money Laundering Regulations; or
   - those whose identity has been verified using the source of funds as evidence.

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 you (or from UK law enforcement agencies or regulators under court order or relevant mutual assistance procedure), copies of the relevant customer records will be made available, 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.

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 equivalent 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 you (or from UK law enforcement agencies or regulators under court order or relevant mutual assistance procedure), copies of the relevant customer records will be made available, 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.

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%)	

*** And dates of birth, if known**

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 who have been subject to Simplified Due Diligence under the Money Laundering Regulations; or
   - those whose identity has been verified using the source of funds as evidence.

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%)	

*** And dates of birth, if known**

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 you (or from UK law enforcement agencies or regulators under court order or relevant mutual assistance procedure), copies of the relevant customer records will be made available, 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.

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 equivalent 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%)	

*** And dates of birth, if known**

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 you (or from UK law enforcement agencies or regulators under court order or relevant mutual assistance procedure), copies of the relevant customer records will be made available, 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.

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 2007, 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 you (or from UK law enforcement agencies or regulators under court order or relevant mutual assistance procedure), copies of the relevant customer records will be made available, 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.

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%)	

*** And dates of birth, if known**

2 CONFIRMATION

We confirm that

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

(i) of the Money Laundering Regulations 2007, 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 you (or from UK law enforcement agencies or regulators under court order or relevant mutual assistance procedure), copies of the relevant customer records will be made available, 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

- "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.

CHAPTER 6

SUSPICIOUS ACTIVITIES, REPORTING AND DATA PROTECTION

- **Relevant law/regulation**
  - Regulations 20(1)(b) and (2)(d) and 21
  - POCA ss327-340
  - SI2006/1070 (Exceptions to overseas conduct defence)
  - Terrorism Act, ss21, 39
  - 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 Serious Organised Crime Agency (SOCA) 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 SOCA 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 HM Treasury website of suspected terrorists or sanctioned individuals and entities, and make an external report to HM Treasury
  - It is a criminal offence for anyone, following a disclosure to a nominated officer or to SOCA, 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 SOCA, 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

POCA ss 330, 331
Terrorism Act s 21A

6.1 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, or attempting, money laundering or terrorist financing. Within this guidance, the above obligations are collectively referred to as "grounds for knowledge or suspicion".

Regulation 20(2)(d)
POCA s 330

6.2 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, or attempting, money laundering or terrorist financing;

Regulation 21

- 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.

POCA, s 331
Terrorism Act s 21A

6.3 If the nominated officer determines that a report does give rise to grounds for knowledge or suspicion, he must report the matter to SOCA. Under POCA, the nominated officer is required to make a report to SOCA 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.

6.4 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, or attempting, money laundering or terrorist financing, must make a report promptly to SOCA.

POCA ss 333A -334
Terrorism Act ss 21D-H, 39

6.5 It is a criminal offence for any person, following a disclosure to a nominated officer or to SOCA, to release information that might 'tip off' another person that a disclosure has been made if the disclosure is likely to prejudice an investigation, if the information released came to that person in the course of a business in the UK regulated sector. It is also an offence for a person to disclose that an investigation into allegations that an offence has been committed is being contemplated or is being carried out; the disclosure is likely to prejudice that investigation and the information on which the disclosure is based came to the person in the course of a business in the regulated sector. It is also an offence for a person to disclose to another anything which is likely to prejudice an investigation resulting from a disclosure, or where the person knows or has reasonable cause to suspect that a disclosure has been or will be made.

Financial sanctions legislation

6.6 It is a criminal offence to make funds, economic resources or, in certain circumstances, financial services available to those persons or entities listed as the targets of financial sanctions legislation. There is also a requirement to report to HM Treasury 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 or entity, a person acting on behalf of a listed person or entity or has committed an offence under the sanctions legislation.

Attempted offences

POCA, s 330

Terrorism Act s21A(2)

6.7 POCA and the Terrorism Act provide that a disclosure must be made where there are grounds for suspicion that a person is engaged in money laundering or terrorist financing. "Money laundering" is defined in POCA to include an attempt to commit an offence under s327-329 of POCA. Similarly, under the Terrorism Act a disclosure must be made where a person has knowledge or suspicion that 'another person had committed *or attempted to commit* an offence under any of the sections 15-18'. There is no duty under s330 of POCA or s21A of the Terrorism Act 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 those Acts.

6.8 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 or terrorist property in existence, then, subject to paragraph 6.9, knowledge or suspicion of money laundering or terrorist financing must be reported to SOCA (see paragraphs 6.40ff). 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)

6.9 In circumstances where neither the identity of the fraudster, nor the location of any related criminal property, is known nor is likely to be discovered, limited useable information is, however, available for disclosure. An example of such circumstances would be the theft of a chequebook, 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 SOCA 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.

Cases which do not meet all of the above criteria may be eligible for reporting by means of a Limited Intelligence Value (LIV) report. Guidance as to when the use of this format may be appropriate and the report form itself is available at www.soca.gov.uk/downloads/LIVGuidance.pdf.

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

POCA, s 330 (2),(3), s 331 (2), (3)
Terrorism Act ss21A, 21ZA, 21ZB

6.10 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 s 330 of POCA or s 21A 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.

6.11 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."*

6.12 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.

6.13 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.

6.14 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), s 331 (2)(b) Terrorism Act s 21A

6.15 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.

6.16 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.

6.17 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 20(2)(d)(ii)
POCA s 330(5)

6.18 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.

6.19 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 POCA 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.

6.20 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.

6.21 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.

6.22 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.

6.23 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.

6.24 Until the nominated officer advises the member of staff making an internal report that no report to SOCA 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

6.25 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. This broad scope excludes offences (other than those referred to in paragraph 6.26) 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.

SI 2006/1070
1968 c 65
1976 c 32
2000 c 8

6.26 Offences committed overseas which the Secretary of State has prescribed by order as remaining within the scope of the duty to report under POCA are those which are punishable by imprisonment for a maximum term in excess of 12 months in any part of the United Kingdom if they occurred there, other than:

- an offence under the Gaming Act 1968;
- an offence under the Lotteries and Amusements Act 1976; or
- an offence under ss 23 or 25 of FSMA

Terrorism Act s21A(11)

6.27 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 ss 15-18 of that Act, that would have been an offence under these sections of the Act had it occurred in the UK.

POCA s 331
POCA ss 327-329
Terrorism Act s 21A

6.28 The obligation to consider reporting to SOCA 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 20(2)(d)

6.29 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 SOCA may be being considered.

6.30 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 SOCA, 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.

6.31 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 SOCA prior to completing a full review of linked or connected relationships, which may or may not subsequently need to be reported to SOCA.

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

External reporting

Regulation 20(2)(d)
POCA, s 331
Terrorism Act, s 21A

6.33 The firm's nominated officer must report to SOCA 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, or to attempted 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

6.34 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. Although a consultation paper on the form and manner of reporting was issued by the Home Office in the summer of 2007, the Home Office decided, on a recommendation from SOCA, not to proceed with the introduction of such an order.

6.35 SOCA prefers that SARs are submitted electronically via the secure internet system SARs Online. Information about access to and guidance on the use of SARs Online can be found at. www.ukciu.gov.uk/(nrajwkjokzajrk3t3e0g41rw)/saronline.aspx.

6.36 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.

6.37 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.

6.38 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. SOCA's website (www.soca.gov.uk) contains guidance on completing SARs in a way that gives most assistance to law enforcement. In particular, SOCA has published a glossary of terms, and find it helpful if firms use these terms when completing a SAR.

Financial sanctions legislation

6.39 Firms must report to HM Treasury 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 entity, or a person acting on behalf of a listed person or entity. 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

6.40 To avoid committing a failure to report offence, nominated officers must make their disclosures to SOCA. The national reception point for disclosure of suspicions, and for seeking consent to continue to proceed with the transaction or activity, is the UKFIU within SOCA

6.41 The UKFIU address is PO Box 8000, London, SE11 5EN and it 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, if secure electronic methods are not available, by fax, as specified on the SOCA website at www.soca.gov.uk. Speed of response is assisted if the appropriate consent request is clearly mentioned in the title of any faxed report (www.ukciu.gov.uk/(nrajwkjokzajrk3t3e0g41rw)/saronline.aspx).

6.42 To avoid committing a failure to report offence under financial sanctions legislation, firms must make their reports to HM Treasury. The relevant unit is the Asset Freezing Unit, HM Treasury, 1 Horse Guards Road, London SW1A 2HQ. Reports can be submitted electronically at assetfreezingunit@hm-treasury.gov.uk and the Unit can be contacted by telephone on 020 7270 5454.

Sanctions and penalties

POCA s334
Terrorism Act s21A

6.43 Where a person fails to comply with the obligation under POCA or the Terrorism Act to make disclosures to a nominated officer and/or SOCA 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

6.44 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 entities or to report knowledge or suspicion, it is open to prosecution.

Consent

6.45 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

6.46 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 SOCA 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 SOCA gives consent. Where urgent consent is required, use should be made of the process referred to in paragraph 6.41 above.

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

6.47 When a 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.

6.48 When consent is needed to undertake a future transaction or activity, or to enter into an arrangement, the disclosure should be sent electronically (ensuring that the tick box for a consent request is marked) or, if electronic methods are not available, faxed to the SOCA UKFIU Consent Desk immediately the suspicion is identified. Consent requests should not be sent by post due to the timings involved, and additional postal copies are not required following submission by electronic means or fax. Further information is available on the SOCA website www.soca.gov.uk. The Consent Desk will apply SOCA policy to each submission, carrying out the necessary internal enquiries, and will contact the appropriate law enforcement agency, where necessary, for a consent recommendation. Once SOCA's 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

6.49 In the event that SOCA 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)

6.50 Consent from SOCA (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.

Consent under Terrorism Act

Terrorism Act s21ZA

6.51 A person does not commit an offence under the Terrorism Act where, before becoming involved in a transaction or arrangement relating to money or other property which he suspects or believes is terrorist property, a report is made to SOCA and consent sought to proceed with that transaction or arrangement. In such circumstances, it is an offence for an authorised officer to consent to a transaction or arrangement going ahead within the seven working day notice period from the working day following the date of disclosure to SOCA, unless SOCA gives consent. [Where urgent consent is required, use should be made of the process referred to in paragraph 6.41 above.]

Terrorism Act s21ZB

6.52 When a 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 authorised 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, the Terrorism Act provides a defence from making a report where there is a reasonable excuse for not doing so, so long as the report is made on his own initiative and as soon as it is reasonably practical for the person to make it. 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.

6.53 When consent is needed to undertake a future transaction or activity, or to enter into an arrangement, the disclosure should be sent electronically (ensuring that the tick box for a consent request is marked) or, if secure electronic methods are not available, faxed to the SOCA UKFIU Consent Desk immediately the suspicion is identified. Consent requests should not be sent by post due to the timings involved, and additional postal copies are not required following submission by electronic means or fax. Further information is available on the SOCA website www.soca.gov.uk. The Consent Desk will carry out the necessary internal enquiries, and will

contact the appropriate law enforcement agency, where necessary, for a consent recommendation. Once SOCA's 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.

Terrorism Act s21ZA(2)

6.54 In the event that SOCA does not refuse consent within seven working days following the working day after the disclosure is made, the firm may proceed with the transaction or arrangement, subject to normal commercial considerations. 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.

Terrorism Act S21ZA(1)-(3)

6.55 Consent from SOCA (referred to as a 'notice' in the Terrorism Act), 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 arrangement, or the nominated officer of the reporting firm, with a defence against a possible later charge under the Terrorism Act in respect of that transaction or arrangement if it proceeds.

General

6.56 The consent provisions can only apply where there is prior notice to SOCA of the transaction or activity; SOCA 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 dealt with as an ordinary standard SAR, 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.

6.57 Where there is a need to take urgent action in respect of an account, and the seven working day consent notice period applies, SOCA 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, SOCA 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.

6.58 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.

6.59 The consent regime as it currently operates in the UK is a difficult one for financial practitioners to work with, and continues to be a matter of discussion between the industry and the authorities. There are operational challenges and legal uncertainties concerning what can realistically constitute a 'pre-event' transaction. There are customer service implications - the potentially litigious consequences of declining a

customer's instructions, the inability to give an explanation because of the risk of tipping-off and the problematic requirement referred to in 6.73 for (in particular, large) deposit-taking institutions to seek consent for all post-disclosure transactions over £250.

Tipping off, and prejudicing an investigation

POCA s 333A (1), (3)
Terrorism Act, s 21D

6.60 POCA and the Terrorism Act each contains two separate offences of tipping off and prejudicing an investigation. The first offence relates to disclosing that an internal or external report has been made; the second relates to disclosing that an investigation is being contemplated or is being carried out. These offences 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 conditions precedent for each offence. Each offence relates to situations where the information on which the disclosure was based came to the person making the disclosure in the course of a business in the regulated sector. There are a number of permitted disclosures that do not give rise to these offences (see paragraphs 6.63 to 6.66).

POCA ss 333A (1), 333D(3)
Terrorism Act, ss 21D(1), 21G(3)

6.61 Once an internal or external suspicion report has been made, it is a criminal offence for anyone to disclose information about that report which is likely to prejudice an investigation that might be conducted following that disclosure. An offence is not committed if the person does not know or suspect that the disclosure is likely to prejudice such an investigation, or if the disclosure is a permitted disclosure under POCA or the Terrorism Act. 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 CDD measures, and should not give rise to the tipping off offence.

POCA, ss 333A(3), 333D(4)
Terrorism Act, ss 21D(3), 21G(4)

6.62 Where a money laundering investigation is being contemplated, or being carried out, it is a criminal offence for anyone to disclose this fact if that disclosure is likely to prejudice that investigation. An offence is not committed if the person does not know or suspect that the disclosure is likely to prejudice such an investigation, or if the disclosure is a permitted disclosure under POCA or the Terrorism Act

Permitted disclosures

POCA s 333D(1)
Terrorism Act, s 21G(1)

6.63 An offence is not committed if the disclosure is made to the FSA (or other relevant supervisor) for the purpose of:

- the detection, investigation or prosecution of a criminal offence (whether in the UK or elsewhere);
- an investigation under POCA; or
- the enforcement of any order of a court under POCA.

POCA, s 333B(1)
Terrorism Act, Ss 21A, 21E(1)

6.64 An employee, officer or partner of a firm does not commit an offence under POCA, s333A, or the Terrorism Act, s 21A, if the disclosure is to an employee, officer or partner of the same firm.

POCA, s 333B(2)
Terrorism Act, s 21E(2)

6.65 A person does not commit an offence if the firm making the disclosure and the firm to which it is made belong to the same group (as defined in directive 2002/87/EC), and:

- the disclosure is to a credit institution or a financial institution: and
- the firm to which the disclosure is made is situated in an EEA State, or a country imposing equivalent money laundering requirements.

POCA s 333C
Terrorism Act, s 21F

6.66 A firm does not commit an offence under POCA, s333A or the Terrorism Act s21D, if the disclosure is from one credit institution to another, or from one financial institution to another, and:

- the disclosure relates to
  - a customer or former customer of the firm making the disclosure and of the firm to which the disclosure is made; or
  - a transaction involving them both; or
  - the provision of a service involving them both.
- the disclosure is for the purpose only of preventing an offence under Part 7 of POCA or under Part III of the Terrorism Act;
- the firm to which the disclosure is made is situated in an EEA State or in a country imposing equivalent money laundering requirements; and
- the firm making the disclosure and the one to which it is made are subject to equivalent duties of protection of personal data (within the meaning of the Data Protection Act 1998).

POCA, ss 335, 336
Terrorism Act, ss21ZA, ZB

6.67 The fact that a transaction is notified to SOCA before the event, and SOCA does not refuse consent within seven working days following the day after the authorized disclosure is made, or a restraint order is not obtained within the 31 day moratorium period, does not alter the position so far as 'tipping off' is concerned.

6.68 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 SOCA;
- cannot later – unless law enforcement/SOCA 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 or the Terrorism Act; and
- cannot tell the customer that law enforcement is conducting an investigation.

6.69 The judgement in K v Natwest [2006] EWCA Civ 1039 confirmed the application of these provisions. The judgement in this case also dealt with the issue of suspicion stating that the "The existence of suspicion is a subjective fact. There is no legal requirement that there should be reasonable grounds for the suspicion. The relevant bank employee either suspects or he does not. If he does suspect, he must (either himself or through the Bank's nominated officer) inform the authorities." It was further observed that the "truth is that Parliament has struck a precise and workable balance of conflicting interests in the 2002 Act". The Court appears to have approved of the 7 and 31 day scheme and said that in relation to the limited interference with private rights that this scheme entails "many people would think that a reasonable balance has been struck". A full copy of the judgement is available at

www.soca.gov.uk/downloads/KvNatWest.pdf.

6.70 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.

6.71 SOCA has confirmed that, in such cases, a firm may tell the FOS's legal department about a report to SOCA 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's legal department will then ensure that the case is handled appropriately in these difficult circumstances – liaising as necessary with SOCA. FOS's 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

6.72 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 SOCA, as appropriate.

POCA s 339A

6.73 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 meets the 'threshold' requirement of £250 or less; where the proposed transaction exceeds £250, permission to vary the 'threshold' payment is required from SOCA before it may proceed.

6.74 The significant practical difficulties involved in meeting the legal requirements set out in paragraph 6.73 are the subject of continuing discussions with the authorities.

POCA, ss 337 (1), 338(4)
Terrorism Act s 21B

6.75 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. SOCA has established a SARs Confidentiality Hotline (0800 2346657) to report breaches from reporters and end-users alike.

6.76 SOCA's 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 or a terrorist finance offence under ss 15-18 of the Terrorism Act. 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.

6.77 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 SOCA for consent to repatriate the funds.

6.78 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.

6.79 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.

6.80 Where the firm does not wish to make the payment requested by a customer, it should notify SOCA 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. SOCA 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.

6.81 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.

6.82 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

6.83 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.

6.84 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.

6.85 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.

6.86 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 SOCA.

6.87 If the customer wishes subsequently to withdraw or transfer the funds, the firm should, in the first instance, contact SOCA for consent. Consent from SOCA 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.

6.88 Although each case must be considered on its facts, the effective use of customer 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.

6.89 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

6.90 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.

6.91 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

6.92 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, s 29

6.93 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.

6.94 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.

6.95 To establish whether disclosure would be likely to prejudice an investigation or a potential investigation, firms should approach SOCA for guidance; SOCA 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.

6.96 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.

6.97 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.

6.98 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 SOCA. 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)

6.99 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 SOCA, 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 7

STAFF AWARENESS, TRAINING AND ALERTNESS

- **Relevant law/regulation**
  - Regulation 21
  - POCA ss 327-329, 330 (6),(7), 333, 334(2)
  - Terrorism Act ss 18, 21A
  - SYSC 6.3.7 (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?

7.1 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.

7.2 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/CTF strategy.

7.3 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 ss 327-329, 334 (2) Terrorism Act ss 18, 21A

7.4 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

SYSC 3.1.6 R SYSC 5.1.1 R

7.5 The FSA requires authorised firms to employ personnel with the skills, knowledge and expertise necessary for the discharge of the responsibilities allocated to them.

TC 2.1 SYSC 3.1.9 G SYSC 5.1.4A G

7.6 Firms carrying out retail activities that are subject to TC are responsible for ensuring 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; and
- the level of competence is appropriate to the nature of the business.

Other firms may nevertheless wish to take TC into account in complying with the high-level training and competence requirement in SYSC.

Regulation 16

7.7 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 take appropriate measures so that all relevant employees are made aware of the law relating to money laundering and terrorist financing, and that they are regularly given training in how to recognise and deal with transactions which may be related to money laundering or terrorist financing.

SYSC 6.3.9 (1) R SYSC 6.3.7 (1) G

7.8 The FSA specifically requires the MLRO to have responsibility for oversight of the firm's AML systems and controls, which include appropriate training for the firm's employees in relation to money laundering.

POCA, s 330 (6) and (7)

7.9 Where a staff member is found 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 16

7.10 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 20

7.11 Senior management must be aware of their obligations under the ML Regulations to establish appropriate systems and procedures to forestall and prevent operations relating to 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 20
SYSC 6.3.8 R
SYSC 6.3.9 R

7.12 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.

7.13 As noted in paragraph 1.29, the relationship between the MLRO and the director(s)/senior manager(s) allocated overall responsibility for the establishment and maintenance of the firm's AML/CTF systems is one of the keys to a successful AML/CTF regime. It is important that this relationship is clearly defined and documented, so that each knows the extent of his, and the other's, role and day to day responsibilities.

7.14 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.

7.15 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

7.16 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.

7.17 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

7.18 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

7.19 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

7.20 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

7.21 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

7.22 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 SOCA where a SAR has been made.

7.23 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 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.

7.24 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

7.25 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.

7.26 The set of circumstances giving rise to an unusual transaction or arrangement, and which may provide reasonable grounds for concluding that it is suspicious (see paragraph 6.11), 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.

7.27 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 the information provided and what would be expected, given the location of the customer?
- 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?

7.28 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).

7.29 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.

7.30 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.

7.31 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 at www.fatf-gafi.org.

7.32 SOCA publishes a range of material at www.soca.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.

7.33 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 at www.jmlsg.org.uk.

Staff based outside the UK

7.34 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/CTF 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

7.35 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.

7.36 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.

7.37 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.

7.38 Whatever the approach to training, it is vital to establish comprehensive records (see paragraph 8.21) to monitor who has been trained, when they received the training, the nature of the training given and its effectiveness.

CHAPTER 8

RECORD KEEPING

➢ **Relevant law/regulation** ▪ Data Protection Act 1998 ▪ Regulations 19 and 20 ▪ SYSC Chapter 3
➢ **Core obligations** ▪ Firms must retain: • copies of, or references to, 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 19

8.1 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.

8.2 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 19
SYSC 3.2.20R
SYSC 6.3.1 R

8.3 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.

8.4 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?

8.5 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.

8.6 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 19

8.7 In relation to the evidence of a customer's identity, firms must keep a copy of, or the references to, the evidence of the customer's identity obtained during the application of CDD measures. Where a firm has received a confirmation of identity certificate, this certificate will in practice be the evidence of identity that must be kept. Some documents which may be used for evidence of identification are more sensitive than others (for example, Armed Forces Cards and Firearms certificates – see paragraph 5.3.74): where originals of these documents are offered, firms should consider retaining only the reference numbers and dates of issue of such documents, rather than taking actual photocopies.

8.8 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.

8.9 A firm may often hold additional information in respect of a customer obtained for the purposes of enhanced customer due diligence or ongoing monitoring.

8.10 Where the individual presents himself to the firm, or at one of its branches, he may produce the necessary evidence of identity 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 evidence of identity, 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.

8.11 The Home Office current guidance on copying passports is available at www.opsi.gov.uk/advice/crown-copyright/copyright-guidance/reproduction-of-the-british-passport.

Regulation 19(3)

8.12 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:

- an occasional 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.

8.13 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, and be available on request, where these areas seek to rely on this evidence, or where they may be called upon by law enforcement to produce them.

8.14 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

8.15 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 19(3)

8.16 Records of all transactions relating to a customer must be retained for a period of five years from the date on which the transaction is completed.

8.17 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 occasional 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

8.18 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 SOCA, a record of the other material that was considered.

8.19 In addition, copies of any SARs made to SOCA should be retained.

8.20 Records of all internal and external reports should be retained for five years from the date the report was made.

Other

8.21 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.

Regulation 20(4)

8.22 A firm must establish and maintain systems which enable it to respond fully and rapidly to enquiries from financial investigators accredited under s3 of POCA, persons acting on behalf of the Scottish Ministers in their capacity as an enforcement authority under the Act, officers of HMRC or constables, relating to:

- whether it maintains, or has maintained during the previous five years, a business relationship with any person; and
- the nature of that relationship.

Form in which records have to be kept

8.23 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.

8.24 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.

8.25 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

8.26 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.

8.27 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.

8.28 Firms should take account of the scope of AML/CTF 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.

8.29 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.

8.30 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.

8.31 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 45(1)

8.32 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
Annex I Financial Institution	An undertaking (other than a credit institution, a consumer credit institution, a money service business or an Approved person) that carries out one or more of the operations (other than trading on their own account where the undertaking's only customers are group companies) listed on Schedule 1 to the ML Regulations. ML Regulation 22(1)
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].
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.direct.gov.uk/en/TravelAndTransport/Passports/Applicationinformation/DG_174151 ➢ Others might include members of a local authority, staff of a higher or further education establishment, or a hostel manager.
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 individual who ultimately owns or controls the customer on whose behalf a transaction or activity is being conducted. Special rules have been made for bodies corporate (1), partnerships (2), trusts (3), entities or arrangements that administer and distribute funds (6) and estates of deceased persons (8). ML Regulation 6
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.
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)]
Equivalent jurisdiction	A jurisdiction (other than an EEA state) whose law contains equivalent provisions to those contained in the EU Money Laundering Directive [see www.jmlsg.org.uk].
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. A Third Money Laundering Directive, adopted in 2005 (2005/60/EC), updated European Community legislation in line with the revised FATF 40+9 Recommendations. It repealed and replaced the First and Second Directives. The Implementing Measures Directive, adopted in 2006 (2006/70/EC) elaborated on some of the terms used in the Third Money Laundering Directive. It defines PEP, lists situations where SDD may be applied, and sets the conditions for the exemption for financial activity on an occasional and very limited basis.
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.
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.
HM Treasury Sanctions Notices and News Releases	Notices issued by HM Treasury 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.
Identification	Ascertaining the name of, and other relevant information about, a customer or beneficial owner.
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 2007 [SI 2007/2157].
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 business	An undertaking which by way of business operates a currency exchange office, transmits money (or any representations of monetary value) by any means or which cashes cheques which are made payable to customers. [ML Regulation 2(1)]
Nominated officer	A person in a firm or organisation nominated by the firm or organisation to receive

	disclosures under Regulation 20(2)(d)(i) 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.
Occasional transaction	Any transaction (carried out other than as part of a business relationship) amounting to €15,000 or more, whether the transaction is carried out in a single operation or several operations which appear to be linked. [ML Regulation 2 (1)]
Politically exposed person	An individual who is or has, at any time in the preceding year, been entrusted with prominent public functions, and an immediate family member, or a known to close associate, of such persons. This definition only applies to those holding such a position in a state outside the UK, or in a Community institution or an international body. [ML Regulation 14(5)]
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 and not excluded by the Financial Services and Markets Act 2000 (Exemption) Order 2001 (which exempts certain persons carrying on specific activities from carrying on regulated activities).
Regulated market	A multilateral system operated and/or managed by a market operator, which brings together or facilitates the bringing together of multiple third-party buying and selling interests in financial instruments - in the system and in accordance with its non-discretionary rules - in a way that results in a contract, in respect of the financial instruments admitted to trading under its rules and/or systems, and which is authorised and functions regularly [and in accordance with the provisions of Articles 36-47 of MiFID]. [MiFID Article 4(14)]
Regulated sector	Persons and firms which are subject to 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, or of a beneficial owner through carrying out risk-based and adequate measures.

Abbreviation	
ACPO	Association of Chief Police Officers
AML	Anti-money laundering
CDD paper	Basel Committee Customer Due Diligence paper, published in October 2001
CTF	Combating terrorism financing
DWP	Department of Work and Pensions
FATF	Financial Action Task Force, an intergovernmental body whose purpose is to develop and promote broad AML/CTF 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
MiFID	The Marketing in Financial Instruments Directive
MLRO	Money Laundering Reporting Officer
SOCA	Serious Organised Crime Agency, 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 and administers the UK's financial sanctions regime	**Serious Organised Crime Agency** • As 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 • Exercises powers under POCA to recover the proceeds of crime through criminal, civil, or tax recovery processes • Supports law enforcement agencies • Trains financial investigators **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 **The Revenue and Customs Prosecutions Office** • Prosecutes money laundering, drug trafficking and certain tax offences investigated by HMRC **Crown Prosecution Service**	**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) **Other regulators include** • Office of Fair Trading • HM Revenue and Customs • Gambling Commission	**Joint Money Laundering Steering Group** • Industry body made up of 18 financial sector trade bodies • Produces guidance on compliance with legal and regulatory requirements and good practice

	• 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		

APPENDIX II

SUMMARY OF UK LEGISLATION

Proceeds of Crime Act 2002[6] (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, as amended:

    - empowers SOCA, to conduct an investigation[7] 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[8]
        - a search and seizure warrant[9]
        - a disclosure order[10]
        - a customer information order[11]
        - an account monitoring order[12]

    - establishes the following criminal offences:

        - a criminal offence[13] 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[14] 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 6.73).

        - a criminal offence[15] 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

[6] 2002 ch 29
[7] section 341(2)
[8] section 345
[9] section 352
[10] section 357
[11] section 363
[12] section 370 – see also Terrorism Act s38A
[13] sections 327 - 329
[14] sections 330 and 331
[15] section 333A

nominated officer or to SOCA, or that the police or customs authorities are carrying out or intending to carry out a money laundering investigation.

- a criminal offence[16] of destroying or disposing of documents which are relevant to an investigation.

- a criminal offence[17] 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 Serious Organised Crime Agency (SOCA) 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 of five years' imprisonment and/or an unlimited fine.

  - for "tipping off" of two 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[18], and the Anti-terrorism, Crime and Security Act 2001[19]

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[20] 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[21] 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 SOCA, or that the police or customs authorities are carrying out or intending to carry out a terrorist financing investigation

   - grants[22] a power to the law enforcement agencies to make an account monitoring order, similar in scope to that introduced under POCA

[16] section 341(2)(b)
[17] section 366
[18] 2000 ch 11
[19] 2001 ch 24
[20] section 21A
[21] section 39
[22] 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. The definition of terrorist property, involvement with which is an offence, includes resources of a proscribed organisation. The primary source of information on proscribed organisations, including up-to-date information on aliases, is the Home Office. A list of organisations which have been proscribed under the Terrorism Act can be found at: www.homeoffice.gov.uk/security/terrorism-and-the-law/terrorism-act/proscribed-groups?version=1.

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.

Counter-terrorism Act 2008, Schedule 7

5. Schedule 7 to the CTA gives power to HM Treasury to issue directions to firms in the financial sector. The kinds of requirement that may be imposed by a direction under these powers relate to
    - customer due diligence;
    - ongoing monitoring;
    - systematic reporting ;
    - limiting or ceasing business.

6. The requirements to carry out CDD measures and ongoing monitoring build on the similar obligation under the ML Regulations. The requirements for systematic reporting and limiting or ceasing business are new.

7. The Treasury may give a direction **if one or more** of the following conditions is met in relation to a non-EEA country:
    - that the Financial Action Task Force has advised that measures should be taken in relation to the country because of the risk of terrorist financing or money laundering activities being carried on
        (a) in the country,
        (b) by the government of the country, or
        (c) by persons resident or incorporated in the country.
    - that the Treasury reasonably believe that there is a risk that terrorist financing or money laundering activities are being carried on
        (a) in the country,
        (b) by the government of the country, or
        (c) by persons resident or incorporated in the country,

and that this poses a significant risk to the national interests of the UK.

- that the Treasury reasonably believe that

  (a) the development or production of nuclear, radiological, biological or chemical weapons in the country, or

  (b) the doing in the country of anything that facilitates the development or production of any such weapons,

  poses a significant risk to the national interests of the UK.

Financial sanctions

8. HM Treasury 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: http://www.hm-treasury.gov.uk/d/sanctionsconlist.pdf

9. It is a criminal offence to make payments, or to allow payments to be made, to targets on the list maintained by HM Treasury. 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.

10. Guidance on compliance with the financial sanctions regime is set out in paragraphs 5.3.41 – 5.3.64.

Money Laundering Regulations 2007[23]

11. The Money Laundering Regulations 2007 specify arrangements which must be in place within firms within the scope of the Regulations, in order to prevent operations relating to money laundering or terrorist financing.

12. The ML Regulations apply[24], 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);
    - Trust and company service providers;
    - Casinos;

[23] SI 2007/2157
[24] Regulation 3

- 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.

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

14. Persons within the scope of the ML Regulations are required to establish adequate and appropriate policies and procedures in order to prevent operations relating to money laundering or terrorist financing, covering:

    - customer due diligence;
    - reporting;
    - record-keeping;
    - internal control;
    - risk assessment and management;
    - compliance management; and
    - communication.

15. The FSA may[25] 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/CTF 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

16. FSMA gives the FSA a statutory objective[26] to reduce financial crime. In considering this objective, the FSA is required[27] 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.

17. Firms may only engage in a regulated activity[28] 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.

---

[25] FSMA, s 402(1)(b)

[26] 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".

[27] FSMA s 6(2)

[28] FSMA s22, Schedule 2, and the Regulated Activities Order. These activities are substantially the same as set out in Regulation [2 (2)(a)].

18. 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.

19. 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 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 6.1.1 R to SYSC 6.3.10 G". (COND 2.5.7G)

20. SYSC requires FSA-regulated firms (subject to some specified exceptions: see paragraph 1.35 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[29];
    - 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 6.1.1 R to SYSC 6.3.10 G[30];
    - DEPP – When considering whether to take disciplinary action in respect of a breach of the money laundering rules in SYSC 3.2 or SYSC 6.3 the FSA will have regard to whether a firm has followed relevant provisions in the JMLSG guidance for the financial sector[31];
    - PRIN - Principle 3 requires a firm to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems[32]; and
    - SYSC - Chapters 2, 3 and 6 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 6.3.1 R to SYSC 6.3.10 G (and SYSC 6.3) cover systems and controls requirements in relation to money laundering[33].

21. 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

[29] APER 2.1.2P
[30] COND 2.5.7(10) G

[31] DEPP 6.2.3 G
[32] PRIN 2.1.1 R
[33] SYSC 2 and 3

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[34], and specifically require appropriate systems and controls over the management of money laundering risk[35].

22. The FSA has also issued a publication "Financial Crime: A Guide for Firms" which provides practical assistance and information for firms on actions they can take to counter the risk that they might be used to further financial crime.

[34] SYSC 6.1.1 R
[35] SYSC 6.3.7 G