



# **The Consultative Committee of Accountancy Bodies**

PO Box 433  
Chartered Accountants' Hall  
Moorgate Place, London EC2P 2BJ  
Telephone: 020 7920 8100  
Facsimile: 020 7628 1874  
Email: [admin@ccab.org.uk](mailto:admin@ccab.org.uk)  
Website: <http://www.ccab.org.uk>

The Institute of Chartered Accountants in England and Wales  
The Institute of Chartered Accountants of Scotland  
The Institute of Chartered Accountants in Ireland  
The Association of Chartered Certified Accountants  
The Chartered Institute of Management Accountants  
The Chartered Institute of Public Finance and Accountancy

## **ANTI-MONEY LAUNDERING GUIDANCE FOR THE ACCOUNTANCY SECTOR**

***Guidance for those providing audit, accountancy, tax advisory, insolvency or related services in the United Kingdom, on the prevention of money laundering and the countering of terrorist financing. Issued by the Consultative Committee of Accountancy Bodies, in December 2007.***

The Guidance has been issued to provide the accountancy sector with not only an interpretation of the requirements of the Money Laundering Regulations 2007 (which become effective from 15<sup>th</sup> December 2007) and primary legislation relating to money laundering and terrorist financing but also to provide practical guidance on good practice for matters not prescribed in law.

The Guidance has been completely refreshed and expanded, from previous versions of the CCAB Guidance, drawing not only on changes in law but the experience of practitioners. For more complex areas of customer due diligence, our Guidance continues to be cross referred to the guidance notes issued by the Joint Money Laundering Steering Group. However, it is intended that, at least for most smaller practitioners, the Guidance will be self contained and the need to refer to additional external material will be minimal.

Certain aspects of the law are still subject to change at the time of issuing this Guidance, particularly in the areas of the expected prescribed form and manner of reporting. We have included advice on compliance with the law as it is expected to be on 15<sup>th</sup> December, to assist firms in their preparation, training and implementation. Inevitably, there may be some future changes. However, we suggest that it is appropriate for firms to continue implementation on the basis of this Guidance, and we will endeavour to bring any changes to the attention of practising accountants and related professionals as soon as possible.

To aid easy access, use is made of defined terms explained in a glossary and each section is prefaced with key points for quick reference.

Additional guidance for tax practitioners, developed by the Chartered Institute of Taxation, the Association of Chartered Certified Accountants, the Association of Taxation Technicians, the Chartered Institute of Management Accountants, HMRC and the Institute of Chartered Accountants in England and Wales, will be issued for consultation shortly and will be available from the ICAEW, CIOT and CCAB websites.

HM Treasury approval of the guidance will be sought (approval will also be sought separately for the additional guidance for tax practitioners in due course). This will mean, if granted, that the Courts must consider the content of the guidance when determining whether an accountant's conduct gives rise to an offence under either the Proceeds of Crime Act 2002 or the Money Laundering Regulations 2007.

If you have any queries please contact [sharon.grant@ccab.org.uk](mailto:sharon.grant@ccab.org.uk).

# **ANTI-MONEY LAUNDERING GUIDANCE FOR THE ACCOUNTANCY SECTOR**

*Guidance for those providing audit, accountancy, tax advisory, insolvency or related services in the United Kingdom, on the prevention of money laundering and the countering of terrorist financing, issued by the Consultative Committee of Accountancy Bodies.*

## CONTENTS

### SECTION 1 – ABOUT THIS GUIDANCE

- 1.1-1.3 INTRODUCTION
- 1.4-1.13 BUSINESSES AND INDIVIDUALS WITHIN THE SCOPE OF THIS GUIDANCE
- 1.14 ROLE OF SUPERVISORY AUTHORITIES
- 1.15-1.21 LEGAL REQUIREMENTS AND STATUS OF THIS GUIDANCE

### SECTION 2 – THE OFFENCES

- 2.1- 2.2 WHAT IS MONEY LAUNDERING?
- 2.3-2.7 MONEY LAUNDERING OFFENCES
- 2.8-2.11 OFFENCES OF FAILURE TO DISCLOSE
- 2.12-2.14 Required Disclosure
- 2.15-2.16 Defences and exemptions
- 2.17-2.21 ‘TIPPING OFF’
- 2.22-2.24 PREJUDICING AN INVESTIGATION
- KNOWLEDGE AND SUSPICION
- 2.25-2.29 Is it Knowledge or Suspicion?
- 2.30-2.33 Reasonable grounds for Knowledge or Suspicion
- 2.34-2.37 NON-COMPLIANCE WITH MONEY LAUNDERING REGULATIONS

### SECTION 3 - ANTI MONEY LAUNDERING SYSTEMS AND CONTROLS

- 3.1-3.2 INTRODUCTION
- 3.3 REQUIREMENTS
- 3.4-3.8 Systems
- 3.9 Record keeping
- 3.10-3.12 Reporting Procedures
- 3.13-3.21 Communications and training

## SECTION 4 – THE RISK BASED APPROACH TO CUSTOMER DUE DILIGENCE

### **RISK ASSESSMENT AND MANAGEMENT**

- 4.1-4.2 Policies and Procedures
- 4.3 Risk profile
- 4.4-4.6 Managing compliance
  
- 4.7-4.12 THE RISK-BASED APPROACH
- 4.13-4.21 Developing and applying a risk-based approach

## SECTION 5 – CUSTOMER DUE DILIGENCE

### **5.1-5.3 WHY THIS IS IMPORTANT**

### **5.4-5.5 WHAT IS THE MEANING OF CUSTOMER DUE DILIGENCE?**

### **5.6-5.7 WHAT IS A BENEFICIAL OWNER?**

### **APPLICATION AND TIMING OF CUSTOMER DUE DILIGENCE**

- 5.8-5.11 Measures to be taken before entering a relationship/carrying out a transaction)
- 5.12-5.15 When delay may be acceptable
- 5.16-5.17 Non compliance (client refusal)
- 5.18-5.19 Continuing client due diligence

### **5.20-5.21 THE RISK-BASED APPROACH TO CLIENT DUE DILIGENCE**

- 5.22-5.24 Simplified due diligence
- 5.25-5.26 Enhanced due diligence
- 5.27-5.29 Politically exposed persons (PEPs)
- 5.30-5.32 Prohibited relationships
- 5.33-5.41 Reliance on third parties

### **CONDUCTING CUSTOMER DUE DILIGENCE**

- 5.42-5.44 Know your client (KYC)
- 5.45 Specific customer due diligence prompts
- 5.46 On-going monitoring
- 5.47-5.48 Risk-based verification
- 5.49-5.51 Documentary evidence used in the verification of identity
- Certification and annotation
- 5.52 Certification
- 5.53 Annotation
- 5.54-5.55 Electronic identification
- 5.56-5.59 Insolvency cases

### **SECTION 5A - Specific prompts for clients**

- A. For entities/businesses**
- B. For individuals**

### **SECTION 5B – Examples of risk-based verification**

- A. Individuals**
- B. Entities**
  - i. Private company/LLP**
  - ii. Listed or regulated entity**
  - iii. Government bodies**
  - iv. Money services businesses**

## SECTION 6 – INTERNAL REPORTING

### **6.1-6.5 WHAT MUST BE REPORTED?**

#### **6.6 TYPES OF REPORT**

- 6.7-6.8 The Protected Disclosure**
- 6.9 The Authorised Disclosure**
- 6.10 Confidentiality Protection**
- 6.11 Non-POCA Reporting**

#### **RECOGNISING MONEY LAUNDERING**

- 6.12-6.14 The Key Elements**
- 6.15-6.17 Criminal Conduct**
- 6.18-6.19 Criminal Property**
- 6.20-6.22 Intent**
- 6.23-6.27 Determining whether and when to Report**

#### **HOW TO REPORT**

- 6.28-6.30 Internal Reports to the MLRO**
- 6.31 Reports to SOCA**

## SECTION 7 – Role of MLRO and SAR Reporting

### **7.1-7.3 THE ROLE**

#### **7.4-7.9 ASSESSING INTERNAL REPORTS**

- 7.10-7.11 The Reporting Record**

#### **7.12-7.19 MAKING EXTERNAL REPORTS**

- 7.20-7.25 Guarding Confidentiality**

#### **7.26-7.33 THE PRIVILEGE REPORTING EXEMPTION**

- 7.34 Legal Advice**
- 7.35 Litigation**
- 7.36-7.39 Examples of Privileged Circumstances**
- 7.40-7.41 Recording and Discussion with MLRO**
- 7.42-7.46 The Crime/Fraud Exception**

## SECTION 8 – CONSENT

### **8.1-8.9 MATTERS FOR CONSENT**

#### **8.10 CONSTRUCTIVE TRUST**

#### **8.11-8.14 SUSPENSION OF ACTIVITY**

#### **8.15-8.19 APPLYING FOR AND RECEIVING CONSENT**

- 8.20-8.21 Refusal of Consent**

#### **8.22 EXEMPTIONS FOR BANKS AND DEPOSIT TAKERS**

## SECTION 9 – POST SAR ACTIONS

### **CONTINUING WORK IN CONNECTION WITH A REPORTED MATTER**

**9.1-9.4 Client relationships**

**9.5-9.10 Balancing Professional Work and POCA Requirements**

### **REQUESTS FOR FURTHER INFORMATION**

**Requests arising from a change in professional appointment (professional enquiry)**

**9.11-9.17 Requests from SOCA or Law Enforcement Agencies**

**9.18 Requests regarding identification information**

**9.19 Requests regarding suspicious activity**

**9.20-9.22 DATA PROTECTION ACT - SUBJECT ACCESS REQUESTS**

## SECTION 1 – ABOUT THIS GUIDANCE

### KEY POINTS

- UK *anti-money laundering* regime requirements are set out in the Proceeds of Crime Act 2002 (*POCA*) (as amended by the Serious Organised Crime and Police Act 2005 (*SOCPA*)), the Money Laundering Regulations 2007 (*2007 Regulations*) and the Terrorism Act 2000 (*TA 2000*) (as amended by the Anti-Terrorism, Crime and Security Act 2001 (*ATCSA 2001*) and the Terrorism Act 2006 (*TA 2006*)).
- HM Treasury approval for this *Guidance* will be applied for. If granted the Courts must take it into account in deciding whether or not an offence has been committed under ss330-331, *POCA* or the *2007 Regulations* by an *individual* or *business* within its scope. Until HM Treasury approval is received, the Courts may take the *CCAB Guidance* into account.
- *Businesses* and *individuals* should take account of this *Guidance* when acting in the course of business as auditors, *external accountants*, *insolvency practitioners* and *tax advisers*, and when acting in the course of business as trust and company service providers. Failure to do so could have serious legal, regulatory or professional disciplinary consequences.
- Where other professional or trade bodies have produced specialist *Guidance* concerning particular services or activities, *businesses* and *individuals* may need, to have regard to that *Guidance* as a supplement to this *Guidance*.

---

### INTRODUCTION

- 1.1 Terms that appear in *italics* in this *Guidance* are explained in the Glossary.
- 1.2 This *Guidance* has been drafted to be consistent with the *Guidance* for the UK financial sector issued by the Joint Money Laundering Steering Group (*JMLSG*). Some of the material contained in this guide draws significantly on *JMLSG* wording, for which thanks are due to the *JMLSG*. The *JMLSG Guidance* is very comprehensive, and where *businesses* or *individuals* require further guidance, they may seek it from the *JMLSG Guidance*. *Businesses* and *individuals* carrying out *defined services* who follow the *JMLSG Guidance*, adapted for the circumstances in which they are practising, will be deemed to have followed this *Guidance*.
- 1.3 This *Guidance* has been prepared to assist accountants and related *businesses* and professionals in complying with their obligations, arising from United Kingdom legislation, in relation to the prevention, recognition and reporting of *money laundering*.

---

### **BUSINESSES AND INDIVIDUALS WITHIN THE SCOPE OF THIS GUIDANCE**

- 1.4 The *Guidance* is addressed to *businesses* and *individuals* covered by Regulation 3 (1)(c) of the *2007 Regulations* ie, those who act in the course of a business carried on by them in the United Kingdom as an auditor, *external accountant*, *insolvency practitioner* or *tax adviser* (as defined in Regulation 3(4) to 3(8)), and those who act in the course of business as trust or company service providers under Regulation 3 (1)(e) of the *2007 Regulations* (as defined in Regulation 3(10)). These services are referred to together for the purpose of this *Guidance* as the *defined services*. However, this *Guidance* is not addressed to *independent legal professionals*, even where they are acting as *tax advisers*, *insolvency practitioners* or trust or company service providers. *Independent legal professionals* should refer to *Guidance* issued by their professional body or *anti-money laundering supervisory authority*. Where *businesses* have sub-contracted parts of their work for clients to other *individuals* or *businesses* situated outside of the United Kingdom, it is likely that those others will be subject to local anti-money laundering law

and not to United Kingdom law in respect of the work undertaken by them. However, the responsibility of United Kingdom *businesses* and *individuals* for compliance with the 2007 Regulations and *POCA and TA* in respect of the conduct of their business, and in respect of information or other matters coming to them in the course of conducting that business, remains whether or not parts of the work are sub-contracted.

- 1.5 Regulation 3(7) defines *external accountant* as someone who provides *accountancy services* by way of business to other persons, when providing such services. *The 2007 Regulations* do not define the term *accountancy services*. For the purpose of this *Guidance*, *Accountancy services* includes, any service provided under a contract for services (ie, not a contract of employment) which pertains to the recording, review, analysis, calculation or reporting of financial information.
- 1.6 Employees of organisations which are not providing *defined services* are outside the scope of this *Guidance*. Those employed in other *regulated sectors* (financial services, law firms, estate agents, high value dealers or casinos) should have regard to *Guidance* issued by the employer's trade or professional body or *anti-money laundering supervisory authority*. Employees are not engaged in the *regulated sector* for the purposes of the *anti-money laundering* legislation, if their employer is not acting in the *regulated sector*. Nor are those providing services privately on an unremunerated and voluntary basis, since those services will not have been provided 'by way of business'. Services provided in the course of employment or business in *defined services* will however be included, even if provided to the *client* on a pro-bono or unremunerated basis.
- 1.7 All persons (including those outside the *regulated sector*) risk committing the *money laundering offences* and are required to report suspicions of *terrorist financing* formed in the course of their trade, profession or employment. However, those outside the *regulated sector* have no mandatory requirements for reporting knowledge or suspicions of non-terrorism related *money laundering* (although if they are themselves involved in the *money laundering*, reporting under s338, POCA (authorised disclosures) is required if the person is to benefit from the defence available in this regard under ss 327-329, POCA), or for maintaining *anti-money laundering* systems. Additional guidance on both the legal requirements and on the avoidance of *money laundering* risk, for accountants or tax advisers working outside the *regulated sector*, may be sought from an appropriate trade or professional body.
- 1.8 All *businesses* and *individuals* within the scope of this *Guidance* should have regard to its content, in respect of all *defined services*. Members and member firms of the CCAB member bodies and other professional bodies which adopt this *Guidance* should be aware that failure to take account of the provisions of this *Guidance* can give rise to a liability to disciplinary action. *Businesses* and *individuals* undertaking *defined services* who are supervised by HMRC should refer to the HMRC's web site to determine the likely effects of failure to take into account this *Guidance*.
- 1.9 It should also be noted that the way in which *businesses* and *individuals* apply the provisions of this *Guidance* will be likely to influence decisions by their professional bodies on whether they have complied with general ethical requirements, for example relating to integrity, the need to consider the public interest, or regulatory requirements.
- 1.10 *Businesses* and *individuals* may also need to have regard to *Guidance* issued by other standard setters, professional bodies or trade associations where this relates to particular specialist services. Additional *Guidance* should be read in conjunction with this *Guidance*. Such *Guidance* includes (but may not be limited to):
  - Auditors – Auditing Practices Board Practice Note 12 'Money Laundering: Interim *Guidance* for Auditors in the UK'.
  - *Tax advisers* - [To follow].

- *Insolvency practitioners* – [If necessary – to follow].

- 1.11 This *Guidance* does **not** deal with the specific requirements of the Financial Services Authority (*FSA*). Accordingly, those providing financial services and regulated by the *FSA* should additionally refer to *FSA* requirements, which incorporate *anti-money laundering Guidance* issued by the Joint Money Laundering Steering Group (*JMLSG*).
- 1.12 However, this *Guidance* **does** cover the requirements of firms providing services under the Designated Professional Body provisions of Part XX, section 326 of the Financial Services and Markets Act 2000, or otherwise providing financial services under the oversight of their professional body. Such activities for the purpose of this *Guidance* are included within the scope of *defined services*.
- 1.13 As well as '*business relationship*', the *2007 Regulations* refer to 'occasional transactions', ie, those outside the *business relationship* valued at over €15,000. 'Occasional transactions' is a cogent term in a banking context but is difficult to apply in the context of *accountancy services*. Therefore this *Guidance* uses only '*business relationship*', a more natural term for *accountancy and related services*, throughout.

---

## ROLE OF SUPERVISORY BODIES

- 1.14 The *2007 Regulations* require all *businesses* to be supervised by an appropriate *anti-money laundering supervisory authority*. For many *businesses* acting as *external accountants* and/or auditors, *tax advisers* or *insolvency practitioners* the supervisory authority will be the professional body to which they belong. A full list of approved supervisory authorities for the accountancy sector is set out in Schedule 3 to the *2007 Regulations*, including all six *CCAB* member bodies and certain other accountancy and tax bodies. Those *businesses* that are not members of, or otherwise regulated by, one of the approved bodies will be supervised by HMRC. Where a *business* or *individual* is subject to more than one *anti-money laundering supervisory authority* the relevant *anti-money laundering supervisory authorities* may (Regulation 23 (2)) agree that one shall act in respect of that *business* or *individual* but they are not obliged to do so. Accordingly some *businesses* and *individuals* will continue to have to respond to more than one *anti-money laundering supervisory authority*.

---

## LEGAL REQUIREMENTS AND STATUS OF THIS GUIDANCE

- 1.15 The legislation which embodies the UK *anti-money laundering* regime is contained in:

- The Proceeds of Crime Act 2002 (*POCA*) as amended by The Serious Organised Crime and Police Act 2005 (*SOCPA*) and relevant statutory instruments;
- The Terrorism Act 2000 (*TA 2000*) (as amended by the Anti Terrorism Crime and Security Act 2001 (*ATCSA*) and the Terrorism Act 2006 (*TA 2006*)) and relevant statutory instruments; and
- The Money Laundering Regulations 2007 (*2007 Regulations*) and relevant statutory instruments.

*POCA* and *TA 2000* contain offences which may be committed by *individuals* or entities, whereas the *2007 Regulations* deal with the systems and controls which *businesses* are required to have and contain offences which may be committed by *businesses* as well as the key *individuals* within them.

- 1.16 Approval by HM Treasury has been sought in relation to this *Guidance*. Approval means the Courts must have regard to the *Guidance* in deciding whether *businesses* or *individuals* affected by it have committed an offence under the *2007 Regulations* or under ss330-331, *POCA*. Of course, this *Guidance* cannot be exhaustive. It may be necessary to seek advice either from trade or professional bodies, *anti-money laundering*

*supervisory authorities* or other sources on issues and situations not covered by this *Guidance*.

- 1.17 This *Guidance* has been prepared on the basis that compliance with its requirements, and recommendations, will ensure compliance with relevant legislation and professional requirements. Within this *Guidance*, the term ‘must’ is used to indicate a legal or regulatory requirement and accordingly the use of this term indicates where following this *Guidance* is considered mandatory. *Businesses* and *individuals* may seek alternative interpretations of the UK *anti-money laundering* regime if they wish but they are recommended to consider the impact of any advice they receive on their obligations and be able to justify why they have preferred to implement an alternative interpretation. However, there are many instances where law and regulation does not prescribe the required actions. In such instances the term ‘should’ (and other terms suggesting possible ways in which *Businesses* and *Individuals* may approach matters subject to this *Guidance*) are used to indicate good practice methods that may be employed to meet statutory and regulatory requirements. *Businesses* and *individuals* need to consider the specific circumstances of their own situation in determining whether the suggested good practice methods are appropriate, or whether they consider alternative practices may be employed to achieve compliance with law and regulation. In all cases, *Businesses* and *individuals* need to be prepared to be able to explain to their *anti-money laundering supervisory authority* the rationale for their procedures and why they consider they are compliant with law and regulation.
- 1.18 Note that the UK *anti-money laundering* regime does not apply to some services that *businesses* may undertake and applying the regime’s requirements to all their services may in these cases be unnecessarily costly. This *Guidance* assumes that many *businesses* will find it easier, and more effective, to apply the requirements to all their services. However, it is a decision for each *business* to take. Where *businesses* choose to outsource or subcontract work to non-regulated entities, they should bear in mind that they remain subject to the obligation to maintain appropriate risk management procedures to prevent *money laundering* activity. In that context, they should consider whether the subcontracting increases the risk that they will be involved in or used for money laundering, in which case appropriate controls to address that risk should be put in place.
- 1.19 Those involved in the provision of management consultancy services or interim management should be particularly alert to the possibility that they could be within the scope of the *anti-money laundering* regime to the extent they supply any of the *defined services* when acting under a contract for services in the course of business.
- 1.20 Throughout this *Guidance*, *businesses* and *individuals* subject to the provisions of the UK *anti-money laundering* regime through being covered in Regulation 3, *2007 Regulations* or Schedule 9 to *POCA* are referred to as being part of the *regulated sector*. Note that whilst *POCA* refers to those covered in Schedule 9 as ‘regulated’ persons and the *2007 Regulations* refer to those covered by Regulation 3 as ‘relevant’ persons, those included in the two categories are identical.
- 1.21 Throughout this *Guidance*, the *nominated officer* required to be appointed by a *business* under the *2007 Regulations* to receive disclosures in accordance with Part 7, *POCA* is referred to by the name commonly used in the *regulated sector* as a *Money Laundering Reporting Officer* or *MLRO*.

## SECTION 2 – THE OFFENCES

### KEY POINTS

- The three *money laundering offences* are those contained in ss327-329, the Proceeds of Crime Act 2002 (POCA). The Terrorism Act 2000 (TA 2000) also creates similar offences relating to *terrorist financing*. In this *Guidance*, the term '*money laundering*' will encompass *terrorist financing* activities.
- Detailed *Guidance* as to the provisions of the TA 2000 has not been provided as the requirements for the *regulated sector* are very similar to those contained in POCA which are described in detail. Reporting of *terrorist financing* suspicions is through the same channels as *money laundering* suspicions.
- The *money laundering* offences are framed very broadly and are designed to catch any activity in respect of *criminal property*, including possession of the proceeds of one's own *criminal conduct*.
- *Criminal conduct* is widely defined by s340, POCA to be conduct that is an offence in any part of the UK as well as conduct occurring elsewhere that would have been an offence if it had taken place in the UK. There are very limited exceptions to this for conduct which is both known to be legal in the country in which it is committed and which falls within the specific exceptions set out in orders made by the Secretary of State.
- *Criminal property* is defined by s340, POCA as being the benefit of *criminal conduct* where the alleged offender knows or suspects that the property in question represents such a benefit.
- *Terrorist property* is defined in s14, TA 2000 as money or property likely to be used for terrorist purposes, or the proceeds of commissioning or carrying out terrorist acts.
- The *money laundering* offences and the similar offences under TA 2000 can be committed by any person, whether or not they are part of the *regulated sector*. Defences available to any person charged with such offences include reporting to the appropriate authorities and obtaining consent. *Individuals* working in any *business* can commit, subject to limited exemptions, the offence of failing to disclose *terrorist financing*.
- There are three further types of POCA offences relevant to *individuals* to whom this *Guidance* relates. These are the failing to disclose offences in ss330-331, POCA (NB: s332 contains a similar offence relating to *MLRO's* outside of the *regulated sector*); *tipping off* (s333, POCA); and *prejudicing an investigation* (s342, POCA). There are similar offences in ss19-21A, TA 2000.
- The offence of failing to make a *money laundering* disclosure (often referred to as failing to report) can be committed by any *individual* working in the *regulated sector* or by an *MLRO* working in other *business*. The offence of *tipping off* is divided into two sections, s333 which applies to those outside the *regulated sector*, and s333A which applies to those in the *regulated sector* only [Subject to expected changes in the law]. The POCA offence of *prejudicing an investigation* can be committed by anyone. There are similar failing to disclose and *tipping off* offences contained in TA 2000.
- There is an offence in s339(1A), POCA of failure to make a disclosure direct to SOCA (usually called a *suspicious activity report*, or SAR) in the prescribed manner and format, [Subject to expected changes in the law].
- It is a criminal offence for a *business* not to comply with the 2007 Regulations, if that *business* is within their scope. It is also an offence for any partner, director or officer of the *business*, to consent to or connive at the non-compliance or by neglect to cause non-compliance.

### WHAT IS MONEY LAUNDERING?

- 2.1 In UK law *money laundering* is defined very widely, and includes all forms of handling or possessing *criminal property*, including possessing the proceeds of one's own crime, and facilitating any handling or possession of *criminal property*. *Criminal property* may take

any form, including in money or money's worth, securities, tangible property and intangible property. *Money laundering* can be carried out in respect of the proceeds of conduct that is an offence in the UK as well as most conduct occurring elsewhere that would have been an offence if it had taken place in the UK. For the purpose of this *Guidance*, *money laundering* is also taken to encompass activities relating to *terrorist financing*, including handling or possessing funds to be used for terrorist purposes as well as proceeds from terrorism. Terrorism is taken to be the use or threat of action designed to influence government, or to intimidate any section of the public, or to advance a political, religious or ideological cause where the action would involve violence, threats to health and safety, damage to property or disruption of electronic systems. Materiality or de minimis exceptions are not available in relation to either *money laundering* or *terrorist financing* offences.

2.2 *Money laundering* activity may range from a single act, eg, being in possession of the proceeds of one's own crime, to complex and sophisticated schemes involving multiple parties, and multiple methods of handling and transferring *criminal property* as well as concealing it and entering into arrangements to assist others to do so. *Businesses* and *individuals* need to be alert to the risks of *clients*, their counterparties and others laundering money in any of its possible forms. The *business* or its *client* does not have to be a party to *money laundering* for a reporting obligation to arise (see section 3). Where criminal proceeds have already arisen, s340(11), *POCA* includes within the definition of *money laundering* any attempt, conspiracy or incitement to commit an offence under ss327-329, *POCA* as well as aiding, abetting, counselling or procuring an offence under ss327-329, *POCA*. In the case of *terrorist financing*, it is an offence to attempt to commit an offence under ss15-18, *TA 2000* even if *terrorist property* has not come into being, eg, under s15(1), *TA 2000* where the invitation to provide money or other property for *terrorist financing* is in itself an offence. Further, the definition of '*terrorist property*' means that all dealings with funds or property which are likely to be used for the purposes of terrorism, even if the funds are "clean" in origin, is a *terrorist financing* offence.

---

## MONEY LAUNDERING OFFENCES

2.3 Sections 327-329 in the Proceeds of Crime Act (*POCA*) (as amended by the Serious Organised Crime and Police Act 2005 (*SOCPA*)) define the *money laundering* offences. **Anyone** can commit one of these. Conviction of any of these offences is punishable by up to 14 years imprisonment and/or an unlimited fine. A person commits a *money laundering* offence if he:

- **Conceals**, disguises, converts or transfers *criminal property*, or removes *criminal property* from England and Wales, or from Scotland or from Northern Ireland (s327);
- Enters into or becomes concerned in an **arrangement** which he knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of *criminal property* by or on behalf of another person (s328); or
- **Acquires**, uses or has possession of *criminal property* except where adequate consideration was given for the property (s329).

2.4 None of these offences are committed if:

- the persons involved did not know or suspect that they were dealing with the proceeds of crime; or
- a report of the suspicious activity is made promptly to an *MLRO* (an *internal report*) or direct to *SOCA* (a *suspicious activity report*, or *SAR*) under the provisions of s338, *POCA*, and (if the report is made before the act is committed) the appropriate consent is obtained before doing the act; or
- if no report is made, there was a reasonable excuse for this failure (note that there is no *money laundering* case law on this issue and it is anticipated that only relatively extreme circumstances, such as duress, might be accepted); or

- if the act is committed by someone carrying out a law enforcement or judicial function; or
- if the conduct giving rise to the *criminal property* was reasonably believed to have taken place outside of the UK, and the conduct was in fact lawful under the criminal law of the place where it occurred, and the maximum sentence if the conduct had occurred in the UK would have been less than 12 months (except in the case of an act which would be an offence under the Gaming Act 1968, the Lotteries and Amusements Act 1976 or under ss23 or 25, *FSMA*, which will fall within the exemption even if the relevant sentence would be in excess of 12 months). In this *Guidance*, this is referred to as the *overseas conduct exemption*.

- 2.5 It should be noted that the tests relating to overseas conduct (set out in SI 2006 No1070 and in Section 2.4, final bullet, of this *Guidance*) are complex and onerous. These are very stringent tests, and as such *individuals* and *businesses* need to be cautious in their application.
- 2.6 There is a further exemption for deposit taking bodies (accountancy *businesses* holding clients' money cannot use this exemption) who may continue to run an account containing *criminal property* where the each transaction is less than the threshold amount (currently £250) set out in s339A, *POCA*.
- 2.7 Note that ss15-18, Terrorism Act 2000 (*the TA 2000*) also create similar offences (*terrorist offences*) to those contained in ss327-329, *POCA* but that there is no *overseas conduct exemption* or threshold amounts.

---

## OFFENCES OF FAILING TO DISCLOSE

- 2.8 *Individuals* in the *regulated sector* commit an offence if they fail to make a disclosure in cases where they have knowledge or suspicion, or reasonable grounds for suspicion, that *money laundering* is occurring. Disclosure must be made to their *MLRO* or direct to *SOCA* under ss330,, *POCA*. In this *Guidance*, disclosure to an *MLRO* is referred to as an *internal report* and to *SOCA* as a *suspicious activity report* or *SAR*. *MLROs* have a duty to make disclosures under s331, *POCA* if they have knowledge, suspicion or reasonable ground to suspect *money laundering* as a consequence of an *internal report*. The s332 failure to disclose offence is similar and would apply to an *MLRO* in a business outside of the *regulated sector*, including an *MLRO* appointed to deal with reports emanating from non-regulated business within a *business* that conducted both regulated, and non-regulated services, in respect of suspicions arising from *internal reports*. This is not further addressed in this *Guidance*. These offences are punishable by imprisonment of up to 5 years and/or an unlimited fine.
- 2.9 Similar provisions regarding failure to disclose are contained in s19, and 21A, *TA 2000*. The s19 failure to report offence is applicable to **anyone** in employment or business outside of the regulated sector, with s21A being applicable to all those in the *regulated sector*.

### The failure to disclose offence under Sections 330 and 331 *POCA*

- 2.10 The failure to disclose offence in s330 is committed if an *individual* fails to make a report comprising the *required disclosure* as soon as is practicable either in the form of an *internal report* to his *MLRO* or in the form of a *SAR* to a person authorised by the Serious Organised Crime Agency (*SOCA*) to receive disclosures. The obligation to make the *required disclosure* arises when:
- a person knows or suspects, or has reasonable grounds for knowing or suspecting that another person is engaged in *money laundering*;

- the information or other matter on which the above is based came to him in the course of business in the *regulated sector*;
- he either can identify that other person, or has information concerning the whereabouts of the laundered property or the information he has may assist in identifying the person or the whereabouts of the property (the laundered property is that which forms the subject of the matter of the known or suspected *money laundering*).

2.11 An *MLRO* is obliged to report if he is satisfied that the information received in *internal reports* meets the tests set out in 2.10. An *MLRO* may commit the s331, *POCA* offence if he fails to pass on reportable information in *internal reports* that he has received, as soon as is practicable, to *SOCA*.

## Required Disclosure

2.12 *Individuals* need to take care to ensure that any information held by them which is part of the *required disclosure*, ie, the identity of the suspect (if known), the information or other matter on which the knowledge or suspicion of *money laundering* (or reasonable grounds for such) is based and the whereabouts of the laundered property (if known) is passed as soon as is practicable to the *MLRO*. Additional information held by the *individual* which identifies other parties involved in or connected to the matter should also be given to the *MLRO*.

2.13 *POCA* s339 provides for the form and manner of *SARs* to be prescribed [subject to implementing legislation being in place]. This is important, as failure to report in the form and manner prescribed will be an offence under s330 1(A), *POCA* punishable by a fine and will come into force following implementation.

2.14 Further *Guidance* on the making of *SARs*, including the appropriate form and manner of reporting, is given in sections 5 and 6 below.

## Defences and exemptions

2.15 There are defences to and exemptions from the failing to disclose offences as follows:

- there is reasonable excuse for not making a report (note that there is no *money laundering* case law on this issue and it is anticipated that only relatively extreme circumstances, such as duress and threats to safety, might be accepted); or
- the *privilege reporting exemption* (see sections 7.26 to 7.46 below) applies; or
- the *individual* does not actually know or suspect *money laundering* has occurred and has not been provided by his employer with the training required by the *2007 Regulations* (Regulation 21). If the employer has failed to provide the training, this is an offence on the part of the employer. The effect for the individual who has not been provided with training is that the objective test (of being required to report if there are 'reasonable grounds' for knowledge or suspicion) is removed; or
- it is known, or believed on reasonable grounds, that the *money laundering* is occurring outside the UK, and is not unlawful under the criminal law of the country where it is occurring.

In determining whether an offence has been committed under ss330 and 331, the Courts must have regard to the content of this *Guidance* [Subject to HMT approval] when applied to an *individual* delivering *defined services* or to an *MLRO*.

2.16 Whilst an *individual* in the *regulated sector* has a duty to report, other persons may voluntarily report to *SOCA* and also receive the protections available both in terms of potentially creating a defence to a *money laundering* offence and also the protection

against accusations of breach of confidentiality providing the report is properly made under the provisions of either of ss337 and 338, *POCA* (See section 6.10) as appropriate.

---

## TIPPING OFF

2.17 The offence of *Tipping off* was previously set out in s333, *POCA*, but was removed by statutory instrument (with an expected effective date of 26 December 2007) The s333, *POCA* offence meant **anyone** not acting in the course of a business in the *regulated sector* could commit this offence which consisted of:

- knowing or suspecting that a report has been made either to an *MLRO* or to *SOCA* (under either s337 or s338, *POCA*); and
- making any disclosure which he knows or suspects is likely to prejudice any investigation that might follow that report.

There were limited exceptions relating to persons carrying out law enforcement or judicial functions, and to legal advisers acting in privileged circumstances provided the disclosure is not made with the intention of furthering a criminal purpose.

The penalty for this offence is a maximum of 5 years imprisonment, or an unlimited fine, or both.

2.18 Section 333, *POCA* is replaced by s333A *POCA* which applies only to the *regulated sector*. The criminal offence of *tipping off* in s333A, *POCA* arises where a person in the *regulated sector* discloses either:

- that a disclosure has been made by a person of information obtained in the course of a *regulated sector business* either to an *MLRO* or to *SOCA* (under either s337 or s338, *POCA*) or to any other person authorised by *SOCA* to receive disclosures, or to the police or HMRC and the disclosure is likely to *prejudice any investigation* that might be conducted following the disclosure referred to; or
- that an investigation into allegations that a *money laundering* offence has been committed, is being contemplated or is being carried out and the disclosure is likely to prejudice that investigation and the information disclosed came to the person in the course of a *business* in the *regulated sector*.

A *tipping off* offence will not be committed under s333A, *POCA* if the person did not know or suspect that the disclosure was likely to *prejudice any investigation* that followed.

The penalty for this offence on summary conviction is a maximum of three months imprisonment, or a fine on scale 5, or both and on conviction on indictment to imprisonment for a term not exceeding two years, or a fine or both. There are a number of exceptions to this prohibition on revealing the existence of a report or an actual or contemplated investigation which are as follows:

- **Disclosures within an undertaking or group etc**, (s333B): a person does not commit an offence if he makes a disclosure to another person employed by the same undertaking as him, and nor does an *independent legal professional* or a *relevant professional adviser* commit an offence if the disclosure is made to another *independent legal professional* or a *relevant professional adviser* where both the person making the disclosure and the person to whom it is made are in either an EEA state or a state imposing equivalent anti-*money laundering* requirements and those persons perform their professional activities within different undertakings that shares common ownership, management or control.
- **Other permitted disclosures between institutions etc** (s333C): an *independent legal professional* or a *relevant professional adviser* does not commit an offence if he

makes a disclosure to another person of the same kind from a different undertaking but of the same professional standing as himself (including as to duties of professional confidentiality and the protection of personal data) where the disclosure relates to the same *client* or former *client* of both advisers and involves a transaction or provisions of a service that involved them both, the disclosure is only made for the purpose of preventing a *money laundering* offence and the disclosure is made to a person in an EU Member State or a State imposing an equivalent money laundering requirements. This means that eg, an accountant may only disclose to another accountant, and not to a lawyer or another kind of *relevant professional adviser*.

- **Other permitted disclosures (general)** (s333D): an offence is not committed if a disclosure is made to a *anti-money laundering supervisory authority* by virtue of the Money Laundering Regulations 2007 or for the purpose of the prevention, investigation or prosecution of a criminal offence in the UK or elsewhere, an investigation under *POCA*, or enforcement of any order of a court under *POCA*. In addition, and of importance to those who are *relevant professional advisers*, an offence is not committed by a *relevant professional adviser* if he makes the disclosure to his *client* for the purpose of dissuading the *client* from engaging in conduct amounting to an offence.

2.19 Any of the *tipping off* offences contained in s333 and s333A will only occur in the circumstances described, but there may be circumstances where a money launderer may be alerted to the possibility that a report will be or has been made or an investigation conducted, other than by a disclosure of such fact eg, by unexpected delay caused by waiting on *consent*. These have been distinguished in this *Guidance* by use of the phrase '*alerting a launderer*'. *Businesses* will also need to take care to guard against *alerting a launderer*, as part of their policies and procedures aimed at preventing operations related to *money laundering*.

2.20 A *tipping off* disclosure may be made in writing or verbally, and either directly or indirectly – including through inclusion of relevant information in published information. Considerable care is required in carrying out any communications with *clients* or third parties following a report. Before any disclosure is made relating to matters referred to in an *internal report* or *SAR*, it is important to consider carefully whether or not it is likely to constitute offences of *tipping off* or prejudicing an investigation. It is suggested that *businesses* keep records of these deliberations and the conclusions reached (sections 7.10 and 7.11).

2.21 However, *individuals* and *businesses* in the *regulated sector* will frequently need to continue to deliver their professional services and a way needs to be found to achieve this without falling foul of the *tipping off* offence. Section 333D(2) is of assistance in this regard (disclosure to his *client* for the purpose of dissuading the *client* from engaging in conduct amounting to a *money laundering* offence). More *Guidance* on acting for a *client* after a *money laundering* suspicion has been formed is given in section 9.

---

## PREJUDICING AN INVESTIGATION

2.22 This offence is set out in s342, *POCA*. This offence is committed where a person:

- knows or suspects that a *money laundering*, confiscation or civil recovery investigation is being conducted or is about to be conducted; and
- makes a disclosure which is likely to *prejudice the investigation*; or
- falsifies, conceals or destroys documents relevant to the investigation, or causes that to happen.

As with *tipping off* offences, the person making the disclosure does not have to intend to prejudice an investigation for this offence to apply. However, there is a defence available

if the person making the disclosure did not know or suspect the disclosure would be prejudicial, did not know or suspect the documents were relevant, or did not intend to conceal any facts from the person carrying out the investigation.

- 2.23 There are limited exceptions relating to persons carrying out law enforcement or judicial functions, and to legal advisers acting in privileged circumstances provided the disclosure is not made with the intention of furthering a criminal purpose.
- 2.24 Considerations similar to those set out under *tipping off* above apply in terms of how the offence may be committed and of taking precautions to ensure any disclosure made does not prejudice an investigation. *Businesses* should ensure they have sufficient document retention policies in place (see Section 3.9 of this *Guidance* – Record Keeping) to meet the needs of this section of *POCA* and the *2007 Regulations*, as well as their legal and professional obligations more generally.

---

## KNOWLEDGE AND SUSPICION

### Knowledge or suspicion?

- 2.25 An offence is committed by an *individual* in the *regulated sector* if he fails to report where he has knowledge, suspicion or reasonable grounds for suspecting *money laundering* activity. There is no definition of knowledge or suspicion within *POCA* and so interpretation of their meaning will rely on judgements in past legal cases, as well as this *Guidance* and on the ordinary meaning of the words.
- 2.26 Having knowledge means actually knowing that something is the case.
- 2.27 Case law suggests that suspicion is a state of mind more definite than speculation, but falls short of knowledge based on evidence. It must be based on some evidence, even if that evidence is tentative – simple speculation that a *client* may be *money laundering* is not sufficient grounds to form a suspicion. Similarly, a general assumption that low levels of crime (eg, not declaring all cash takings) are endemic in particular industry sectors does not amount to reasonable grounds for suspicion of particular *clients* operating in that sector.
- 2.28 A frequently used description is that ‘...A suspicion that something exists is more than a mere idle wondering whether it exists or not; it is a positive feeling of actual apprehension or mistrust, amounting to a “slight opinion, but without sufficient evidence”’ (*Queensland Bacon PTY Ltd v Rees [1966] 115 CLR 266 at 303, per Kitto J*). In another more recent case, *Da Silva [2006] EWCA Crim 1654*, ‘It seems to us that the essential element in the word “suspect” and its affiliates, in this context, is that the defendant must think that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice.’
- 2.29 *Money laundering* occurs only when *criminal property* has accrued to someone from a criminal act. In addition, it must be borne in mind that for property to be *criminal property* not only must it constitute a person’s benefit from *criminal conduct*, but the alleged offender (ie, the person alleged to be laundering *criminal property*) must know or suspect that the property constitutes such a benefit. This means, for instance, that if someone has made an innocent error, even if such an error resulted in benefit and constituted a strict liability criminal offence, then the proceeds are not *criminal property* for the purposes of *POCA* and no *money laundering* offence has arisen until and unless the offender becomes aware of the error (eg, s167(3), Customs and Excise Management Act 1979). *MLROs* need to consider carefully before reporting whether the information or other matter they intend to report meets these criteria. Examples of unlawful behaviour which may be observed, and may well result in advice to a *client* to correct an issue, but which are not reportable as *money laundering* are given below:

- offences where no proceeds or benefit results, such as the late filing of company accounts. However, *businesses and individuals* should be alert to the possibility that persistent failure to file accounts could represent part of a larger offence with proceeds, such as fraudulent trading or credit fraud involving the concealment of a poor financial position.
- misstatements in tax returns, for whatever cause, but which are corrected before the date when the tax becomes due.
- attempted frauds where the attempt has failed and so no benefit has accrued (although as this may still be a Fraud Act offence in England, Wales and Northern Ireland or the common law offence of fraud in Scotland, *individuals* and *businesses* may wish to consider reporting to their local police force or, once operational, the 'National Fraud Reporting Centre'). This includes '419' <sup>1</sup>letters and other attempted advanced fee frauds where there is no knowledge of benefit accruing. In the case of such letters, *individuals* and *businesses* may wish to consider following the guidance on the Metropolitan Police Fraud Alert internet pages ([www.met.police.uk/fraudalert](http://www.met.police.uk/fraudalert)).

Where a *client* refuses to correct, or unreasonably delays in correcting, an innocent error that gave rise to proceeds and which was unlawful, *businesses* should consider what that indicates about the *client's* intent and whether the property has therefore now become *criminal property*.

## Reasonable grounds for knowledge or suspicion

- 2.30 *Individuals* in the *regulated sector* must make an *internal report* or a *SAR*, as applicable, if there are 'reasonable grounds' for knowledge or suspicion, as well as actual knowledge or suspicion. This 'reasonable grounds' test creates an objective test – persons in the *regulated sector* will not be able to rely on an assertion of ignorance or naivety where this would not be reasonable to expect of a person with their training and position. For example, a person might be considered to have reasonable grounds for knowledge of *money laundering* if he had actual knowledge of, or possessed information which would indicate to a reasonable person, that another person was committing or had committed a *money laundering* offence; or had deliberately ignored the obvious inference from information (ie., wilfully shutting one's eyes) known to him that another person was committing or had committed a *money laundering* offence. Please note that the interpretation of 'reasonable grounds' has not, as yet, been tested by the courts for the purposes of *POCA*.
- 2.31 'Reasonable grounds' should not be confused with the existence of higher than normal risk factors which may affect certain sectors or classes of persons. For example, cash-based *businesses* or complex overseas trust and company structures may be capable of being used to launder money, but this capability of itself is not considered to constitute 'reasonable grounds'.
- 2.32 Existence of higher than normal risk factors require increased attention to gathering and evaluation of 'know your *client*' information, and heightened awareness of the risk of *money laundering* in performing professional work, but do not of themselves require a report of suspicion to be made. For 'reasonable grounds' to come into existence, there needs to be sufficient information to advance beyond speculation that it is merely possible someone is laundering money, or a higher than normal incidence of some types of crime in particular sectors.
- 2.33 It is important that *individuals* do not turn a blind eye to information, but make reasonable enquiries such as a professional with their qualifications, experience and expertise might be expected to make in such a situation within the normal scope of their assignment or

---

<sup>1</sup> Otherwise known as 'Nigerian scam' letters or equivalent

client relationship, and draw a reasonable conclusion such as may be expected of a person of their standing. *Individuals* should exercise a healthy level of professional scepticism, and if unsure of the action that should be taken, consult with their *MLRO* or otherwise in accordance with their *businesses'* procedures. If in doubt, *individuals* should err on the side of caution and make a report to their *MLRO*.

---

## NON-COMPLIANCE WITH THE MONEY LAUNDERING REGULATIONS

- 2.34 It is a criminal offence for a *business* not to comply with the *2007 Regulations*, if it is within their scope. An offence may also be committed by any partner, director or officer of the *business*, who has consented to or connived at the non-compliance or where the non-compliance is attributable to his neglect.
- 2.35 The relevant offences are referred to below. *Individuals* and *businesses* should appreciate that there are a wide range of requirements in respect of which failure to comply could be considered to be a criminal offence.
- 2.36 The offences are set out in Regulation 45 and those which are relevant to the provision of *defined services* relate to:
- Regulation 7 – failure to apply *customer due diligence* measures
  - Regulation 8 – failure to apply ongoing monitoring of *business relationships* and *customer due diligence*
  - Regulation 9 – failure to comply with the requirements on timing of verification of identity of *clients* and any beneficial owner
  - Regulation 11 – continuing with transaction/*business relationship* where unable to apply *customer due diligence* measures
  - Regulation 14 – failure to apply enhanced *customer due diligence* and ongoing monitoring where required
  - Regulation 18 – failing to follow a direction made by HM Treasury under this regulation (directions where *FATF* applies counter-measures)
  - Regulation 19 – failure to keep the required records
  - Regulation 20 – failure to establish, maintain, monitor and manage the required policies and procedures
  - Regulation 21 – failure to take appropriate measures to provide the required training
  - Regulations 26, 27 – failures regarding certain registration procedures where the Commissioners (HMRC) are the supervisory body (not applicable to those supervised by a body listed in Schedule 3)
  - Regulation 33 – failure to comply with registration requirements specified by the Commissioners (not applicable to those supervised by a body listed in Schedule 3)
- 2.37 Further *Guidance* on compliance with the *2007 Regulations* is given in sections 3 to 7 below. [When Treasury approval has been obtained] the Court will be obliged to take into account compliance with this *Guidance*, in deciding whether an offence has been committed. Until HM Treasury approval is received, the Courts may take the *CCAB Guidance* into account.

## SECTION 3 - ANTI MONEY LAUNDERING SYSTEMS AND CONTROLS

### KEY POINTS

Under the Money Laundering Regulations 2007 (*2007 Regulations*) *businesses* are required to establish appropriate risk-sensitive policies and procedures in order to prevent activities related to *money laundering* and *terrorist financing* including those policies and procedures which provide for:

- identification and scrutiny of complex or unusually large transactions, unusual patterns of transactions with no apparent economic or lawful purpose and other activities regarded by the regulated person as likely to be of the nature of *money laundering* or *terrorist financing*;
- prevention of use of products favouring anonymity;
- determination of whether a *client* is a *PEP*;
- *customer due diligence*, ie, procedures designed to acquire knowledge about the firm's *clients* and prospective *clients* and to verify their identity as well as monitor *business relationships* and transactions;
- internal reporting including appointment of an *MLRO* to receive the *money laundering* reports required under the Proceeds of Crime Act 2002 (*POCA*) and the Terrorism Act (*TA 2000*) and a system for making those reports;
- record keeping, including details of *customer due diligence* and supporting evidence for *business relationships*, which need to be kept for five years after the end of a relationship and records of transactions, which also need to be kept for five years;
- internal control, risk assessment and management, compliance monitoring, management and communication; and
- in addition, *businesses* are required to take measures to make relevant employees aware of the law relating to *money laundering* and terrorist finance, and to train those employees in how to recognise and deal with transactions which may be related to *money laundering* or *terrorist financing*.

In order to ensure compliance is appropriately managed, *businesses* will need to ensure sufficient senior management oversight, appropriate analysis and assessment of the risks of *clients* and work/product types, systems for monitoring compliance with procedures and methods of communicating procedures and other information to personnel.

### INTRODUCTION

- 3.1 *POCA* offences may be committed not only by *individuals* and *businesses* in the *regulated sector* but by any person. In contrast, the *2007 Regulations* impose obligations on *businesses* in the *regulated sector* as to the systems and controls they need to have in place to meet the requirements of the UK anti-*money laundering* regime. Under these regulations, not only must each *business* put anti-*money laundering* systems and controls in place but it also has a duty to ensure that relevant staff are aware of these systems and are appropriately trained. *Businesses* are explicitly required to monitor and manage their compliance with the *2007 Regulations*, to ensure continued observation of the requirements.
- 3.2 *Individuals* involved in the failure of *businesses* to meet their obligations under the *2007 Regulations* may be subject to criminal sanction, as may the *business* itself. Criminal sanctions for breach of the *2007 Regulations* only apply directly to the *individuals* working within a *business* when their neglect, connivance or consent has led to the failure to comply by the *business*.

---

## THE REQUIREMENTS

3.3 The *2007 Regulations*' requirements of *businesses* are contained in the following Parts:

- *customer due diligence* (Part 2 of the *2007 Regulations*); and
- record-keeping, procedures and training (Part 3 of the *2007 Regulations*).

### Systems

3.4 The *2007 Regulations* place requirements on *businesses* to have in place a wide range of systems in order to prevent operations related to *money laundering* or *terrorist financing*. The requirements cover the following issues. Where a separate section of this *Guidance* deals in detail with this matter, this is shown after the relevant heading, the other matters are dealt with in this section:

- *customer due diligence* and ongoing monitoring (see section 5 of this *Guidance*);
- reporting procedures (see sections 6 and 7 of this *Guidance*);
- record-keeping;
- internal control;
- risk assessment and management (see section 4 of this *Guidance*);
- compliance management; and
- communication.

3.5 The level of detail in the *2007 Regulations* as to what the requirements mean varies considerably, with *customer due diligence* being explained in some detail in Part 2 of the *2007 Regulations*, and with some detail being provided in respect of internal reporting procedures (Regulation 15) and record-keeping (Regulation 19). The *2007 Regulations* are less comprehensive on what is expected in respect of internal control, risk assessment and management, compliance management and communication.

3.6 *Businesses* need to establish systems that create an internal environment or culture in which people are aware of their responsibilities under the *UK anti-money laundering* regime and where they understand that they are expected to fulfil those responsibilities with appropriate diligence. In deciding what systems to install, a *business* will need to consider a range of matters including:

- the type, scale and complexity of its operations;
- the number of different business types it is involved in;
- the types of services it offers, and its *client* profiles;
- how it sells its services;
- the type of business transactions it becomes involved in or advises on;
- and the risks associated with each area of its *business* in terms of the risks of the *business* or its services being used for *money laundering* or terrorist operations, or the risks of its *clients* and their counterparties being involved in such operations.

3.7 *Businesses* should allocate responsibility for internal controls and effective risk management to a member of senior management, and should also ensure that the appointed *MLRO* has sufficient seniority and authority to carry out his task, whether or not these two functions are held by the same person. All *businesses* will need systems and controls, appropriate to the size and nature of their *business*, sufficient to achieve the following:

- determination and recording of the firm's systems for *anti-money laundering* awareness, *client* acceptance, *customer due diligence* and on-going monitoring requirements (including whether a customer is a *PEP*), consultation with and internal

reporting to the *MLRO* (where applicable – sole practitioners with no staff and no associates are not required to have internal reporting procedures or an *MLRO*), and dissemination of such policies and procedures to all relevant staff;

- development and documentation of the firm’s risk assessment of its *business*;
- training of all relevant staff, including systems and controls to ensure training is taken/attended and understood;
- methods for identification of topical update material and its dissemination as appropriate to senior management and other personnel;
- systems for periodic testing that policies and procedures comply with legislative and regulatory requirements;
- monitoring the compliance of the *business* with the policy and procedures including reporting to senior management on compliance and addressing any identified deficiencies.

3.8 In addition, *businesses* are recommended to maintain the following additional systems, for effective internal control and risk management:

- detailed documentation of policies and procedures in relation to matters not routinely a matter for *client* facing staff, such as *customer due diligence* for higher risk *clients*; information provision to senior management, training, awareness and compliance monitoring, and the role of the *MLRO*;
- provision in new product/service development processes for consideration of new services or business areas from an anti-*money laundering* perspective, and update of policy and procedure where appropriate;
- consideration at appropriate intervals of the *business* profile and whether the firm’s risk assessment and/or policy and procedures require updating in response.

Appropriate systems might also include a policy of acceptance of new *clients* being reserved to partners or other senior personnel, who may wish to refer to the *MLRO* for advice, if it is proposed to accept *clients* from outside the usual and well understood *client* base of the firm.

## Record-keeping

3.9 Records must be kept of *clients’* identity, the supporting evidence of verification of identity (in each case including the original and any updated records), the firm’s *business relationships* with them (ie., including any non-engagement related documents relating to the *client* relationship) and details of any occasional transactions and details of monitoring of the relationship. These records must be kept for five years after the end of the relevant *business relationships* or completion of the transactions. Care is needed to ensure retention of historic, as well as current records. *Businesses* are also recommended to store securely information relating to both *internal reports* and *SARs* for at least the same period, ie., at least five years after receipt by the *MLRO*. Documentation of reports is dealt with in further detail in section 7 below. Shown below is a summary of record-keeping requirements specified in the *2007 Regulations* for *customer due diligence* and *business relationships/occasional transactions* and *Guidance* in respect of retention of internal reporting procedures and training records for which specific guidance is not given in the *2007 Regulations*.

Record	Retention period	Comments
<b>Specified in the 2007 Regulations</b>		

i) <i>Client</i> identification, including evidence of identity	<b>5 years</b> from end of <i>business relationship</i> . <sup>2</sup>	Care should be taken to ensure that records are not destroyed by one department, while another is still within the five year retention period or has undertaken new business with the <i>client</i> . Where a <i>business</i> is engaged with several different activities with a <i>client</i> , it may decide to keep details of <i>customer due diligence</i> within each part of the firm so engaged, or to maintain central files, depending on its internal organisation. Evidence of <i>client</i> identity can be held in a variety of forms, eg, in hard copy or in electronic form in accordance with the document retention policies employed within the <i>business</i> .
ii) <i>Business relationships</i>	<b>5 years</b> from the date when all activities in relation to the <i>business relationship</i> were completed - except in the case of particular transactions within that <i>business relationship</i> the retention period is 5 years from the date on which the transaction was completed	Records of <i>business relationships</i> and occasional transactions (ie,. client assignment working papers and related documents) also need to be maintained for 5 years from the end of the relationship or transaction. For particular transactions within a <i>business relationship</i> , the records for the particular transaction need only be retained for 5 years from the completion of that transaction. In the context of provision of <i>defined services</i> it would be reasonable to treat each engagement or assignment as a 'particular transaction'. As <i>businesses</i> will need to maintain records for a wide range of purposes that comply with both legal and professional requirements for retention of documentation, it is not anticipated that any special system should be needed but that the general document retention systems employed within the <i>business</i> , provided they meet these standards, should be sufficient.
<b>Not specified in the 2007 Regulations</b>		
iii) Suspicious activities	Not prescribed	Records of <i>internal reports</i> , the <i>MLRO</i> 's consideration of them, any subsequent reporting decision and issues connected to consent, production of documents etc are a vital record as they may form the basis of a defence to accusations of <i>money laundering</i> and related offences. For this reason, it is recommended that such records are retained for at least 5 years after being made and possibly longer, at least whilst the <i>business relationship</i> continues. Records of <i>internal reports</i> are not considered to form part of <i>client</i> assignment working papers and so it is recommended that such records are kept, in a secure form separately from the <i>businesses</i> ' normal methods for retaining <i>client</i> work documents. This is to guard against inadvertent disclosure to any party who may have or seek access to the <i>client</i> working paper files where the existence of otherwise of an <i>internal report</i> or <i>SAR</i> is not relevant to the purpose for which they are examining the files.
iv) Training	Not prescribed	We recommend that evidence of assessment of training needs and steps taken to meet such needs is retained. <i>Businesses</i> should determine a retention

<sup>2</sup> As well 'business relationship', the 2007 Regulations refer to 'occasional transactions', ie, those outside the *business relationship* valued at over €15,000. 'Occasional transactions' is a cogent term in a banking context but is difficult to apply in the context of *accountancy services*. Therefore this *Guidance* uses only '*business relationship*', a more natural term for *accountancy and related services*, throughout.

period in the light of their normal retention period for training and other internal records, but we recommend they be kept for at least 5 years in order to demonstrate a continuing compliance with current and previous regulations.

## Reporting procedures

- 3.10 A *business's* internal procedures should clearly set out what is expected of *individuals* who form suspicions or obtain knowledge of possible *money laundering*. The reports can take any form specified by the *business* in internal procedures, eg, phone calls, emails, in writing, supplemented by copies of third party documents and working papers but *businesses* should ensure that, whatever forms the reporting takes, relevant personnel are aware of the procedures to be used. Consideration should be given to how to minimise the number of copies of reporting information held within a *business*. *Businesses* may wish to consider whether it is advisable to specify telephone or face to face contact with the *MLRO* as the preferred initial reporting step, with the reporting records being created by the *MLRO*, supplemented as necessary with copy information from *client* files.
- 3.11 It is recommended that all details of *internal reports* are held by the *MLRO* and excluded from *client* files. The duty to report is a matter which does not fall within the delivery of professional services to *clients* and accordingly reporting details are not required to be placed on *client* files. Exclusion of information from *client* files assists in avoiding inadvertent or inappropriate disclosure of information and provides some protection against the threat of *tipping off*. *Client* files should retain only that information relevant to, and required for, the professional work being undertaken. It should be noted that *anti-money laundering supervisory authorities* have an obligation under Regulation 24 (2) to make reports of suspicion. However, the law is not clear as to the interaction of the *POCA privilege reporting exemption* (Section 7.26-7.46) and the 2007 *Regulations* and unless this is resolved, there remains the risk of an *anti-money laundering supervisory authority* reporting a matter that was properly the subject of the *privilege reporting exemption*. Keeping internal reporting papers separate from *client* files may assist in mitigating this risk but is not a complete solution.
- 3.12 Further *Guidance* is given for *individuals*, on forming suspicions and making *internal reports* is given in section 6 and *Guidance* for *MLROs* in checking and validating *internal reports* and making *SARs* to *SOCA* in section 7.

## Communication and Training

- 3.13 The 2007 *Regulations* provide that all 'relevant' employees are required to be 'made aware' of law relating to *money laundering* and *terrorist financing*, and regularly given training in how to recognise and deal with transactions which may be related to *money laundering* or *terrorist financing*. Though the 2007 *Regulations* contain no express requirement, it is considered to be best practice for these provisions to be applied to all partners in firms and to sole practitioners and it is likely to be necessary to train all *client-facing* staff (see section 3.15 below).
- 3.14 In considering a training plan, *businesses* need to keep in mind the objectives they are trying to achieve, which is to create an environment effective in preventing *money laundering* and which thereby helps protect *individuals* and the *business*.
- 3.15 When considering which staff may be considered relevant, *businesses* should consider not only those who have involvement in *client* work, but also, where appropriate, those who deal with the *business* finances, and those who deal with procuring services on behalf of the *business* and who manage those services. Accordingly, it is likely that all

*client*-facing staff will be considered relevant and at least the senior support staff. *Businesses* may decide to provide comprehensive training to all relevant staff members, or may choose to tailor its provision to match more closely the role of the employees concerned. In particular, *MLROs* may require supplementary training, and members of senior management may also benefit from a customised approach or some supplementary training.

- 3.16 A training programme for relevant staff needs to contain content on the law and content which puts this into the context in which the *business* operates, to enable recognition of suspected *money laundering* in that context, and which illustrates the 'red flags' which staff should be aware of in conducting business. The core elements of law making up the UK anti-*money laundering* and anti-terrorism regime, are set out in this *Guidance* ( in particular in section 2). In addition, *businesses* may wish to include reference to other elements of law where criminal penalties may be applied and where these relate directly to the work of the *individual* or *business*, eg, an *FSA* approved person might be expected to have a reasonable working knowledge of the parts of *FSMA 2000* relevant to his work. Whilst it is not necessary for relevant personnel to develop a specialist knowledge of criminal law in general, they may reasonably be expected to apply the general legal and business knowledge which might normally be held by a person of their role and experience in determining whether to make a report to the *MLRO*.
- 3.17 Training also needs to cover how to deal with transactions which might be related to *money laundering* and *terrorist financing*. This would include training on the *businesses'* internal consultation and advisory systems (to assist *individuals* in assessing whether they have a valid suspicion) internal reporting systems and the *businesses'* expectations for confidentiality and the avoidance of *tipping off* and *alerting a money launderer*. Further *Guidance* on recognising *money laundering* by those undertaking *defined services* is given in section 6.
- 3.18 As regards the frequency of training, this is a matter for each *business* to consider. It may be influenced by changes in law, regulation or professional guidance, by new case law or national/international findings, or by a change in the profile and perceived risks of the *business*. Each *business* should consider the frequency of its training, possibly on an annual basis, and document its assessment as to whether the current training and state of awareness of employees is sufficient, or whether a supplement is needed. It may not be necessary to repeat the whole of a training programme on a regular basis, but it may be possible to provide concise update material which accomplishes the dual role of refreshing or expanding knowledge and generally reminding staff of the importance of effective anti-*money laundering* work.
- 3.19 Training methods may be selected to suit the size, complexity and culture of the *business*, and may be delivered in a variety of ways including face to face, self-study, e-learning and video, or a combination of methods. *Businesses* should keep records of attendance at, or completion of, training and are recommended to provide for some form of test or other confirmation of understanding of the training.
- 3.20 Should a *business* fail to make provision for the training of relevant employees, then under s330 (7), *POCA* a member of staff who does not know or suspect someone is engaged in *money laundering* gains a defence against the failure to disclose offence (ie, if there is only reasonable grounds for knowledge or suspicion and the staff member fails to make an *internal report*). However, such an omission is likely to open the *business* to the risk of prosecution for breach of the *2007 Regulations*. The significance of training records to both *individuals*, and *businesses* is reflected in the recommendation in section 3.9.
- 3.21 *Businesses* need to make arrangements to ensure new staff are trained as soon as possible after they join the *business*.



## SECTION 4 – THE RISK BASED APPROACH

### KEY POINTS

- A risk based approach allows *businesses* to target resource and effort where the risk is greatest and, conversely, reduce requirements where the risk is low.
- *Businesses* must establish adequate and appropriate policies and procedures relating to risk assessment and management in order to prevent operations related to *money laundering* or *terrorist financing*.
- *Businesses* must—
  - (a) determine the extent of *customer due diligence* measures (section 5) on a risk-sensitive basis depending on the type of *client*, *business relationship*, or services to be provided;
  - (b) be able to demonstrate to their *anti-money laundering supervisory authorities* that the extent of *customer due diligence* measures is appropriate in view of the risks of *money laundering* and *terrorist financing*.
- *Businesses* are required to take a risk-based approach and have adequate measures to verify the identity of beneficial owners so that they are satisfied that they know who the beneficial owner is and what the control structure is in respect of a *client* who is other than a natural person (Regulation 5(1)(b)).
- *Businesses* are required to undertake scrutiny of transactions and other activities throughout the course of a *business relationship* to ensure consistency with *businesses' and individuals' knowledge* of the *client*, his business and risk profile.
- *Businesses* must also keep up-to-date the information collected in applying *customer due diligence* measures.
- *Businesses* must apply *customer due diligence* measures at appropriate times to existing *clients* on a risk-sensitive basis.

---

## RISK ASSESSMENT AND MANAGEMENT

### Policies and Procedures

- 4.1 All *businesses* must have appropriate policies and procedures for assessment and management of the risk of the *business* being used for *money laundering*, of failing to recognise it where it occurs and report it when required. A risk-based approach to *anti-money laundering* incurs cost which is proportionate to this risk, focusing effort where it is needed and has most impact.
- 4.2 Professional firms are likely to already have in place policies and procedures to minimise professional, *client* and legal risk. *Anti-money laundering* procedures and policies may be integrated into existing risk management systems or be controlled separately. In either case, *anti-money laundering* policies and procedures should be valuable to *businesses*, in contributing to the control of risks to both *businesses* and *individuals* in this and other areas.

### Risk profile

- 4.3 The development of a *money laundering* risk profile for the *business* enables a risk-based policy and approach to be developed, and thus to determine the most cost effective and

proportionate way to manage and mitigate the *money laundering* and *terrorist financing* risks faced by the *business*. The risk profile of a *business* is determined by:

- identifying the *money laundering* and *terrorist financing* risks that are relevant to the *business*; and
- designing and implementing controls to manage and mitigate these risks, and record their operation.

## Managing compliance

- 4.4 *Businesses* are required to monitor and manage their compliance with and internal communication of their policies and procedures and this includes their systems for risk assessment and management, as well as their other anti-*money laundering* policies and procedures (Regulation 20 (1)). All such systems should be managed through monitoring the operation of the controls, updating them where necessary and assessing whether they have been effective. *Businesses* may come into contact with activity in the *client's* business which they perceive as likely, by its nature, to be related to *money laundering* or *terrorist financing* (in particular, complex or unusually large transactions and all unusual patterns of transactions which have no apparent economic or visible lawful purpose). In those circumstances, *businesses* have a duty to pay special attention to such an activity.
- 4.5 *Businesses* can decide for themselves how to carry out their risk assessment, which may be simple or sophisticated depending on the nature of their practice. Where the practice is simple, involving few service lines, with most *clients* falling into similar categories, a simple approach may be appropriate for most *clients*, with the focus being on those *clients* that fall outside the norm.
- 4.6 A risk-based approach can never, by its nature, be an error-free system. However, it ensures the most cost effective results by directing the attention of *businesses* to the risks relating to different *clients* and services, in order to determine what level of knowledge and verification is required when establishing a *business relationship* and in conducting that relationship.

---

## THE RISK-BASED APPROACH

- 4.7 Each *business* needs to make a reasoned decision as to how it intends to manage *money laundering* risk. A risk-based approach does, however, enable a *business* to target its effort on conducting *customer due diligence* more effectively with increased depth of work being conducted where the risks are perceived, on a rational basis, to be higher.
- 4.8 Senior management engagement and commitment is needed to produce and embed a successful risk-based approach, and it also needs effective communication to all staff members who need to use it.
- 4.9 *Businesses* may assess the *money laundering* risks of:
- different products and services,
  - *client* types and sectors, and
  - the jurisdictions of *client* origin, funding, investment and conduct of business.

and apply a simple risk categorisation of low/normal/high on the basis of these categories. Such an approach is valid, and should be capable of minimising complexity, but needs to retain an element of discretion and flexibility where risk ratings may be raised or lowered with appropriate management input in response to particular or exceptional circumstances.

- 4.10 *Businesses* may also wish to consider the different types of risk to which they are exposed. These risks may include
- being used in an active sense to launder money through the handling of cash or assets,
  - becoming concerned in an arrangement which facilitates *money laundering*, through the provision of investment services or the provision of trust or company services.
  - risks attaching to the *client* and/or those who trade with or otherwise interact with *clients* as regards their potential for involvement in *money laundering*.
- 4.11 A simple matrix prepared from a risk-assessment of the factors considered above may be prepared to provide a basic framework for the categorisation of *clients* and engagements, and to direct the depth and type of *customer due diligence* accordingly.
- 4.12 Chapter 4 of the *JMLSG Guidance* notes provides useful additional guidance on the risk-based approach

#### **Developing and applying a risk based approach**

- 4.13 In developing a risk-based approach, *businesses* need to ensure it is readily comprehensible and easy to use for all relevant staff. In cases of doubt or complexity, *businesses* may wish to consider putting in place procedures where queries may be referred to a senior and experienced person, eg, the *MLRO* for a risk-based decision which may vary from standard procedures.
- 4.14 To develop the approach it is necessary to review the *business* and consider what *money laundering* risks might attach to each service type, *client* type etc. One way to consider this in relation to the *defined services* is outlined below, but there are other approaches that may be equally or more valid depending on the type of *business*.
- 4.15 *Businesses* should consider first the type of risk presented:
- is the risk that the *business* might be used to launder money or provide the means to launder money? Examples might include handling *client* money, implementing company and trust structures, handling insolvent estates where assets are tainted by crime etc.
  - is the risk that the *client* or its counterparties might be involved in *money laundering*? Examples might include *clients* who are *PEPs* (see section 5.27), or who are high profile and attract controversy or adverse comment in the public domain, or who are involved in higher risk sectors and jurisdictions (eg, those where corruption is known to be a higher risk), or who are known to be potentially involved in illegal activities, such as tax evaders seeking advice to resolve their affairs, and certain forensic work connected with fraud or other crime etc.
- 4.16 Consideration of these risk types should enable the *business* to draw up a simple matrix of characteristics of the *client* or service which are considered to present a higher than normal risk, and those which present a normal risk. Some may, by long acquaintance and detailed knowledge, or by their status (eg, listed, regulated and government entities as defined for the purpose of *simplified due diligence* in the *2007 Regulations*) be considered to present a lower than normal risk.
- 4.17 This matrix can then be incorporated into *client* acceptance procedures, and as step 1 of the *customer due diligence* process, allows a *money laundering* risk level to be assigned to ensure appropriate, but not excessive, *customer due diligence* work is carried out.

- 4.18 It is important for the approach adopted to incorporate a provision for raising the risk rating from low or normal to high if any information comes to light in conducting the *customer due diligence* that causes concern or suspicion.
- 4.19 In all cases, even where *clients* qualify for *simplified due diligence* under the terms of the *2007 Regulations*, or where they are considered low risk for other reasons, to assist in effective ongoing monitoring *businesses* should gather knowledge about the *client* to allow understanding of:
- who the *client* is
  - where required, who owns it (including ultimate beneficial owners – see section 5.6)
  - who controls it
  - the purpose and intended nature of the *business relationship*
  - the nature of the *client*
  - the *client's* source of funds
  - the *client's* business and economic purpose.
- 4.20 The information specified in the bullet points above are referred to in the remainder of this *Guidance* as 'know your client' or 'KYC' information which is one step in the *customer due diligence* process. However, *businesses* may avail themselves of the opportunity to conduct verification of identity on a simplified basis both under the terms of the *2007 Regulations*, where applicable, and otherwise where the accumulated knowledge of the *client* is considered sufficient to prove its identity on a risk-sensitive basis without collecting additional documents as might be required for a new *client* considered to present a normal risk (provided in both cases that any relevant requirements of the *2007 Regulations*, for example in relation to the identification of beneficial owners, are met).
- 4.21 *Businesses* need to set out clear requirements for collecting KYC information about the *client* and for conducting verification of identity, to a depth suitable to the assessment of risk. Set out in this *Guidance* are some high level guidelines as to how *businesses* might approach this. More detailed *Guidance* is contained in the *JMLSG Guidance* notes, Chapters 4 and 5.

## SECTION 5 – CUSTOMER DUE DILIGENCE

### KEY POINTS

- Effective '*customer due diligence*' measures are an essential part of any system designed to prevent *money laundering* and are a cornerstone requirement of the Money Laundering Regulations 2007 (*2007 Regulations*).
- *Businesses* should take a **risk-based approach** to allow effort to be concentrated on higher risk areas (**also see section 4**). Risks must be assessed before the appropriate level of *customer due diligence* can be applied.
- *Customer due diligence* measures need to be carried out:
  - \* when establishing a *business relationship*,
  - \* when carrying out an occasional transaction,
  - \* where there is a suspicion of *money laundering* or *terrorist financing*; and
  - \* where there are doubts concerning the veracity of previous identification information.
- *Businesses* are required to ensure *customer due diligence* procedures are applied to all *clients*, both new and existing. *Customer due diligence* must be applied to existing *clients* (ie those existing prior to the *2007 Regulations* coming into force) at appropriate times on a risk-sensitive basis.
- **Before** entering a *business relationship*, *businesses* must:
  - \* identify and verify the *client's* identity using documents or information from reliable and independent sources.
  - \* identify the beneficial owner of the *client* (where required), including understanding the ownership and control structure of the *client* and verifying, according to risk, the identity of the beneficial owner(s).
  - \* obtain information on the purpose and intended nature of the *business relationship*.
- Verification of identity may in certain circumstances be conducted during the establishment of a *business relationship* if this is necessary not to interrupt the normal course of business and there is little risk of *money laundering* or *terrorist financing* occurring, provided the verification is completed as soon as practicable after contact is first established.
- **During** a *business relationship*, *businesses* must monitor activity on an ongoing basis. This includes scrutiny of transactions, source of funds and other elements of knowledge collected in the *customer due diligence* process, to ensure the new information is consistent with other knowledge of the *client* and keeping the documentation concerning the *client* and the relationship updated.
- *Businesses* can use a variety of tools and methods to conduct *customer due diligence*; the onus is on them to satisfy themselves and to be able to demonstrate to their *anti-money laundering supervisory authority* the appropriateness of their approach.

---

## WHY IS THIS IMPORTANT?

- 5.1 *Customer due diligence* measures are a key part of the anti-money laundering requirements. They ensure that *businesses* know who their *clients* are, ensure that they do not accept *clients* unknowingly which are outside their normal risk tolerance, or whose business they will not understand with sufficient clarity to be able to form *money laundering* suspicions when appropriate. If a *business* does not understand its *client's* regular business pattern of activity it will be very difficult to identify any abnormal business patterns or activities. In addition *businesses* must be in a position to supply the *client's* identity to SOCA should that *client* become the subject of a SAR.
- 5.2 Many *businesses* will have other procedures for *client* acceptance, for example to ensure compliance with professional requirements for independence and to avoid conflicts of interest. The requirements of the *2007 Regulations* may either be integrated with those procedures or addressed separately. In either case, initial *customer due diligence* information not only assists in acceptance decisions, but also enables the *business* to form well-grounded expectations of the *client's* behaviour which provides some assistance in detecting potentially suspicious behaviour during the *business relationship*.
- 5.3 The processes required for compliance with anti-money laundering initial *customer due diligence* requirements contribute vitally to the overall picture of potential *clients* and appropriate risk assessment of them. However, a lack of concern raised during *customer due diligence* does not automatically mean that the *client* and engagement will remain in their initial risk category. Continued alertness for changes in the nature or ownership of the *client*, its business model, or its susceptibility to *money laundering* – or actual evidence of the latter - must be maintained.

---

## WHAT IS CUSTOMER DUE DILIGENCE?

- 5.4 The *2007 Regulations* provide an outline of the required components of *customer due diligence* which *businesses* need to ensure are integrated into *client* acceptance processes and the continuing conduct of the *business relationship*. The required components are:
- identifying the *client* (ie, knowing who the *client* is) and verifying the identity of the *client* (ie, confirming that identity is valid by obtaining documents or other information from sources which are independent and reliable);
  - identifying the beneficial owner(s) (see section 5.6) of a *client*, if there is one, so that the identity of the individual(s) who is the ultimate owner or controller is known, the ownership and control structure is understood and also that their identities are verified, as required, on a risk-sensitive basis; and
  - information on the purpose and intended nature of the *business relationship*.
- 5.5 Whilst the *2007 Regulations* do indicate some cases where either *simplified due diligence* may be employed or *enhanced due diligence* must be employed, they do not specify, comprehensively, how to apply a risk-based approach in conducting *customer due diligence*. Section 4 of this *Guidance* provides a high level outline of the key elements of a risk-based approach. If further detail is required it is recommended that reference is made to the *JMLSG Guidance* notes which cover the subject in depth and, as HM Treasury approved *Guidance* for the financial services industry, may be considered as a reliable additional source of information in supplement to this *Guidance*.

---

## WHAT IS A BENEFICIAL OWNER?

- 5.6 The *2007 Regulations* set out in some detail the meaning of 'beneficial owner' in terms of bodies corporate, partnerships, trusts and other legal entities/arrangements not falling

into the three categories listed above as well as special provisions regarding estates of deceased persons and a catch all provision that, where not otherwise specified, defines the beneficial owner as the person who ultimately owns or controls the *client* or on whose behalf a transaction is being conducted. The provisions regarding beneficial ownership are set out in Regulation 6 and are summarised below:

- **Bodies corporate** –beneficial owner means any individual who, in respect of any body other than a company whose securities are listed on a *regulated investment market*, owns or controls, directly or indirectly including through bearer share holdings, more than 25% of the shares or voting rights in the body or who otherwise exercises control over the management of the body.
- **Partnerships** (other than limited liability partnerships established under the Limited Liability Partnerships Act 2000) - beneficial owner means any individual who ultimately is entitled to or controls (directly or indirectly) more than 25% of the capital or profits of the partnership or more than 25% of the voting rights in the partnership or who otherwise exercises control over the management of the partnership.
- **Trusts** - beneficial owner means any individual who is entitled to a *specified interest* in at least 25% of the capital of the trust property, or where a trust is not set up entirely for the benefit of persons with a *specified interest*, the class of persons in whose main interest the trust is set up or operates or any individual who has control (*a trust controller*) over the trust. Where a class of persons is identified, it is not a requirement for all members of that class to be separately identified.
- **Other entities and arrangements** (meaning an entity or arrangement which administers and distributes funds) – where the individuals who benefit from the entity or arrangement have been determined, beneficial owner means any individual who benefits from at least 25% of the property of the entity or arrangements. Where those benefiting have yet to be determined, beneficial owner means the class of persons in whose main interest the entity or arrangement is set up or operates or an individual who exercises control over at least 25% of the property of the entity or arrangement. Where a class of persons is the beneficial owner, it is not a requirement for all members of that class to be separately identified. Note that where an individual is the beneficial owner of a body corporate which benefits from, or exercises control over, the property of an entity or arrangement, the individual is to be regarded as having that benefit or control and so is classed as the beneficial owner.
- **Estates of deceased persons** – the beneficial owner is considered to be the executor or administrator of the estate (full detail is shown in Regulation 6(8)).

5.7 The focus on identifying and, where appropriate, verifying the identity of beneficial owners is not only an important element of the required *customer due diligence* information, but is also an important factor in an effective risk-based approach to *client* acceptance. *Businesses* will need to be diligent in their enquiries in this field, taking into account that information may sometimes not be readily available from public record sources. This will necessitate a flexible approach to information gathering which will often involve direct enquiry of *clients* and their other advisers and professional service providers as well as undertaking public record searches in the UK and overseas.

---

## APPLICATION AND TIMING OF CUSTOMER DUE DILIGENCE MEASURES (WHEN)

5.8 Identification and verification of identity procedures (together termed as “ID procedures”) should normally be completed **before** entering into a *business relationship*. This applies also to occasional transactions. ID procedures are also required at other times, for example, when there is a suspicion of *money laundering* or *terrorist financing* or where there are doubts about the sufficiency of identification information already held. If it is

concluded the information held is insufficient, the *business* should remedy this as soon as is practicable. Should a suspicion be developed about the *client*, *businesses* will need to consider whether they are satisfied that the information already held is sufficient and up to date or whether any additional or updated information is required in respect of the *client(s)* in question in order that the information required by Regulation 5 (customer due diligence) is met. In particular, in any case where suspicion is developed, *simplified due diligence* may no longer be applied. This means if *simplified due diligence* had been applied, additional information will need to be collected in accordance with *businesses'* risk-based procedures. *Businesses* must bear in mind in conducting this *customer due diligence* work the need to avoid disclosing that a *money laundering* report has been made, or that an investigation is underway, or may be commenced (see section 2.17-2.21 Tipping Off).

- 5.9 The *2007 Regulations* allow for completion of ID procedures 'during the establishment of a *business relationship*' rather than before if the measures are completed as soon as practicable after the initial contact **but only** when such a process is necessary not to interrupt the normal conduct of business and there is little risk of *money laundering* or *terrorist financing* occurring. *Guidance* on how this might reasonably be applied in the case of provision of the *defined services* is provided below, although this is not intended to be prescriptive, or exclusive. *Businesses* should not complete any assignment for a *client* (eg ,including transfer of *client* monies or delivery of work product) before *customer due diligence* has been carried out in full in accordance with the *businesses'* procedures.
- 5.10 If procedures are not completed before entering a *business relationship*, *businesses* and their *clients* may suffer considerable cost and inconvenience in having to terminate a relationship if ID procedures either cannot be completed, or where the results are unsatisfactory.
- 5.11 *Customer due diligence* should also be completed before undertaking occasional services for the *client* that do not form part of an ongoing *business relationship*. *Businesses* must understand why the *client* requires the service, the identities of other parties that might be involved, and any potential for *money laundering* that may arise.

#### When delay may be acceptable

- 5.12 In forming new *business relationships*, there are some cases where delay **may** be acceptable, such as in urgent insolvency appointments, and urgent appointments that involve ascertaining the legal position of a *client* or defending the *client* in legal proceedings.
- 5.13 In such cases, *businesses* should still gather enough information to allow them to at least form a basic assessment of the identity of the *client* and *money laundering* risk and to complete other acceptance formalities such as considering the potential for conflicts of interest.
- 5.14 In other cases, where the majority of information required has been collected before entering a *business relationship*, short time extensions to complete collection of remaining information may be acceptable, provided this is caused only by administrative or logistical issues, and not by any reluctance of the *client* to provide the information and is necessary not to interrupt the normal course of business. Such extensions should be exceptional, rather than the norm. It is recommended that such extensions of time are considered and agreed by a member of senior management or the *MLRO* to ensure the reasons for the extension are valid and do not give rise to concern over the risk category of the *client* or the potential for *money laundering* suspicion.
- 5.15 If evidence is delayed (rather than refused), *businesses* should consider;

- the credibility of the *client's* explanation,
- the length of delay,
- whether the delay is in itself reasonable grounds for suspicion of *money laundering* requiring a report to SOCA and/or a factor indicating against acceptance of the *client* and engagement, and
- documenting the reasons for delay and steps taken.

### Non-compliance through client refusal

- 5.16 If a prospective *client* refuses to provide evidence of identity or other information properly requested as part of *customer due diligence*, the *business relationship* or occasional transaction must not proceed any further and any existing relationship with the *client* must be terminated (but see sections 5.56 – 5.59 on insolvency cases). Consideration must be given as to whether a report needs to be made to SOCA under POCA or TA 2000
- 5.17 Where the appointment is of either a lawyer or *relevant professional advisor* in the course of ascertaining the legal position for the *client*, or performing the task of defending or representing the *client* in or concerning legal proceedings (including advice on instigating or avoiding proceedings) the requirement to cease acting and consider reporting to SOCA does not apply although *customer due diligence* information will still need to be collected within the time constraints in Regulation 9. *Businesses* are advised to consider the position very carefully before applying this exception to ensure that the type of work and their professional status fall within the definitions set out in Regulations 11(2) and (3).

### Continuing customer due diligence

- 5.18 In addition to considerations before entering a *business relationship*, *customer due diligence* must be exercised on an ongoing basis during the relationship, as part of regular monitoring of *money laundering* risks or occasioned by the *client* undergoing significant changes. *Businesses* may wish to consider reviewing *customer due diligence* and other *client* information on a periodic basis, as well as in response to perceived risks.
- 5.19 Changes such as the appointment of new senior managers or shareholders and/ or controlling parties, changes in the *client's* strategy or changes of business profile should prompt *businesses* to re-apply *customer due diligence* procedures. These may differ from those adopted for a new *client*, and although there may be a change in focus the objective remains the same: to have a sound understanding of the *client's* identity and activities in order to assess risks of *money laundering* and to have accurate underlying records.

---

## THE RISK BASED APPROACH TO CLIENT DUE DILIGENCE

- 5.20 Regulation 7(3) requires *customer due diligence* measures to be carried out on a risk-sensitive basis. This means that *businesses* need to consider how their risk assessment and management procedures (see section 3 above) flow through into their *client* acceptance and ID procedures, to give sufficient information and evidence, in the way most appropriate to the *business* concerned.
- 5.21 In addition, there are certain circumstances where the 2007 Regulations themselves lay down categories where *simplified due diligence* or *enhanced due diligence* is appropriate, according to national and international assessments of the risk of *money laundering*.

### Simplified due diligence

- 5.22 ‘*Simplified due diligence*’ is a phrase used in the 2007 Regulations (Regulation 13) which means that a *business* is not required to apply the *customer due diligence* measures laid out in Regulation 7, as set out in section 5.20 above, where the *business* has reasonable

grounds for believing that a *client* falls into the relevant categories. *Businesses* who may be permitted to apply the *simplified due diligence* exemptions but who perceive other than a low risk of *money laundering* in a specific case, should consider applying their standard or *enhanced due diligence* processes. In any case where a *client* or potential *client* has been subject to *simplified due diligence* and a suspicion of *money laundering* or *terrorist financing* arises in relation to that *client*, the *simplified due diligence* provisions must no longer be applied and the *customer due diligence* requirements of Regulation 7 must be applied, subject to any *tipping off* issues.

5.23 The main categories of relevance to those providing *defined services* are:

- *credit* or *financial institutions* subject to the provisions of the *money laundering directive* or equivalent overseas requirements,
- companies listed on a regulated EEA market or equivalent overseas requirements subject to *specified disclosure obligations*,
- UK public authorities and certain public authorities in the EU and EEA (see Schedule 2 paragraph 2).

*Simplified due diligence* is also available for some categories of products and transactions which may be provided by financial institutions.

5.24 *Businesses* should set out clearly in their internal procedures what is considered to constitute reasonable grounds for a belief that a *client* can be made subject to *simplified due diligence*. Evidence should be obtained either as to the regulated status of the *credit* or *financial institution* (such as a print out from the regulator's official web-site or listing), or the listed status of the company (such as a print out from the exchange's official web-site or listing, or details of the listing obtained from a trusted, independent commercial provider of company information). With regard to public authorities, recourse to official government web-sites is recommended. In each case, where the body is not subject to UK, EC or EEA law, justification will also need to be recorded as to how the provisions and other conditions regarding *specified disclosure obligations* in respect of listed companies, and the check and balance procedures and other conditions in respect of public authorities outside the UK, have been met. Recourse to information provided from time to time by the *JLMSG* is recommended [ref to *JMLSG* source]. Where *simplified due diligence* applies, *businesses* are not required to apply standard *customer due diligence* measures. However, *businesses* must still carry out ongoing monitoring (see section 5.46) and appropriate KYC information should therefore still be obtained (see section 4.19).

### **Enhanced due diligence**

5.25 A risk-based approach to *customer due diligence* will identify situations which by their nature can present a higher risk of *money laundering* or *terrorist financing*. Regulation 14 sets out a general provision that *enhanced due diligence* must be applied in such situations and means that the *business* must obtain additional *customer due diligence* information about the *client*.

5.26 The *2007 Regulations* also specify that *enhanced due diligence* must be applied in a number of situations, of which two are relevant to providers of *defined services* and are outlined below:

- if a *client* has not been physically present for identification purposes, and if so, one or more additional measures must be taken to *enhance due diligence*, for example by, inter alia, either gathering additional documents, data or information, or taking additional steps to verify documents or obtain a confirmatory certificate from a *credit* or *financial institution* subject to the *money laundering directive*; and

- if a *business relationship* or occasional transaction is to be undertaken with a *politically exposed person (PEP)* in which case the *business* must provide for senior management approval for the relationship to be established, must take adequate measures to establish the source of wealth and funds which are involved and must conduct enhanced monitoring of any relationship entered into.

### Politically exposed persons (PEPs)

- 5.27 The *2007 Regulations* define a *PEP* as a person ‘...who is or has, at any time in the preceding year been entrusted with a prominent public function by a state other than the United Kingdom, a community institution or an international body’ or a family member or known close associate of such a person. Details of what are considered to be prominent public functions are shown in Schedule 2, paragraph 4(1)(a). For risk management and reputational risk reasons, *businesses* may wish to treat as *PEPs* individuals who held such positions more than a year ago. As regards establishing whether someone is considered to be a family member or known close associate, regard need only be had to information in the public domain or in the possession of the *business*. ‘International body’ is not defined, and due consideration should be given to the type, reputation and constitution of the body before excluding it or its representatives from *enhanced due diligence*. However, bodies such as the United Nations, NATO and *FATF* may reasonably be included within the definition of an international body for this purpose.
- 5.28 Under the *2007 Regulations*, *clients* who are *PEPs* must always be subject to the *enhanced due diligence* measures referred to in section 5.26 above.
- 5.29 *Businesses* are required to have risk sensitive measures in place to recognise *PEPs*. This can be a simple check conducted by enquiring of the *client* and perhaps using an internet search engine. *Businesses* that are likely to regularly undertake services for *PEPs* may need to subscribe to a specialist database. To the extent possible, *businesses* should be aware of any news during a *business relationship* that could change a *client’s* status to *PEP*.

### Prohibited relationships

- 5.30 The *2007 Regulations* set out circumstances which constitute prohibited relationships. In Regulation 16, correspondent banking relationships with *shell banks*, or a bank known to permit use of its accounts by a *shell bank* are prohibited. In addition, set up of anonymous accounts in the UK is prohibited, and *customer due diligence* must be applied to any existing accounts continuing in existence after 15 December 2007 before such an account is used.
- 5.31 All *businesses* must pay special attention to services or, where relevant, products or transactions that might allow anonymity and take measures to prevent their use in *money laundering* or terrorist activity. *Businesses* must include any such product or transaction within those requiring *enhanced due diligence*.
- 5.32 In addition, *businesses* must comply with any prohibition issued by HM Treasury in respect of any person, or State to which the Financial Action Task Force has decided to apply counter-measures (see also section 5.44). Directions may be given not to enter into *business relationships*, carry out *occasional transactions* or proceed with any such arrangements already in progress.

### Reliance on third parties

- 5.33 *Businesses* may rely on third parties, subject to the third parties’ consent, to complete all or part of *customer due diligence* as set out below but they should be cautious in relying on third parties as they will remain liable for any failure to comply notwithstanding their

reliance on a third party (See Regulation 17). *Businesses* should consider requiring copies of relevant information and documentation from the third parties, in order that they may satisfy themselves the information is sufficient.

5.34 Reliance may be made on persons who are:

- regulated *credit or financial institutions* (excluding money service businesses);
- professional lawyers, auditors, *external accountants, insolvency practitioners or tax advisers*;

'professionals' in the second of these categories must be regulated by one of the *anti-money laundering authorities* listed in Schedule 3 to the *2007 Regulations*, or be subject to equivalent regulation in an EEA or non-EEA state including mandatory professional registration recognised by law and supervision for compliance with requirements equivalent to the *money laundering directive*. *Businesses* may outsource their *customer due diligence* measures but remain liable for any failure in the *customer due diligence*.

5.35 Information on equivalence is very limited at present, but further information should [shortly be published by HM Treasury following an EU study].

5.36 Before reliance may be placed on one of those specified above, the other *individual or business* must agree to reliance being placed. If consent is obtained, the *individual or business* consenting to the reliance must take great care to ensure they have adequate systems in place to keep proper records and to respond to any request for these.

5.37 An *individual or business* consenting to be relied upon must, if requested, make available to the person relying as soon as is reasonably practicable:

- any information obtained about the *client* (and any beneficial owner) when applying *customer due diligence* measures; and/or
- copies of any identification and verification data and other documents on the identity of the *client* (and any beneficial owner) obtained when applying *customer due diligence* measures.

5.38 Before placing reliance, an *individual or business* seeking to rely must take steps to ensure the person being relied upon will provide the required information.

5.39 Any *individual or business* consenting to be relied upon must ensure the records of *customer due diligence* which become the subject of reliance are retained for 5 years from the date on which reliance commences.

5.40 Failure by a person who has been relied upon to comply with the requirements in relation to responding to requests for information, relying upon a person without having ensured they will provide the information required on request, or failing to keep the records required after reliance has been allowed are all criminal offences as set out in Regulation 45.

Where reliance is placed on a third party, *businesses* are not required to apply standard *customer due diligence* measures. However, *businesses* must still carry out ongoing monitoring (see section 5.46) and appropriate KYC information should therefore still be obtained (see section 4.19).

5.41 Whilst reliance may be a useful and efficient feature of a *customer due diligence* system between parties who are able to build a relationship of trust, it should not be entered into lightly. *Individuals* and *businesses* need to consider carefully whether they wish to be relied upon and before so consenting ensure:

- their *client* (and any other third party whose information would be disclosed) has no objection to their information being passed to the person seeking reliance; and
- that they have in place the necessary record-keeping systems.

---

## CONDUCTING CUSTOMER DUE DILIGENCE

### ‘Know your client’ or ‘KYC’

- 5.42 The resources used to undertake effective *customer due diligence* are not prescribed. Various sources may be used to enhance a *business’* knowledge of their *client*, including direct discussion with the *client*, information (eg, websites, brochures, reports etc) prepared by the *client* and review of public domain information.
- 5.43 *Businesses* need to consider whether there are any particular steps they wish to specify for use in higher risk cases to increase the depth of *customer due diligence*, such as seeking out wider information from extensive internet and press searches concerning the potential *client*, its key counterparties, its sector and jurisdiction, or possibly using subscription databases which provide a quick way of accessing public domain information and in many cases provide links to persons or companies known to be associated with the potential *client* (see sections 5.54 to 5.55 on electronic identification).
- 5.44 *Businesses* might, as appropriate to their risk assessment, wish to check the names of new *clients* against lists of known terrorists and other sanctions information (HM Treasury maintains the UK list of these persons and *businesses* but recourse may be had to further lists such as those issued by the UN and the US Treasury Office of Foreign Assets Control or OFAC). Some electronic resources also include an automated check against this information as part of the product.

### Specific *customer due diligence* prompts

- 5.45 It may be helpful for a list of questions or prompts to be incorporated into *customer due diligence* procedures. Examples are given at the end of this section (section 5A) which should be amended to suit the particular *business’ client* base and services.

### Ongoing monitoring

- 5.46 Ongoing monitoring of the *business relationship* is required. This comprises scrutiny of activity during the relationship, including enquiry into source of funds if needed, to ensure all is consistent with expected behaviour based on accumulated *customer due diligence* information. In addition, it is required that the documentation concerning the relationship (including *customer due diligence*) is kept updated as laid out in Regulation 8, 2007 *Regulations*. The need to update *customer due diligence* information should be considered at appropriate times, following a risk based approach, according to the firm’s knowledge of the *client* and changes in its circumstances or the nature of services provided by the firm. A firm also may wish to consider this need, on a more routine basis, as appropriate opportunities arise. Examples of such opportunities are:
- at the start of new engagements and when planning for recurring engagements;
  - when a previously stalled engagement restarts;
  - whenever there is a change of control and/or ownership of the *client*;
  - when there is a material change in the level, type or conduct of business; and
  - where any cause for concern, or suspicion, has arisen (in such cases, care must be taken to avoid making any disclosure which could constitute *tipping off*).

### Risk-based verification

- 5.47 Application of a risk-based approach is of considerable importance in verification, both to ensure a good depth of knowledge in higher risk cases, but also to avoid superfluous effort in lower or normal risk cases. Very extensive information is contained in the *JMLSG Guidance* notes. Reference to this is recommended, particularly for overseas *clients*, or those *clients* who have a legal form other than that of a UK private or public company, a UK partnership or LLP, or a UK government body.
- 5.48 With the more frequently encountered *client* types, ie individuals, UK private or public companies, UK partnerships or LLPs, a UK regulated *business*, or a UK government body, outline *Guidance* on a risk based approach to verification of identity is set out at the end of this section (section 5B).

### **Documentary evidence used in the verification of identity (How)**

- 5.49 The purpose of verification of identity is to confirm and prove the information collected in so far as it relates to the identity of the *client*. Recourse to documents from independent sources is important. The amount of reliance that can be placed upon, and thus the strength of, particular forms of evidence varies.
- 5.50 The following are illustrative of a different of strength of various forms of documentary evidence starting with the highest:
- documents issued by a government department or agency or a Court (including documents filed at Companies House or overseas equivalent)
  - documents issued by other public sector bodies or local authorities
  - documents issued by *businesses* regulated by the Financial Services Authority or overseas equivalent
  - documents issued by professionals regulated for anti-*money laundering* purposes by the bodies listed in Schedule 3 of the *2007 Regulations* or overseas equivalents
  - documents issued by other bodies.
- 5.51 In the case of individuals, documents from highly rated sources that contain photo identification as well as written details are a particularly strong source of verification of identity.

### **Certification and annotation**

#### Certification

- 5.52 *Businesses* may wish to consider whether copies of original documents and copies of certified copies of original documents should be certified as true copies to demonstrate their provenance. *Businesses* may wish to create standard stamps or labels to apply to documents, which can then simply be filled in with name, signature and date. *Businesses* should have regard to the standing of the person certifying and may wish to consider specifying from whom certification may be accepted, for instance, *businesses* may decide to restrict acceptance to those documents certified by a person in the permitted categories for reliance (Regulation 17 of the *2007 Regulations*) which are broadly a credit or *financial institution* authorised by the *FSA*, a professionally qualified auditor, *external accountant*, *insolvency practitioner* or *tax adviser*, or *independent legal professional*, or their equivalent in EU countries and other countries which have equivalent law and provided in all cases that the person is subject to supervision as to his compliance with those requirements.

#### Annotation

- 5.53 This should be used when the document is as good as an original but is not the original itself. This particularly applies to printouts from the Internet, such as downloads from Companies House, regulator, stock exchange or government websites, or similar

trustworthy business information sources. Each document so obtained should bear written evidence showing who printed it, when, from where and should be signed by the relevant person.

## Electronic identification

- 5.54 There are now a number of subscription services that give access to databases of information on identity. Many of these services can be accessed on-line and are often used by *businesses* to replace or supplement paper verification checks. Subject to 5.55, this means *businesses* may use on-line verification as a substitute for paper verification checks for *clients* considered normal risk, supplemented by additional paper verification checks for higher risk *clients*, or vice versa.
- 5.55 Before using electronic databases, however, *businesses* should question whether the information supplied is sufficiently reliable, comprehensive and accurate. The following points should be considered before deciding to use an electronic source (either as part of a wider process or, where appropriate, on its own)<sup>3</sup>:
- **Does the system draw on multiple sources?** A single source, eg, the Electoral Roll, is usually not sufficient. A system which uses both negative and positive data sources is generally more robust than one that does not.<sup>4</sup>
  - **Are the sources checked across a period of time?** Systems that do not regularly update their data are generally prone to more inaccuracies than those that do.
  - **Are there control mechanisms to ensure the quality and reliability of data?** Systems should have built-in checks that ensure the integrity of data and should ideally be transparent enough to show the results of these checks and their bearing on the integrity of data.
  - **Is the information accessible?** Systems need to allow a *business* either to download and store the results of searches in appropriate electronic form, or to print off a hardcopy record containing all necessary details as to name of provider, source, date etc.

## Insolvency cases

- 5.56 In the context of insolvency work, the person or entity entering into the *business relationship* is considered to be the insolvent. *Insolvency practitioners* are also referred to the *Guidance* provided by R3.<sup>5</sup>
- 5.57 An *Insolvency practitioner* should obtain verification of the identity of the person or entity over which he is appointed. Acceptable evidence of verification may include a court order, a court endorsed appointment, or an appointment made by a debenture holder or creditors meeting supported by a company search or similar. It is not always possible or necessary to obtain identification evidence direct from individuals or individual shareholders or directors in an appointment in respect of a company as their co-operation may not be forthcoming.
- 5.58 It is important for an officeholder to be sure about the identity of the person or entity over which he is taking appointment given the urgency of the situation and the necessity not to delay when this might risk dissipation of assets and erosion of value. However, completion of other KYC elements of *customer due diligence* may not be possible prior to

---

<sup>3</sup> The JMLSG *Guidance* (Section 2, paragraphs 5.3.11 – 5.3.18) also covers indicators of good electronic identification resources.

<sup>4</sup> 'Positive' data are those that prove an individual exists, e.g. name, current address, date of birth etc, whereas 'negative' data relate known incidents of fraud, including identity fraud, other known offences and registers of deceased persons.

<sup>5</sup> [www.r3.org.uk](http://www.r3.org.uk) The Association of Business Recovery Professionals, better known as 'R3' (rescue, recovery, renewal).

appointment and should be completed as soon as practicable after appointment (if possible, usually within 5 working days).

- 5.59 *Insolvency practitioners* post appointment have a very different relationship with the insolvent *client* than that with a normal audit or advisory *client* and have access to a very wide range of information which alters the need for traditional pre-appointment KYC. However, particular focus is needed before, and immediately after, appointment on considering the way the business has been operated and assessing the risk of assets being tainted by crime in which case it may well be necessary, but not as a matter of routine in every case, to apply to SOCA for *consent* to perform the normal range of duties of collection, realisation and distribution of assets (see section 8).

## SECTION 5 A – SPECIFIC PROMPTS FOR CLIENTS

These are suggested prompts only. In order to make the most use of these *businesses* should amend the text to suit their own *client* base and services offered.

### A. For entities/businesses

1. What is its purpose in entering into any transaction forming the basis of the proposed engagement or its purpose in seeking services where not related to a specific transaction?
2. What are the entity's main trading and registered office addresses?
3. What are its business activities or purposes and sector?
4. Who controls and manages it (ie, has executive power over the entity – this may be directors, shadow directors or others depending on the circumstances)?
5. If the client is audited, were the accounts qualified and, if so, why?
6. Name and check that the person(s) purporting to represent the entity is/are who they say they are.
7. Who owns it - ultimate beneficial owner(s) and steps in between (at a minimum for companies provide details of any ultimate beneficial owners of more than 25% – for trusts, supply details of trustees and settlors and details of either beneficiaries with more than 25% interest, or the classes of beneficiary, and for collective investment funds or other similar arrangements provide details of the general partner and/or investment manager together with details of any person with more than 25% interest)?
8. What is its business model/intended business model (ie, the mechanism by which a business intends to generate revenue and profits and serve its customers – in terms of broad principles)?
9. What are the key sources of:
  - ◆ income (eg, trading, investment etc); and
  - ◆ capital (eg, public share offer, private investment etc)?
10. The history and current (also forecast if readily available) scale of the entity's:
  - ◆ earnings (eg, turnover and profits/losses); and
  - ◆ net assets.
11. The entity's geographical connections, so that you are in a position to ask such questions as “Why is it getting so much money from that place?” and “Why is it sending assets to that place?”
12. Has the entity been subject to insolvency proceedings, or is it in course of being dissolved/struck-off, or has it been dissolved/struck-off?

## B. For individuals

- ◆ His or her purpose in entering into any transaction forming the basis of the engagement or purpose in seeking services where not related to a specific transaction.
- ◆ Home address and, if applicable/different, trading address.
- ◆ His or her purpose in entering into any transaction forming the basis of the engagement or purpose in seeking services where not related to a specific transaction.
- ◆ The scale and sources of the individual's capital (past and future).
- ◆ The scale and sources of the individual's income (past and future).
- ◆ The type and sector of the individual's business activities.
- ◆ The individual's geographical connections, so that you are in a position to ask such questions as "Why is he getting so much money from that place?" and "Why is she buying assets from that place?"
- ◆ Has the individual been subject to bankruptcy proceedings?

If after enquiry of the individual it is considered that the individual has been subject to bankruptcy proceedings, information can be obtained:

- ◆ for England and Wales, on: [www.insolvency.gov.uk/eiir/](http://www.insolvency.gov.uk/eiir/)
  - ◆ [for Scotland – call The Accountant in Bankruptcy on 0131 473 4600 \(Search Team\).](#)
  - ◆ [for Northern Ireland](#) - call The Insolvency Service on 02890 251441 (Insolvency Search Department)
- ◆ Has the individual been disqualified as a director?
- Consult Companies House: [www.companieshouse.gov.uk/ddir/](http://www.companieshouse.gov.uk/ddir/)

# SECTION 5 B – EXAMPLES OF RISK-BASED VERIFICATION

Set out below are examples of risk-based verification for some of the more common client types. For Guidance on other situations, reference should be had to the JMLSG Guidance Notes.

## A. Individuals

Met face to face? **Yes and normal risk** – obtain:  
 either: proof of identity – photo identity  
 or: proof of identity – non-photo identity and proof of address (Please note P.O. Boxes are not acceptable addresses) or date of birth (can be electronic)

**No and/or higher risk** – obtain:  
 either: proof of identity – photo identity and an additional piece of evidence  
 or: proof of identity – non-photo identity, proof of address (Please note P.O. Boxes are not acceptable addresses) or date of birth  
 Plus: an additional piece of evidence

Sources of evidence	
<p><i>List 1: Evidence of identity</i></p> <p>Acceptable photo identity</p> <ul style="list-style-type: none"> <li>● valid passport; or</li> <li>● valid photocard driving licence (full or provisional); or</li> <li>● national identity card (non-UK nationals issued by EEA member states and Switzerland); or</li> <li>● firearms certificate or shotgun licence; or</li> <li>● identity card issued by the Electoral Office for Northern Ireland</li> </ul> <p>Acceptable non-photo evidence of identity:</p> <p>Documents issued by a government department, incorporating the person's name and residential address or their date of birth, eg,</p> <ul style="list-style-type: none"> <li>● a current UK full driving licence old version (<b>not</b> provisional licences); or</li> <li>● 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; or</li> <li>● documents issued by HMRC, such as PAYE coding notices and statements of account (NB: employer issued documents such as P60s are not acceptable)</li> <li>● end of year tax deduction certificates.</li> </ul>	<p><i>List 2: Evidence of address or date of birth</i></p> <ul style="list-style-type: none"> <li>● instrument of a court appointment (such as a grant of probate, bankruptcy); or</li> <li>● current council tax demand letter or statement; or</li> <li>● current (within the last 3 months) bank statements, or credit/debit card statements issued by a regulated financial sector firm in the UK, EU or JMLSG equivalent jurisdiction (but not those printed off the internet); or</li> <li>● a file note of a visit by a member of the firm to the address concerned ("home visit"); or</li> <li>● an electoral register search showing residence in the current or most recent electoral year (can be done via <a href="http://newcorp.192.com/search/index.cfm">http://newcorp.192.com/search/index.cfm</a>); or</li> <li>● a recent (last available) utility bill (gas, water, electricity, telephone – <b>not</b> mobile phone bills); it must be a bill or statement of account (<b>not</b> correspondence); or</li> <li>● valid photocard driving licence (full or provisional); or</li> <li>● a current UK full driving licence old version (<b>not</b> provisional licences); or</li> <li>● 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; or</li> <li>● documents issued by HMRC, such as PAYE coding notices and statements of account (NB: employer issued documents such as P60s are not acceptable); or</li> <li>● a firearms/shotgun certificate; or</li> <li>● a solicitor's letter confirming recent house purchase or land registry confirmation (you must also verify the previous address).</li> </ul>

## B. Entities

## i. Private company/LLP

<p>Met a representative face to face?</p>	<p><b>Yes and normal risk</b> – obtain:            Full company search from a national companies registry (or equivalent information obtained through a commercial provider of registry information)  <i>Or</i>            Certified copies of taken from original documents evidencing details of incorporation or registration, registered office and list of directors and shareholders/members</p> <p>Identify any shareholder/member in the entity holding more than 25% of the equity (rights to either income, capital or voting), or if there is no holding over 25%, where considered appropriate on a risk sensitive basis, the largest holding.</p> <p>Repeat step above until appropriate ultimate beneficial owners have been identified.</p>
	<p><b>No and/or higher risk</b> – obtain            Select individual(s) and entities that is/are capable of exercising significant influence over this entity either as an appointed director, or as a shadow director or equivalent, <b>identify</b> it/them according to whether a legal or natural person</p> <p>Select any shareholder/member in the entity holding more than 25% of the equity (rights to either income, capital or voting), or where no holding over 25%, the largest holding <b>and identify</b> it/them according to whether a legal or natural person</p> <p>Repeat step above until appropriate ultimate beneficial owners have been verified.</p> <p>For all entities, if a money service business, verify HMR&amp;C registered number (obtain certified copy of certificate or call HMR&amp;C National Advice Service on 0845 0109000, Opt. 3)</p>

## ii. Listed or regulated entity

Obtain either a printout from the relevant regulator's or exchange's web-site (and annotate), or obtain direct written confirmation from the regulator or exchange, confirming the regulated or listed status of the entity (ensure basic details of name, address, any membership or registration details, and any disciplinary details where applicable are provided).

Additional verification steps are not generally considered necessary in such cases as these entities in the UK qualify for application of *simplified due diligence*.

## iii. Government body

Obtain and annotate evidence to confirm the body's:

- main place of operation; and
- the government or supra-national agency controlling it (government and supra-national agency web-sites are a useful source of information)
- for Housing Associations, the printout must contain its registered number, registered company number (where appropriate) and registered address

Useful, trusted sites include:

UK Government information portal - <http://www.direct.gov.uk/Homepage/fs/en>

Housing Association Register - <http://www.housingcorp.gov.uk>

EU official site - <http://www.europa.eu.int/>

United Nations list of main bodies - <http://www.un.org/aboutun/mainbodies.htm>

USA government information portal -

[http://www.firstgov.gov/Agencies/Federal/All\\_Agencies/index.shtml](http://www.firstgov.gov/Agencies/Federal/All_Agencies/index.shtml)

Additional verification steps are not generally considered necessary in such cases as these entities in the UK qualify for application of *simplified due diligence*.

#### **iv. Money Service business**

Verify HMR&C registered number (obtain certified copy of certificate or call HMR&C National Advice Service on 0845 0109000, Opt. 3).

## SECTION 6 - REPORTING

### KEY POINTS

- *Suspicious activity reports* submitted by the *regulated sector* are an important source of information used by SOCA in meeting its harm reduction agenda, and by law enforcement more generally.
- *Businesses* are required to have procedures which provide for the nomination of a person (in this *Guidance* the *MLRO*) to receive disclosures (*internal reports*) under Part 7 of *POCA* and which require that everyone in the *business* complies with Part 7 of *POCA* in terms of reporting knowledge, suspicion or reasonable grounds for knowledge or suspicion of *money laundering*
- Failure to report in accordance with Part 7 of *POCA* where the relevant information or other matter has been obtained through the course of work in the *regulated sector* is a criminal offence which can be committed by any *individual* (s330, *POCA*), or by the *MLRO* (s331, *POCA*). There is a similar offence for *MLRO*'s outside the *regulated sector* in s332, *POCA*.
- An *individual* other than the *MLRO* fulfils his reporting obligations by making an *internal report* to his *MLRO*.
- The *MLRO* is responsible for assessing *internal reports*, making further inquiries if need be (either within the *business* or using public domain information), and, if appropriate, filing *SARs* with SOCA.
- Where a *relevant professional advisor* forms knowledge or suspicion or reasonable grounds for such in 'privileged circumstances' no report should be made to SOCA unless this '*privilege reporting exemption*' is overridden by the crime/ fraud exception ie where the information or other matter is communicated to the *relevant professional advisor* with the intent of furthering a criminal purpose (Section 7.42 to 7.46).
- When reports are properly made they are 'protected' under s337, *POCA* in that nothing in them shall be taken to breach any restriction on the disclosure of information, however imposed.
- A person who considers he may have engaged or is about to engage in *money laundering*, should make an 'authorised' disclosure (s338, *POCA*). Such a disclosure, provided it is made (and SOCA's consent to the act is obtained) before the act is carried out, or is made as soon as possible on the initiative of that person after the act is done and with good reason being shown for the delay, may provide a defence against charges of *money laundering*. When properly made such reports shall not be taken to breach any restriction on the disclosure of information, however imposed.
- *Consent* may be sought from SOCA under s335, *POCA* (and confirmed to the *business* by the *MLRO* under s336 *POCA*) to carry out activity that would otherwise be *money laundering* under ss327-329 *POCA*. If granted, the *consent* provides complete protection against charges of *money laundering* but only in respect of the activity covered by the *consent*.
- *TA 2000* provides for broadly equivalent provisions regarding the reporting of knowledge, suspicion or reasonable grounds for such of *terrorist financing*. The definition of '*terrorist property*' is set out in s14, *TA 2000* and the *terrorist offences* and provisions regarding reporting, *consent* and *tipping off* are set out in ss15-21A.

---

### WHAT MUST BE REPORTED?

- 6.1 Under ss330-332, *POCA*, failing to report knowledge or suspicion, or reasonable grounds for such, of *money laundering* is a criminal offence (see section 2 of this *Guidance*, which

outlines the offences and details of exemptions). The following must be reported, as soon as practicable. These are collectively known as 'the *required disclosure*':

- the identity of the suspect (if known);
- information or other matter on which the knowledge or suspicion of *money laundering* (or reasonable grounds for such) is based; and
- the whereabouts of the laundered property (if known)

- 6.2 Care is needed to ensure that any information held concerning identity (such as date of birth, passport number, address, registration numbers for companies and so on) is included within reports and in the correct designated fields in the SOCA prescribed forms, as well as details of the laundered property and its whereabouts, where known, and reasons for knowledge or suspicion.
- 6.3 Even if the name of a suspect is not known, any information available which may assist in identifying the suspect or the whereabouts of any of the laundered property must be included in the report, under the provisions of s330 (3A), POCA. For example, even if the *business* does not have the name of the suspect, if the *business* is aware the *client* holds the detail the report needs to reflect this as information which may assist in identifying the suspect.
- 6.4 In cases where the suspect is not known, another subject should be included in the report, whether this is the victim or another subject associated with the activity. The fact that in these cases the subject of the report is not a suspect should be made clear in the report.
- 6.5 The disclosure requirement relates to any information coming to a person in the course of business in the *regulated sector*, and not just information relating to *clients* and their affairs. This means that reports made may be required on the basis of information not only about *clients*, but about potential *clients*, associates and counterparties of *clients*, acquisition targets and even employees of *businesses* in the *regulated sector*.

---

## TYPES OF REPORT

- 6.6 Reports made in accordance with the provisions of POCA are made under either s337 (protected disclosures) or s338 (authorised disclosures).

### The Protected Disclosure

- 6.7 A protected disclosure is any report made by a person providing the *required disclosure*, based on information or other matter coming to their attention in the course of their trade, profession, business or employment, where this information has led to knowledge or suspicion (or reasonable grounds for such) that another person is engaged in *money laundering*.
- 6.8 A protected disclosure may be made by any person forming a *money laundering* suspicion, at work or carrying out professional activities, whether or not acting within the *regulated sector*. This means that any *individual* or *business*, or other organisation (such as a charity) meeting these conditions may make a voluntary report to SOCA in the public interest and benefit from the protections contained in s337, POCA against allegations of breach of confidentiality. In the *regulated sector*, such reports are compulsory (save where an exemption such as the *privilege reporting exemption* applies).

### The Authorised Disclosure

- 6.9 An authorised disclosure is a report made by a person who makes the disclosure:

- before he has carried out a prohibited act (ie, done something which would constitute a *money laundering* offence under ss327-329, *POCA*); or
- whilst he is doing the prohibited act, or after he has done such an act provided that when he started to do the act he didn't realise that it was *money laundering* (ie, did not realise that *criminal property* was involved) and made the report on his own initiative as soon as he knew or suspected *criminal property* was involved; or
- after he has done the prohibited act, provided that there was good reason for not reporting before he committed the act, and he made the report on his own initiative as soon as it was practicable to make it. There is no guidance in *POCA* as to what might constitute 'good reason', but this is likely to be applied narrowly.

### Confidentiality protections

- 6.10 Any report properly made under the provisions of ss337 and 338, *POCA* cannot be taken to breach any restriction on disclosure of information, however this is imposed. This means considerations of *client* or other duties of confidentiality must not impede reporting, unless the *privilege reporting exemption* applies (see section 7 below) where different considerations apply. Such protection does not exist for reports which are made founded only on speculation or made defensively, founded on generalities or 'just in case'.

### Non-POCA reporting

- 6.11 This *Guidance* deals only with obligations under the UK anti-*money laundering* regime – *businesses* and *individuals* should have regard to other obligations they may have, such as reporting responsibilities under the Statements of Auditing Standards, statutory regulatory returns, and reports of misconduct of fellow members of professional bodies. In all cases, the risk of *tipping off* must be considered and avoided. Further *Guidance* on acting for *clients* who are the subject of SARs is given in section 9.

---

## RECOGNISING MONEY LAUNDERING

### The key elements

- 6.12 The anti-*money laundering* requirements only relate to criminal matters, that is those which attract criminal penalties. Other acts may be unlawful, but not criminal. This distinction is particularly important in areas of work where an array of penalties on both civil and criminal levels exist. An example of this is in relation to infringement of the requirements of the Companies Act where there is a mixture of issues attracting civil penalties and those attracting criminal penalties.
- 6.13 In most cases of suspicion, the reporter will have in mind a particular type of underlying or predicate *criminal conduct*. However, on occasion a transaction or activity may so obviously lack any normal economic rationale or business purpose as to lead to a suspicion that it may be linked to *money laundering* in the absence of any other credible explanation. *Individuals* should not hesitate to exercise professional scepticism and judgement and should report such matters if appropriate.
- 6.14 For a matter to be *money laundering*, there must not only be *criminal conduct*, but also proceeds or *criminal property*. These terms are described below.

### Criminal conduct

- 6.15 *Criminal conduct* is that which constitutes an offence in any part of the UK or would do if it was committed in the UK. However, *businesses* and *individuals* should note that under the provisions of the *overseas conduct exception* (s330(7)(A) *POCA*) there are limited

exceptions to the requirement to report conduct occurring overseas – see sections 2.4 and 2.5.

- 6.16 Since UK law defines *money laundering* so widely, any *criminal conduct* which has resulted in any form of *criminal property* will also constitute *money laundering*. It is not expected that *individuals* will become expert in the very wide range of underlying or predicate criminal offences which lead to *money laundering* but they will be expected to recognise those that fall within the professional competence of their role but should use professional scepticism, judgement and independence as appropriate to identify offences.
- 6.17 If a person knowingly engages in criminal activity but does not successfully benefit from it, he may have committed some other offence (often fraud) but not *money laundering*. If an activity does not result in *criminal property* it cannot constitute a *money laundering* offence. Consequently, there is no obligation to file a *money laundering* report. However, *businesses* and *individuals* may wish to report the matter to the Police, or may have other reporting duties (such as those referred to in section 6.11 above).

### **Criminal property**

- 6.18 *Criminal property* is the benefit derived from a person's criminal activity. Note that *criminal property* (or 'proceeds') can take any form. For example, cost savings from ignoring mandatory health and safety regulations (amounting to a criminal offence) savings as a result of tax evasion, and other less obvious financial benefits can also constitute *criminal property*. Where *criminal property* is used to acquire further assets these further assets themselves become *criminal property*. It is important to note that there is no de minimis level and thus *criminal property* is not identified by its value.
- 6.19 *POCA* defines *criminal property* in s340(3)(b), *POCA* as 'property is *criminal property* if it constitutes a person's benefit from *criminal conduct* and the alleged offender knows or suspects, that it constitutes or represents such a benefit'

### **Intent**

- 6.20 Except for certain strict liability offences, *criminal conduct* requires an element of criminal intent. S 340(3)(b) of *POCA* means that an offender must know or suspect that property is criminal. Conduct which is an innocent error or mistake may be criminal where it constitutes a strict liability offence but will not also be *money laundering*.
- 6.21 If an *individual* or *business* knows or believes that a *client* is acting in error, the *individual* may approach the *client* and explain the situation and legal risks to him. However, once the criminality of the conduct is explained to the *client*, he must bring his conduct (including past conduct) promptly within the law to avoid a *money laundering* offence being committed. Where there is uncertainty about the legal issues, outside the competence of the *individual*, *clients* should be referred to an appropriate specialist or professional legal adviser.
- 6.22 Note that if there are reasonable grounds to suspect that a *client* knew or suspected that his/ its actions were criminal, a report must be made. Even if the *client* does not have the relevant intent, but *businesses* or *individuals* are aware that there is *criminal property*, consideration needs to be given to whether a report has to be made under s 338, *POCA* to avoid an offence under ss 327-329, *POCA* (see also section 6.27 and section 8).

### **Determining whether and when to report**

- 6.23 There can be no hard and fast rules on how to recognise *money laundering*. It is important for all *individuals* to be alert to this issue and to apply their professional judgement and experience.

- 6.24 *Individuals* need to consider whether activity or conduct observed in the course of business has the characteristics of *money laundering* and, therefore, warrants a report. Most *businesses* will include in their standard anti-*money laundering* systems and procedures arrangements to allow *individuals* to discuss whether the information they hold amounts to a reportable knowledge or suspicion, and *individuals* should take advantage of these arrangements where necessary.
- 6.25 *Individuals* must report promptly to the *MLRO* (or exceptionally direct to *SOCA*) once the requisite knowledge or suspicion has been formed, or reasonable grounds for such have come into existence. There are no external requirements for the format of an *internal report* and *businesses* may design their systems for *internal reporting* as they wish. *Internal reports* may be made orally or in writing, and may refer to *client* files or contain all the requisite information in a standard form, provided that all the information in the *required disclosure* and other information which the *business* requires under its procedures for the reporting of *money laundering* are reliably provided and recorded.
- 6.26 To decide whether or not a matter is suspicious *individuals* may need to make further enquiries (within the normal scope of the assignment or *business relationship*) of the *client* or their records. The anti-*money laundering* legislation does not prevent normal commercial enquiries being made to fulfil duties to *clients*, and such enquiries may also assist in understanding a matter to determine whether or not it is suspicious. However, investigations into suspected *money laundering* should not be conducted unless this is within the scope of the engagement, and information is limited to that to which the *individual* would normally be entitled in the course of business. Normal business activities should be maintained and such information or other matter which flows from this will form the proper basis of *internal reports* and *SARs*. To carry out additional investigations is unnecessary and could risk *alerting a money launderer*.
- 6.27 *Individuals* should be cautious and report to their *MLRO* if in doubt, but may wish to consider the following questions to assist their decision:
- Am I suspicious, or do I know, that activity I have seen is criminal and has caused someone to benefit from it in some way?
  - Am I suspicious of an activity which, whilst I can't identify a specific *predicate offence*, is so unusual or lacking in normal commercial rationale that it causes suspicion that money is being laundered?
  - If so, do I suspect a particular person or persons of having been involved in criminal activity (or do I know who undertook criminal activity), or does another person that I can name have details of this person(s) or information that might assist in identifying this person(s)?
  - Do I know who might have received, or still be holding, the benefit of the criminal activity or where the *criminal property* might be located or have I got any information which might allow the property to be located?
  - Do I think that the person(s) involved in the activity knew or suspected that the activity was criminal or do I think the activity arose from innocent error?
  - Can I explain coherently what and who I am suspicious of, and why, either in terms of knowledge or suspicion that a *predicate offence* has been committed, or in terms of abnormal activities which may constitute *money laundering*?

Consideration must also be given to whether *individuals* or *businesses* have engaged, or intend to engage, in conduct which could constitute a *money laundering* offence under ss327-329, POCA (eg, transferring *client* money that comprises *criminal property*). If so, this must also be reported to the *MLRO* as a report may be required under s 338, POCA and *consent* requested.

---

## HOW TO REPORT

### Internal reports to the *MLRO*

- 6.28 The *2007 Regulations* require *businesses* to maintain internal reporting procedures that allow any *individual* in the *business* to submit to the *MLRO* a report of knowledge or suspicion or reasonable grounds for such, of *money laundering*. Only by doing this can the *individual* fulfil his obligations under s330, *POCA* (or in exceptional circumstances, reporting direct to *SOCA*). Of course, sole practitioners who do not employ any staff will simply make their own *SARs* directly to *SOCA*.
- 6.29 Under s330, *POCA*, the *internal report* must reach the *MLRO* – a report to a line manager or other colleagues is not enough to comply with the legislation.<sup>6</sup> An *individual* may discuss his suspicion with managers or other colleagues to assure himself of the reasonableness of his conclusions but, other than in group reporting circumstances, the responsibility for reporting to the *MLRO* remains with him. It cannot be transferred to anyone else, however junior or senior they are.
- 6.30 Where a group (more than one *individual*) arrives at knowledge or reasonable suspicion together by consolidating their thoughts, a single *internal report* may be submitted, in terms agreed by those forming the suspicion and in the names of them all. This may occur, for example, where an engagement team has a reason to be suspicious.

### Reports to *SOCA*

- 6.31 The *MLRO* will be responsible for making decisions on whether the information contained in an *internal report* needs to be relayed to *SOCA* in the form of a *SAR*, and compiling and despatching the *SAR* to *SOCA* (section 7). The *MLRO* will also be responsible for determining whether *consent* is required to continue with the engagement or any aspect of it, and will usually be responsible for decisions on how business should be conducted pending receipt of *consent* (section 8).

---

<sup>6</sup> Both the *2007 Regulations* and *POCA 2002* use the term 'nominated officer' for *MLRO*.

## SECTION 7 – THE MLRO AND REPORTING TO SOCA

### KEY POINTS

- The role of the *MLRO* carries significant responsibility and should be undertaken by a senior person within the *business* who has sufficient authority to take independent decisions, and who is properly equipped with sufficient knowledge, and resources, to undertake the role.
- The key role is that of receiving *internal reports*, and making *SARs* to *SOCA* as applicable, but *MLROs* may undertake other functions relating to the *businesses'* systems and controls in relation to its *anti-money laundering* activities.
- *Businesses* should make provision for delegates or deputies to cover any absence of the appointed *MLRO* and should ensure all relevant employees are aware of the reporting channels laid down by the *business*.
- It is for *businesses* to determine the format of *internal reports* but reports to *SOCA* must be made in the prescribed form in accordance with s339, *POCA*.
- A *relevant professional adviser* who suspects or has reasonable grounds for knowing or suspecting that another person is engaged in *money laundering* is exempted from making a *money laundering* report where his knowledge or suspicion comes to him in privileged circumstances (the *privilege reporting exemption*).

---

### THE ROLE

7.1 The role of the *Money Laundering Reporting Officer (MLRO)* carries significant responsibility and should be undertaken by an appropriately experienced *individual*. Although there is no prescribed level of seniority, one of the principals of an accounting firm, or similar in other *businesses*, is likely to be suitable, or another senior and skilled person with sufficient authority to enable decisions to be taken independently. *MLROs* are **required** to:

- consider *internal reports* of *money laundering*;
- decide if there are sufficient grounds for suspicion to pass those reports on to *SOCA* in the form of a *SAR*, and, if so, to make that *SAR*; and
- act as the key liaison point with *SOCA* and law enforcement agencies including dealing with *consent* and disclosure issues.

*MLROs* **may** also take responsibility for:

- training within the *business*;
- advising on how to proceed with work once an *internal report* and/or *SAR* has been made in order to guard against risks of *tipping off* or *prejudicing an investigation*; and
- the design and implementation of internal *anti-money laundering* systems and procedures.

If this role is not undertaken by the *MLRO*, these responsibilities should be taken on by another sufficiently senior and skilled person within the *business*. This person should work closely with the *MLRO*.

- 7.2 The functions of an *MLRO* can be delegated, although this does not relieve that *MLRO* of his responsibility, and *businesses* should have contingency arrangements for discharging the duties of an *MLRO* during periods of absence or unavailability. It is recommended that *businesses* appoint an alternate or deputy *MLRO* for these situations and ensure that the reporting channels are well known to all relevant employees.
- 7.3 Like all *individuals*, *MLROs* can commit the *money laundering* offences as well as the related offences of *failure to disclose*, *tipping off*, and *prejudicing an investigation*.

---

## ASSESSING INTERNAL REPORTS

- 7.4 When first approached by a colleague with an *internal report*, there are two matters for immediate consideration. Rapid consideration is needed by the *MLRO* as to whether an application for *consent* is required (see section 8). In addition, the *MLRO* should first establish by discussion and review whether or not the *privilege reporting exemption* may apply, as this exemption significantly affects not only whether a *SAR* must be made under the legislation, but also whether it may be made. The *privilege reporting exemption* is limited to *relevant professional advisers*, and will not be available other than to members of well established professional bodies such as those listed in Schedule 3 to the *2007 Regulations* and who meet the requirements set out in s 330 (14), *POCA*. Further *Guidance* on the *privilege reporting exemption* is given in sections 7.26 to 7.46 below.
- 7.5 Once the *MLRO* receives an *internal report*, he must assess it and determine whether it meets the criteria laid down in s 331, *POCA* ie:
- does he know, suspect or have reasonable grounds to know or suspect that another person is engaged in *money laundering*; and
  - did the information or other matter giving rise to the knowledge or suspicion come to him in a disclosure made under s 330, *POCA*; and
  - does he know the name of the other person or the whereabouts of any laundered property from the s 330 disclosure; or
  - can he identify the other person or the whereabouts of any laundered property from information or other matter contained in the s 330 disclosure; or
  - does he believe, or is it reasonable for him to believe, that the information or other matter contained in the s 330 disclosure will or may assist in identifying the other person or the whereabouts of any laundered property.
- 7.6 In each case the *MLRO* should ensure the report contains all the relevant information known to the *individual(s)* making the report and records all necessary aspects as follows:
- who is making the report
  - the date of the report
  - who is suspected or information that may assist in ascertaining the identity of the suspect (which may simply be details of the victim and the fact that the victim knows the identity but this is not information to which the *business* is privy in the ordinary course of its work)
  - who is otherwise involved in or associated with the matter and in what way
  - what the facts are
  - what is suspected and why
  - information regarding the whereabouts of any *criminal property* or information that may assist in ascertaining it (which may simply be the details of the victim who has further information but this is not information to which the *business* is privy in the ordinary course of its work)
  - what involvement does the *business* have with the issue in order that requirements for *consent*, the need for consideration of *tipping off* issues, basis of continuance of work and any other necessary guidance for engagement staff may be considered.

- 7.8 The *MLRO* may also wish to make reasonable enquiries of other *individuals* and systems within the *business*. Such enquiries may either have the effect of confirming the knowledge or suspicion, or reasonable grounds for such, or may provide additional material which enables the cause of suspicion to be eliminated at which point the matter may be closed without a *SAR* being issued.
- 7.9 In conducting his assessment, the *MLRO* may well wish to consider the criteria set out in section 6 [determining whether to report]. If the *MLRO* considers the information or other matter he has received in an *internal report* meets these criteria then a *SAR* to *SOCA* will be required unless either the *privilege reporting exemption* has been applied on the reporter seeking advice from the *MLRO* and not overridden by the crime/fraud exception or, on analysis of the *internal report* received, the *MLRO* determines that the *overseas conduct exemption* applies (sections 2.4 and 2.5).

### The Reporting Record

- 7.10 It is vital for the control of legal risk that adequate records of *internal reports* are maintained, usually by the *MLRO*. These would normally be details of all *internal reports* made including details of the *MLRO*'s handling of the matter, his requests for further information, assessments of the information received, decisions as to whether to conclude immediately or to wait for further developments or information, whether to make a *SAR* or not and on what grounds, any advice given to engagement teams as regards continuation of work and any *consent* requests made.
- 7.11 Details of *internal reports* submitted as *SARs* should also be retained. For efficiency, and ease of reference for the *MLRO*, it is recommended that some form of index of reports is kept and internal reference numbers given. The records may be simple, or sophisticated, depending on the size of the *business* and the volume of reporting, but all need to contain broadly the same information and be supported by appropriate working papers. These records are important as they may subsequently be required to justify and defend the actions of an *individual* or *MLRO*. There is no prescribed form specified in *POCA* or elsewhere for *internal reports* to an *MLRO*.

---

### MAKING EXTERNAL REPORTS

- 7.12 Once an *MLRO* has concluded a report is required, it should be prepared and submitted promptly to *SOCA*.
- 7.13 The requirement set out in *POCA* as to timing of reports is that a report should be made 'as soon as is practicable' after the information required is received. In practical terms, the interval between receiving an *internal report* and making a *SAR* will vary quite widely. Some matters may be disposed of very rapidly where all the information required to make a *SAR* is received with the first contact, and where this occurs a quick turnaround should be achieved. It is particularly important to work rapidly in matters where *consent* is required, or where '*money laundering* in action' is suspected, ie, another is engaged in current criminal activity which may provide law enforcement with opportunities to intervene. In other cases, where not all the required information is immediately to hand, or where there is material uncertainty as to whether the matter is reportable or not, the *MLRO* may reasonably chose to await further expected developments, and/or seek further information before making a reporting decision.
- 7.14 Following the implementation of the relevant legislation *MLROs* must use one of *SOCA*'s prescribed manners and methods of submission, to make reports. Failure to do so will be an offence under s3391A, *POCA*, although *SOCA* indicate that in urgent and unusual circumstances flexibility will be allowed. The requirement to use the prescribed manners and methods covers all reports made by the *regulated sector*, *MLRO*'s outside of the

*regulated sector*, and anyone seeking to make a report under s 338 in order to gain the benefit of a defence. The prescribed manners and methods are:

- SAR on-line, using internet transfer
- Moneyweb, using extranet transfer
- Secure (encrypted email) using electronic file transfer by email
- Bulk reports in electronic form using CD etc for transfer
- Hard copy SOCA forms (obtainable on the internet or by post on request to SOCA) to be typed and submitted by post or fax

The prescribed manner must be used in conjunction with the prescribed method to ensure security, eg, completed hard copy forms may not be sent on non-encrypted email. The manners most likely to be of relevance to those providing *defined services* are SAR on-line, Moneyweb and the hard copy forms, the other two manners and methods are normally only used by retail banks and others submitting very large quantities of reports. We recommend that *individuals* and *businesses* have regard to guidance on how to make reports published from time to time by SOCA. Details of SOCA's preferred reporting methods are available from their web site at [www.soca.gov.uk](http://www.soca.gov.uk)

- 7.15 Each of the prescribed manners contain compulsory fields which require information, where known, to be provided in accordance with the *required disclosure* provisions. These fields relate to the identity of the reporter, the details of subjects (to the extent known but at least one must be named whether as victim or suspect and the identity information known provided in the correct specified fields), and in the free text box (variously called 'reason for disclosure' or 'reason for suspicion') the whereabouts of the laundered property, where known, and the description of the reason for suspicion or knowledge.
- 7.16 *MLROs* should be aware that once legislation is implemented, failure to use the prescribed form will be an offence, punishable by a fine. Please note that currently there is no prescribed form.
- 7.17 In preparing *SARs*, *MLROs* should seek to present information in a way that is clear and succinct. In particular:
- the full name of the reporting *business* must be provided and the internal reference for the report should be provided in each case;
  - identification information held by the *business* (name, address, date of birth, registration numbers etc) must be presented in the appropriate subject fields, and not simply incorporated into the 'reason for suspicion' text;
  - where it assists in explaining the matter being reported, it may be appropriate to include a number of subjects in the report, providing such identification information as is known in the manner above for each of them;
  - for each subject their role, as far as it is known, in the matter should be made clear and the options of flagging each subject as suspect/victim/unknown used as appropriate;
  - where bank account/transaction details are available and relevant, these should be included in the appropriate fields;
  - the activity observed should be explained clearly in the reasons for suspicion field, without using jargon or terms which might not be readily understood by non-accountants and, as far as known, giving details of when events occurred;
  - features of the activity which are unusual or are considered to denote either a *predicate offence to money laundering*, or *money laundering*, should be highlighted as such;
  - such information held as to the whereabouts of any laundered property should be given;
  - the information given in the reasons for suspicion field should be succinct; and

- the report should be submitted without any supporting documents and accordingly should be able to stand alone to explain the suspicion through provision of the information comprising the *required disclosure*.

7.18 If the *MLRO* so wishes, he may make use of the *SAR Glossary of Terms* provided by *SOCA* and incorporate the relevant terms in his report.

7.19 An important role for the *MLRO* on receipt of an *internal report* and on making a *SAR* is to advise engagement teams on how to continue their work and interact with the *client* to balance professional responsibilities, risk to the *business* and responsibilities under *POCA*. This area of work is examined in section 9.

## Guarding confidentiality

7.20 If *clients* or third parties become aware that an *individual* or *business* has made a *SAR*, this can have adverse effects on *client* relationships and may ultimately endanger the security of staff members. Maintaining the confidentiality of *SARs* is important to *SOCA*<sup>7</sup>. Access to *SAR* information is now provided to end-users in law enforcement and similar agencies by *SOCA* only on condition that undertakings are taken as to compliance with Home Office guidance on preserving the confidentiality of *SARs*. (Home Office Circular 53 / 2005 'Money Laundering: The Confidentiality And Sensitivity Of Suspicious Activity Reports (*SARs*) And The Identity Of Those Who Make Them').

7.21 *SOCA* has provided a reporting line for concerns over breach of confidentiality by end-users of reports and details may be found on <http://www.soca.gov.uk/financialIntel/sarBreachLine.html>.

7.22 Whilst it is reasonable for the *regulated sector* to expect *SOCA* to make strenuous efforts to protect the confidentiality of those who make *SARs*, reporters should also take such steps as are available to them to protect the confidentiality of *individuals* and *businesses* and the information reported.

7.23 In making reports, *MLROs* should disclose information relevant to the suspicion or knowledge of *money laundering* and information necessary to allow the reader to gain a proper understanding of the matters reported. It is recommended that reporters:

- refrain from including other confidential information where this is not required for compliance with obligations under *POCA*
- show the name of the *business*, *individual*, or *MLRO* submitting the report only once in the source ID field but nowhere else in the report;
- do not include names of personnel who made *internal reports* to the *MLRO*;
- only include parties as subjects where this information is necessary for an understanding of the report, or to meet the standards of the *required disclosure*; and
- highlight clearly in the reasons for suspicion/disclosure field any particular concern the reporter has about safety (in physical, reputational or other terms).

7.24 Whilst it is reasonable for an *MLRO* to answer questions from a *SOCA* officer or a law enforcement officer aimed simply at clarifying the content of a *SAR*, any further disclosure to *SOCA* or law enforcement or prosecuting agencies should normally only be undertaken in response to the exercise of a power to obtain information contained in relevant legislation, or in compliance with professional guidance on the balance of confidentiality and making disclosures in the public interest. This provides protection for the *MLRO* and the *business* against any allegation of breach of confidentiality.

---

<sup>7</sup> The review into the future of the *SAR* regime, known as the Sir Stephen Lander Review, included recommendations regarding the importance of maintaining and improving confidentiality in the *SAR* regime.

7.25 A facility exists for any person to make voluntary disclosures to SOCA under s34, SOCPA provided that:

- the disclosure is made for the purposes of the exercise by SOCA of any of its functions (ss2-4, SOCPA);
- it is not a disclosure of personal data in contravention of the Data Protection Act 1998 where that personal data is not exempt from its provisions;
- it is not a disclosure prohibited by Part 1, Regulation of Investigatory Powers Act 2000 (relating to unlawful interception of communications).

If a disclosure meets these requirements, the person making the disclosure does not breach any duty of confidentiality or other restriction on the disclosure of information, however imposed. We recommend a cautious approach to disclosure under this section, as it is important to be sure that all the required conditions are met.

---

## THE PRIVILEGE REPORTING EXEMPTION

7.26 With effect from 21 February 2006, a *relevant professional adviser* who suspects or has reasonable grounds for knowing or suspecting that another person is engaged in *money laundering* is exempted from making a *money laundering* report where his knowledge or suspicion comes to him in privileged circumstances (the *privilege reporting exemption*). In such circumstances, provided that the information is not given to him with the intention (by his *client* or another person) of furthering a criminal purpose ('the crime/fraud exception' – see sections 7.42 to 7.46 below), s330(6) affords the adviser a complete defence against a charge of failure to disclose (ie, to make a SAR). By implication, the exemption also means that in these circumstances a *business* should not make a SAR, as they are expected to be bound by the same standards of behaviour as is the case for legal professional advisers subject to legal professional privilege.

7.27 Discussions with the MLRO to seek advice about making a report under s 330, POCA shall not be taken to be an *internal report* when it was not intended as such, eg, if the person initiating the discussion believes the matter falls within the *privilege reporting exemption* and contacts the MLRO to confirm this. On receipt of such an approach, it is recommended the MLRO still collects the information which would otherwise be included in the *required disclosure* to enable careful consideration with the reporter of whether or not the matter falls within the *privilege reporting exemption* and, if it does, whether this is overridden by the crime/fraud exception. It is recommended that the MLRO documents the decision reached in this regard and the reasons for reaching that decision.

7.28 A *relevant professional adviser* is defined in the legislation as:

- an accountant, auditor or *tax adviser* who is a member of a professional body which is established for accountants, auditors or *tax advisers* (as the case may be); and which makes provision for;
  - (a) testing the competence of those seeking admission to membership of such a body as a condition for such admission; and
  - (b) imposing and maintaining professional and ethical standards for its members, as well as imposing sanctions for non-compliance with those standards.

The *privilege reporting exemption* also extends to persons in partnership with (or equivalent), or employed by, the *relevant professional adviser* to provide them with assistance or support. The information must come to these partners or employees in connection with this assistance or support and to the *relevant professional adviser* in privileged circumstances.

- 7.29 The legislation does not list which professional bodies meet the criteria listed in s 330 (14), but the CCAB member bodies meet those criteria and, accordingly, *individuals* who are members of a CCAB member body, those in partnership with such *individuals* in *businesses* regulated by the CCAB and the employees of such *businesses* and *individuals* are within the scope of the exemptions. If *businesses* or *individuals* are in any doubt as to whether these provisions apply to them, it is recommended that they seek legal advice.
- 7.30 However, the amendments referred to above affect only the duty to make *money laundering* reports and related disclosures under POCA. They do not in any way extend legal professional privilege to advice given by *relevant professional advisers* in any other circumstances. However, *businesses* and *individuals* need to be aware, when responding to requests for further information (sections 9.11 to 9.17), documents subject to a *client's* privilege are not disclosable.
- 7.31 If a *relevant professional adviser* considers that the information or other matter on which his knowledge or suspicion is based came to him in privileged circumstances, he is obliged to apply the *privilege reporting exemption* in s330(6), POCA (unless the crime/fraud exception applies) and so has no discretion to make a *money laundering* report. This means that the *relevant professional adviser* could find himself in a situation where he might wish to make a report but is prevented from doing so. In such circumstances, he should consider whether he may continue to act, but in carrying out his decision will need to bear in mind the provisions of POCA relating to *prejudicing an investigation* (s342, POCA).
- 7.32 Whether or not the *privilege reporting exemption* applies needs to be considered carefully, including a consideration as to whether the *relevant professional adviser* was working in privileged circumstances when the particular information or other matter came to him. This is an important consideration, as a *relevant professional adviser* may be providing a variety of services to a *client*, not all of which may create privileged circumstances for this purpose. Accordingly, it is strongly recommended that a careful record is maintained of the provenance of information considered when a decision is made on the applicability or otherwise of the *privilege reporting exemption*.
- 7.33 Set out below is a description of the two types of privileged circumstances and some examples of work which may fall within or outside of them.

### Legal advice

- 7.34 For the privileged circumstances set out in s330(10)(a) and (b), POCA to apply, the following conditions need to exist:
- there needs to be a confidential communication (written or oral) between the *relevant professional adviser* and his *client*, or a representative of the *client*, in which the *client* seeks or the *relevant professional adviser* gives legal advice;
  - that communication must take place within the confines of a professional relationship between them, including an initial meeting which does not progress to a *business relationship*; and
  - the communication must relate to legal advice (ie, advice concerning the rights, liabilities and obligations or remedies of the *client* under the law).

### Litigation

7.35 For the privileged circumstance set out in s330(10)(c), *POCA* to apply, the following conditions need to exist:

- there must be a confidential communication (written or oral) between the relevant professional advisor and the *client* or third party;
- the confidential communication must be made for the dominant purpose (ie, the overriding purpose) of being used in connection with actual, pending or contemplated litigation.

Defining contemplated litigation is difficult. In summary, it is usually necessary to be able to identify some act that gives rise to a cause of action in relation to which some threat of legal action has either been clearly intimated or is more than reasonably likely to follow. The party seeking to claim the benefit of litigation privilege must show that he was aware of circumstances that rendered litigation between himself and a particular person or class of persons a real likelihood rather than a mere possibility.

### Examples of privileged circumstances

7.36 Examples where *relevant professional advisers* might frequently fall within privileged circumstances as regards legal advice privilege include, where this advice is delivered as part of the provision of a *defined service*:

- advice on taxation matters, where the *tax adviser* is giving advice on the interpretation or application of any element of tax law and in the process is assisting a *client* to understand his tax position;
- advice on the legal aspects of a take-over bid, for example on points under the Companies Act legislation;
- advice on duties of directors under the Companies Act;
- advice to directors on legal issues relating to the Insolvency Act 1986, eg, on the legal aspects of wrongful trading; and
- advice on employment law

7.37 Examples where *relevant professional advisers* might fall within privileged circumstances as regards litigation privilege include:

- assisting a *client* by taking witness statements from him or from third parties in respect of litigation;
- representing a *client*, as permitted, at a tax tribunal; and
- when instructed as an expert witness by a solicitor on behalf of a *client* in respect of litigation.

7.38 It should be noted that conducting audit work does not of itself give rise to privileged circumstances for this purpose, as the *relevant professional adviser* is neither providing legal advice, nor is he instructed in respect of litigation. Nor do routine book-keeping, accounts preparation or tax compliance assignments, though privileged circumstances may arise if the *client* requests or the adviser gives, legal advice on an informal basis, during the course of such an assignment

7.39 It is recommended that the reasons for the conclusion reached as to whether the *privilege reporting exemption* applies are carefully documented. If the *relevant professional adviser* decides it does apply, he must act in accordance with the *privileged reporting exemption* unless the crime/fraud exception applies. If in doubt, it is recommended that *businesses* and *individuals* seek professional or legal advice.

## Recording and discussion with the *MLRO*

- 7.40 Even where the *client* service team believe that the *privilege reporting exemption* applies, *businesses* should consider whether all matters involving knowledge or suspicion of *money laundering* should still be referred to the *MLRO* for advice or to another appropriate person (see section 7.41 of this *Guidance*). Discussion of a matter with the *MLRO*, where the purpose of the discussion is the obtaining of advice about making a disclosure under s330, does not alter the applicability of the *privilege reporting exemption*. Given the complexity of these matters, and the need for considered and consistent treatment with adequate documentation of decisions made, a referral to and discussion with the *MLRO* is likely to be beneficial and is recommended. The *MLRO* may decide, with the reporter, to seek further appropriate advice.
- 7.41 Likewise reporters within a *business* are entitled to seek advice from an appropriate specialist (either a person within the *business* who would fall into the category specified in s330(7B) or an external adviser who himself is able to apply the *privilege reporting exemption*) without altering the applicability of the *privilege reporting exemption*.

## The Crime/Fraud Exception

- 7.42 Before determining whether the *privilege reporting exemption* must be applied, consideration needs to be given to whether the exemption is lost through application of the crime/fraud exception. This exception, as set out in s330(11), *POCA*, overrides the *privilege reporting exemption* which:
- ‘does not apply to information or other matter which is communicated or given with the intention of furthering a criminal purpose’.
- This means that communications that would otherwise qualify under one or other of the above two types of privilege are not covered by the *privilege reporting exemption* where the communication was intended to facilitate or to guide someone (usually the *client* but possibly a third party) in the commission, or furtherance, of any crime or fraud. An example of this might be where tax advice was sought ostensibly to enable the affairs of a tax evader to be regularised but in reality was sought to aid continued evasion by improving the evader’s understanding of the relevant issues.
- 7.43 The crime/fraud exception also applies where communication takes place between a *client* and his adviser in circumstances where the *client* is the innocent tool of a third party’s criminal or fraudulent purpose. An example of this might be where a money launderer gives money to a family member, who is unaware of the source of that money, to purchase a property, for which purpose he communicates with his adviser.
- 7.44 The crime/fraud exception does not apply where the adviser is approached to advise on the consequences of a crime or fraud or similar conduct that has already taken place and where the *client* has no intention, in seeking advice, to further that crime or fraud. This means that a person who is concerned that he may be guilty of tax evasion can approach a *tax adviser* for legal advice in this regard without fear of the exception being invoked. This remains the case even if the potential *client* declines a *client* relationship having received the advice, and the adviser does not know whether the person will proceed to rectify his affairs. However, if the person behaves in a way that makes the adviser suspicious that he intends to use the advice to further his evasion, then a *money laundering* report could be required.

7.45 The crime/fraud exception is a difficult area and the Courts will not usually allow the exception to be invoked unless there is reasonably compelling circumstantial evidence available that demonstrates that the communications have in some way been intended to further the crime or the fraud. A mere speculation may not be sufficient as a basis to invoke it. It is strongly recommended that professional or legal advice is sought in all cases of doubt.

7.46 In summary, the following issues need to be considered before deciding whether to apply the *privileged reporting exemption*:

- (a) Are those who received the information or other matter which gave rise to knowledge or suspicion of *money laundering relevant professional advisers* (s330(14) and s330(6)(b))?
- (b) Was the *relevant professional adviser* acting in privileged circumstances (s330(10))?
- (c) Was the information or other matter which gave rise to knowledge or suspicion of *money laundering* actually received in privileged circumstances (s330(10)) and not in some other communication or situation?
- (d) Was the information or other matter received or communicated with the intention of furthering a criminal purpose (*ie*, does the crime/fraud exception apply (s330(10))?)

If the answers to (a), (b), and (c) are yes, and the answer to (d) is no, the *privileged reporting exemption* must be applied. If the answer to (a), (b), and (c) are yes and the answer to (d) is yes, the crime fraud exception applies and a *money laundering* report must be made. Further advice should be sought from the relevant professional body or a lawyer in cases of doubt. This issue may be vital in balancing legal and professional requirements for confidentiality and for serving the public interest and the interests of *clients*. If doubts cannot be resolved through internal discussion, through access to normal sources of professional advice, *businesses* are strongly recommended to seek advice from a professional legal adviser with experience of these matters.

## SECTION 8 – CONSENT

### KEY POINTS

- If a *business* or an *individual* believes an activity they are going to undertake would constitute a *money laundering* offence under ss327-329 *POCA* then they must make an authorised disclosure under s338, *POCA* (or have a reasonable excuse for not having made such a report); and
- If the authorised report was made before the *money laundering* activity took place, the reporter must receive an appropriate *consent* (s335, *POCA*) before proceeding with the activity or an offence will be committed
- On receipt of the appropriate *consent* under s335, *POCA*, an *MLRO* may then provide this *consent* to the *business* under the provisions of s336, *POCA*
- Once a *consent* request is made, this may be granted by *SOCA* or given by default once 7 working days starting the working day after submission of the *consent* request (the 'notice period') has elapsed, or *consent* may be refused
- If *consent* is refused during the 7 working day notice period, a moratorium period of 31 days starts on the day notice of refusal is received during which the activity may not be undertaken unless and until the moratorium period expires.
- Once the moratorium has expired, then if no restraining action has been taken by law enforcement, the activity in question may be continued.

---

### MATTERS FOR CONSENT

- 8.1 The *MLRO* needs to consider carefully when preparing to make a *SAR* whether continuation of activity by the *business* in respect of the subject matter of the *SAR* may potentially involve the *business* in carrying out an act which would constitute a *money laundering* offence.
- 8.2 Whilst this, on the face of it, appears relatively unlikely in the context of the *defined services* there are situations where *consent* issues do arise and careful consideration should be given to this possibility.
- 8.3 Before applying for *consent* it is important to consider whether the proposed activity is a matter to which *SOCA* is empowered to *consent*. *SOCA*'s power is strictly limited to being able to *consent* to activity that would otherwise be an offence under any of ss327-329, *POCA*. In particular, it should be noted that *consent* may not be sought or given for offences under s333A, *POCA* (*tipping off*) or s342, *POCA* (*prejudicing an investigation*) or for any other *POCA* offence except those under ss327-329, *POCA*. As well as having only restricted powers to consent to *POCA* offences, it does not have the power to *consent* to an act which would otherwise constitute the commission of any other criminal offence. Accordingly, it cannot give *consent* to *eg*, an adviser knowingly submitting a false VAT return on behalf of a *client* as this would be a separate criminal offence on the part of the adviser as well as an offence under s328, *POCA*.
- 8.4 If in doubt as to whether a matter requires (or is eligible for) *consent* or not, either legal advice should be sought, or recourse had to helplines provided by the relevant supervisory bodies. Advice should not be sought from *SOCA* as they are not in a position to advise, although it will make clear if a matter falls outside of its powers.
- 8.5 Some of the more common instances where a *consent* may be required include:

- acting as an insolvency officeholder where there is knowledge or suspicion either that the assets may in whole or in part represent *criminal property*, or where the insolvent entity may enter into or become concerned in an arrangement under s328, *POCA*
- designing and implementing trust and company structures for *clients*, including acting as trustees or company officers, where there is knowledge or suspicion that these structures are being, or may be about to be, used to launder money;
- acting on behalf of the *client* in the negotiation and implementation of transactions where these involve an element of *criminal property* being either bought or sold by a *client*, for example corporate acquisitions;
- handling money in *client* accounts which is suspected to be of criminal origin; and
- providing outsourced business processing for *clients* where money is suspected to be of criminal origin.

- 8.6 There will be some cases where *businesses* consider they no longer wish to act for the *client* in question and will decline to conduct the requested activity and possibly terminate the relationship. This is a matter for the *business* and not a matter for *consent*. However, this is unlikely to be the case in terms of insolvency appointments, or when acting for the innocent purchaser of assets of suspicious origin. *Businesses* may on occasion decide that undertaking an activity which might otherwise constitute an offence under ss327-329, *POCA* may, at least in the short term, provided there is *consent*, be the most practical option even if there is no intention to continue acting for the *client* in the longer term. In particular, this might apply when monies are already held in *client* account and need to be returned to or paid away on the instructions of a known or suspected criminal and either a *consent* is required to enable transfer of monies away, or law enforcement confiscation activity is required to resolve the matter.
- 8.7 *Consent* requests must be clear as to the nature of the knowledge or suspicion of *money laundering* and specific as to the type and extent of the activity for which consent is requested, including how that activity would otherwise constitute an offence under ss327-329, *POCA*, or the *consent* request will not be accepted as a valid request by *SOCA* and no protection will be obtained.
- 8.8 *SOCA*'s priority in terms of dealing with *consent* issues are understandably focussed on those where there is an opportunity for law enforcement intervention either to confiscate assets or to prevent the commission of crime or acts of terrorism. Clearly, these may not entirely match with the priorities of the person requesting *consent*, who will be driven by *client* and transaction related considerations. To give the best chance of having a *consent* request processed rapidly, it is important to tick the *consent* box provided on the prescribed forms and it is recommended that any critical timescale attaching to the activity is explained clearly, and if the report is complex, a summary of key facts and the request is given at the beginning of the report, before explaining the supporting detail.
- 8.9 In terms of insolvency, *SOCA* are accustomed to dealing with *consent* requests from officeholders and, in general, officeholders should request *consent* to carry out their duties as an officeholder rather than attempting to request *consent* for specific transactions or activities. *SOCA* will try and provide a very rapid turnaround to such requests, as they recognise the unique position of a licensed officeholder acting as such. In order that *SOCA* can rapidly identify requests for *consent* from an insolvency officeholder, this should be made clear at the beginning of the report requesting *consent*, specifying the type of insolvency appointment as well as providing all the other required detail.

---

## CONSTRUCTIVE TRUST

- 8.10 Where *client* assets or monies are held, and in forming knowledge or suspicion of *money laundering* *businesses* become concerned about potential third party claims to the assets or monies, appropriately qualified legal or professional advice should be sought. This is a

complex area of law and any *SOCA consent* will not protect a *business* against the claims of a third party, but only against any accusation of *money laundering*. However, *SOCA* are aware of the need to avoid any unwarranted disadvantage accruing to the *regulated sector*, arising from issues of constructive trusts. Where constructive trusts could be an issue, *businesses* are strongly advised to draw this to the attention of *SOCA* when making a *SAR*, so that this can be taken into account in the way *SOCA* deals with the application for *consent*.

---

## SUSPENSION OF ACTIVITY

- 8.11 Once a *consent* request has been made, the process must be adhered to and the activity that would otherwise be a *money laundering offence* refrained from unless and until *consent* has been received (or the notice period expired), or in the event *consent* has been refused, until the moratorium period has expired. Failure to do so risks prosecution either for a *money laundering offence* and/or, in the case of an *MLRO* giving *consent* for an activity to continue before he is entitled to do so, an offence under s336 (5) punishable by imprisonment and/or a fine.
- 8.12 It is appreciated that it is extremely difficult, in some cases, to explain to *clients* and other parties why activity has ceased in an unexpected fashion. Whilst *SOCA* will make every reasonable effort to deliver a rapid *consent*, in some cases the full 7 working days will be taken before a decision is reached whilst the matter is considered with law enforcement, and the potential for intervention in terms of confiscation, arrest etc is considered.
- 8.13 There is nothing in the legislation which provides for how a *business* may/may not deal with the issues arising from delay. There is nothing which requires a *business* to lie to *clients* or other parties, and clearly to lie would be unacceptable conduct for a professional, but *businesses* must take into account the provisions of the offences concerning *tipping off* and *prejudicing an investigation* when informing parties of delays. If the delay is such as to cause the *client* or other parties to question the *business* as to the reasons for delay, *businesses* may be well advised simply and persistently to refuse to enter into any discussion of the matter and explain that, with regret, they are unable at this point to discuss the matter further. Clearly, this is not a form of behaviour or communication with *clients* that would normally be engaged in, but the period after a request for *consent* has been made is an exceptional period, although frequently of very short duration and manageable in the normal course of business.
- 8.14 In exceptional circumstances, where an unexpected delay in carrying out a service for a *client* is likely to *alert a money launderer*, in a way that could bring harm to an *individual* or the *business* or could materially undermine a criminal investigation, *MLROs* are recommended to ask *SOCA* to be put in touch with the Law Enforcement Authority dealing with the situation, to discuss the circumstances.

---

## APPLYING FOR AND RECEIVING CONSENT

- 8.15 *Consent* may only be requested on the basis of a properly submitted *SAR*, made under the provisions of s338, *POCA* (authorised disclosures). The 'consent required' option should be selected on all methods of submission to alert *SOCA* to the request and enable them to prioritise appropriately. In cases of real urgency, a telephone call may also be made to alert *SOCA* to any special circumstances.
- 8.16 The *consent* request should be clear as to the reasons for knowledge or suspicion, the intended activity, and the nature of the consent requested. Great care is needed when requesting consent to cover the extent of the intended activity in a way that makes it clear to *SOCA* exactly what is being requested. Too narrow a *consent* request may mean repeated requests will be required causing issues of cost and efficiency to the *business* and possibly unnecessary *client* service impact. Too broad or ill-defined a *consent* may

well result in SOCA having to refuse *consent* or possibly even determining the request is not validly made as it does not show clearly the act or acts to be undertaken which would otherwise be an offence under ss327-329, *POCA*.

- 8.17 *Consent* will frequently be received initially over the telephone from SOCA, and the name and contact number of the officer, and the *consent* reference should be noted on the *MLRO* records with the date and time of the call. Written confirmation ordinarily follows in due course but this may take several days and *MLROs* may rely on the telephone *consent*.
- 8.18 Once *consent* has been received by the *MLRO* under the provisions of s335 *POCA*, he should then (under the provisions of s336, *POCA*) promptly inform the engagement team affected and give them clearance to continue their work, and any other guidance they might require as regards *money laundering* matters.
- 8.19 If a period of 7 working days, starting the first working day after the *consent* request is made (the notice period), has elapsed with no refusal having been received, consent is deemed to have been given and the activity may be allowed to continue.

### **Refusal of consent**

- 8.20 If *consent* is refused during the notice period, then a further 31 days must elapse, starting with the day on which the consent is refused, before the activity may continue (the moratorium period). It may be that during either the notice period, or the moratorium period, that action is taken by law enforcement which means that the activity may no longer be able to be continued (eg, confiscation or other enforcement action may occur).
- 8.21 If no action has been taken to restrain the activity during the moratorium period, the activity may continue as planned.

---

### **EXEMPTIONS FOR BANKS AND DEPOSIT TAKERS**

- 8.22 The Serious Organised Crime and Police Act 2005 put in place a threshold provision in *POCA* (ss327-329) that allows banks and deposit takers to continue to operate an account with an activity which potentially constitutes *money laundering* provided this relates to transactions worth £250 or less or as laid down from time to time in statutory instruments. Note that this change does not affect the requirement to report suspicions, does not constitute a 'de-minimis' provision, and is **not** available to providers of *defined services*.<sup>8</sup>

---

<sup>8</sup> See JMLSG *Guidance* for details on the change in thresholds for banks and deposit taking institutions.

## SECTION 9 – POST SAR ACTIONS

### KEY POINTS

- Once a SAR has been submitted, the *business* needs to consider whether or not the content of the SAR requires any change to, or even cessation in, any related *client* relationship.
- In addition, careful consideration needs to be given to reconciling the need to fulfil professional duties, whilst avoiding the risks of *tipping off*.
- A SAR may be followed by requests for further information from law enforcement or prosecuting agencies, both informal and by means of relevant orders. *Businesses* need to have in place procedures for checking the validity of requests, and for ensuring a proper response is made.

---

### CONTINUING WORK IN CONNECTION WITH A REPORTED MATTER

#### Client relationships

- 9.1 *Businesses* do not have to stop working after submission of a SAR unless a *consent* has been requested, in which case all or part of *client* work may well require to be suspended until consent is received. In cases where *consent* has been requested and refused, the work which was the subject of the request will need to be suspended.
- 9.2 However, even where consent was not required, where a SAR involves a *client* as a suspect, *businesses* may wish to consider whether the behaviour observed is such that for professional reasons the *business* no longer wishes to act.
- 9.3 Generally, if following a report of suspicion a *business* wishes for its own commercial or ethical reasons to exit a relationship, there is nothing to prevent this provided the way the exit is communicated does not constitute *tipping off*. This also applies to the *prejudicing an investigation* offence outlined below.
- 9.4 If a decision is made to terminate a *client* relationship, a *business* should follow its normal procedures in this regard, whilst always bearing in mind the need to avoid *tipping off*.

#### Balancing professional work and POCA requirements

- 9.5 Normal commercial enquiries to understand a transaction carried out in the course of an engagement will not generally lead to *tipping off*, although care should be exercised to avoid either making a disclosure prohibited under ss333A-333D, POCA (see section 2.19 of this *Guidance*) or making accusations or suggesting that any person is guilty of an offence. It is important to confine enquiries to those required in the ordinary course of business and not attempt to investigate a matter unless that is within the scope of the professional work commissioned.
- 9.6 Continuation of work may require discussion with *client* senior management of matters relating to suspicions formed. This may be of particular importance in audit relationships. Care must be taken to select appropriate, and non-complicit, members of senior management for such discussion whilst always bearing in mind the need to avoid *tipping off*.
- 9.7 In more complex circumstances, consultation with law enforcement may be necessary before enquiries are continued, but in most cases a common sense approach will resolve the issue. Note that neither SOCA nor law enforcement may give consent to *tipping off*, but discussions with them are still valuable.

- 9.8 *Businesses* may wish to consult the *MLRO* or other suitable specialist (for example a solicitor) regularly if there are *tipping off* concerns, and in particular it is important that before any document referring to the subject matter of a report is released to a third party the *MLRO* is consulted and, in extreme cases, law enforcement. Some typical examples of documents released to third parties are shown below as an aide memoire:
- public audit or other attest reports;
  - public record reports to regulators;
  - confidential reports to regulators (eg to the *FSA* under relevant auditing standards);
  - provision of information to sponsors or other statements in connection with Rule 2.12 of the UK Stock Exchange Listing Rules;
  - reports under the Companies Directors Disqualification Act 1986;
  - reports under s218 of the Insolvency Act 1986;
  - Companies Act statements on resignation as auditors;
  - professional clearance/etiquette letters;
  - communications to *clients* of intention to resign.
- 9.9 In particular, audit resignations require statements to be filed at Companies House and the contents of such statements require careful consideration to ensure that statutory and professional duties are met, without including such information as may constitute *tipping off*. There is no legal mechanism for obtaining clearance from *SOCA* for the contents of such statements or other documents relating to resignation. However, *businesses* may well wish in cases of complexity to discuss the matter with *SOCA* or the relevant law enforcement agency in order to understand their perspective and document such discussion.
- 9.10 *MLROs* may on occasion need advice to assist them in formulating their instructions to the *business*. Legal advice may be sought from a suitably skilled and knowledgeable professional legal adviser, and recourse may also be had to helplines and support services provided by professional bodies. Discussion with *SOCA* and law enforcement may well be valuable, but *MLROs* should bear in mind these authorities are not able to advise, and nor are they entitled to dictate how professional relationships should be conducted.

---

## REQUESTS FOR FURTHER INFORMATION

### Requests from *SOCA* or Law Enforcement Agencies

- 9.11 *SOCA* or a Law Enforcement Authority may contact a *business* (usually the *MLRO*) or an *individual* to ask for further information about a *SAR* it/he has submitted. Before responding, it is recommended that a verification process is undertaken to ensure the person making contact is a bona fide member of *SOCA*/law enforcement. This may be most simply achieved by taking a caller's name and agency/force details, and then calling the main switchboard of the agency/force to be put through to the person.
- 9.12 To the extent that the request is simply aimed at clarifying the content of a *SAR*, *businesses/individuals* may respond without the need for any further process.
- 9.13 However, if the request is for production of documents, or provision of information additional to the *SAR*, it is recommended that *businesses/individuals* require the relevant agency to use its powers of compulsion before they respond. This is not intended to be non co-operative, and indeed *businesses/individuals* are recommended to engage in constructive dialogue with *SOCA*/law enforcement, including as to the content and drafting of the request, but is intended to protect *businesses/individuals* from allegations that they breached confidentiality. *Client* or other third party consent is not required in cases of compulsion, and nor should it be sought due to the risk of *tipping off*.

9.14 Before responding to orders for production of information, *businesses/individuals* should ensure they understand:

- the authority under which the request is made;
- the extent of the information requested;
- the required timing and manner of the production of information; and
- what information should be excluded eg, that subject to legal privilege,

If in any doubt, *businesses/individuals* should seek legal advice. *Businesses* should document their consideration of the issues.

9.15 None of the notices or orders will require the production of information that is subject to legal privilege or legal professional privilege. Terms used in the various relevant Acts of Parliament and the way the terms are defined vary slightly and it may be appropriate to take legal advice if unsure. The interaction of the *privilege reporting exemption* with the carve-outs for privileged material in the notices and orders outlined below is not clear, and has yet to be tested. This is a complex area of law. If *individuals* or *businesses* are unsure as to whether certain documents fall within the privileged category or not, they should not include these documents in initial disclosure and, before the expiry of the time allowed for disclosure, should inform the person to whom the information is to be provided that they believe they have material subject to privilege and request that, if they think it necessary to gain access to this material, the relevant agency appoint independent counsel to opine as to whether the material is disclosable, or not. The opinion of counsel may then be complied with.

9.16 Before passing across information to an officer, *businesses* should require the person identify themselves by eg showing a warrant card and a copy of the relevant order, or *businesses* may attend the premises of the relevant agency to hand over the information.

9.17 Orders for production of information may be received under a variety of legislation. In each case, production may be required in hard copy even where stored on a computer, or in electronic form where stored as such. Those which most commonly flow from SARs include the following:

- Production Orders under the provisions of *POCA*

Production Orders are made under s354, *POCA*, and are made only by a judge in respect of a confiscation investigation, or a *money laundering* investigation. The maximum period for compliance will be 7 days starting with the day on which the order is made unless the judge thinks a shorter period should be applied. Failure to comply is treated as breach of a Court Order and penalties will be applied as such. There is no requirement to produce documents which are privileged, being material which a person would be entitled to refuse to produce on grounds of privilege in the High Court. For the interaction of this provision with the *privilege reporting exemption*, see section 9.15 of this *Guidance*.

- Disclosure Notices under the provisions of *SOCPA*

A disclosure notice may be issued by an investigating authority (the Director of Public Prosecutions, the Director of Revenue and Customs Prosecutions and the Lord Advocate or their permitted delegates under s60, *SOCPA*) in respect of certain offences only. These are broadly those listed in Schedule 2 (Schedule 4 in Scotland) to *POCA*, offences under ss15-18, *TA 2000*, certain duty offences, false accounting (s17, Theft Act 1968 in England and Wales) and certain matters concerning attempts at/conspiracy to commit certain offences. S61, *SOCPA* should be referred to in the case of any such notice being received to check it is in respect of a qualifying offence. ss62-65, *SOCPA* then set out the procedures in respect of the issue of the notice, and the response to it. The provisions of the notice will govern the extent of the

information to be provided, and the timing, place and manner of disclosure. There is no requirement to produce documents or answer questions where the matter is subject to legal professional privilege, or legal privilege (as defined in s412, POCA). For the interaction of this provision with the *privilege reporting exemption*, see section 9.15. Failure, without reasonable excuse, to comply is a criminal offence and penalties of up to two years imprisonment and/or an unlimited fine may be levied.

- S2 notices issued by the Serious Fraud Office under the provisions of the Criminal Justice Act 1987.

Under s2, Criminal Justice Act 1987, staff authorised by the Director of the Serious Fraud Office have powers to require a person to answer questions, provide information or produce documents for the purposes of an investigation. Written notice is given where the Serious Fraud Office exercise these powers. In urgent cases, the Serious Fraud Office may require immediate compliance with a notice, but frequently will give a period of time for compliance. There is no requirement to produce documents which are privileged, being material which a person would be entitled to refuse to produce on grounds of privilege in the High Court. Failure to comply is a criminal offence punishable with imprisonment for up to 6 months and/or a fine not exceeding level 5 on the standard scale. For the interaction of this provision with the *privilege reporting exemption*, see section 9.15 of this *Guidance*.

## **Requests arising from a change of professional advisor (professional enquiries)**

### Requests regarding identification information

- 9.18 In such a case the disclosure request may be made under the provisions of Regulation 17, reliance, or the new adviser may simply want copies of identification evidence, in order to assist it in satisfying its own identification procedures. *Businesses* should not release confidential information without the *client's* consent. If reliance is being placed on the *business*, it should follow the guidance in section 5.36 above in relation to record keeping.

### Requests for information regarding suspicious activity

- 9.19 In general, it is recommended that such requests are declined as the *tipping off* offence in the *regulated sector* greatly restricts the ability to make such disclosures. However, to the extent that the request is within the provisions of s333C, POCA (section 2.19 of this *Guidance*) information may be provided (but there is no obligation to do so).

## **Data Protection Act - Subject Access Requests**

- 9.20 Under the Data Protection Act 1998 *businesses* are exempted from disclosure under a subject access request where disclosure would be or is likely to be prejudicial to the prevention or detection of crime or the capture or conviction of offenders. Where personal data is held on a subject and relates to knowledge or suspicion of *money laundering* (ie, it has been processed for the purpose of the prevention or detection of crime) it is not required to be disclosed under a subject access request if disclosure may constitute a *tipping off* offence. This exception should be applied to internal **and** SAR reporting records.
- 9.21 Guidance has been issued by HM Treasury ([www.hm-treasury.gov.uk/media/D/F/money\\_laundering.pdf](http://www.hm-treasury.gov.uk/media/D/F/money_laundering.pdf)) supporting the position that where granting access would amount to '*tipping off*' then the s29 Data Protection Act exemption would apply.

9.22 It is recommended that *businesses* document any considerations surrounding the decision to grant or refuse access to information requested in such circumstances (known as a 'subject access request').

## GLOSSARY

<i>2007 Regulations</i>	Statutory Instrument 2007 no 2157 - Financial Services “The Money Laundering Regulations 2007”
<i>Alerting a money launderer</i>	Disclosures that do not constitute <i>tipping off</i> but which nonetheless alert the money launderer to the suspicion regarding their activities.
<i>Accountancy Services</i>	<i>Accountancy services</i> includes for the purpose of this <i>Guidance</i> any service provided under a contract for services (ie, not a contract of employment) which pertains to the recording, review, analysis, calculation or reporting of financial information.
<i>Anti-Money Laundering Supervisory Authority</i>	Bodies identified by Regulation 23, <i>2007 Regulations</i> as being empowered to supervise the compliance of <i>individuals</i> and <i>businesses</i> with the <i>2007 Regulations</i> . The professional bodies designated as <i>anti-money laundering supervisory authorities</i> are listed in Schedule 3 to the <i>2007 Regulations</i> .
<i>Businesses</i>	A company, partnership or other organisation undertaking <i>defined services</i> . This includes accountancy practices, whether structured as partnerships, sole practitioners or corporate practices.
<i>Business relationship</i>	A business, professional or commercial relationship between a relevant person (ie someone to whom the Regulations 2007 apply) and a customer, which is expected by the relevant person, at the time when the contact is established, to have an element of duration.
CCAB	Consultative Committee of Accountancy Bodies: body representing the Institute of Chartered Accountants in England and Wales; the Institute of Chartered Accountants of Scotland; the Institute of Chartered Accountants in Ireland; the Association of Chartered Certified Accountants; the Chartered Institute of Management Accountants; and the Chartered Institute of Public and Finance and Accountancy.
<i>Client</i>	A person in a <i>business relationship</i> , or carrying out an occasional transaction, with a <i>business</i> .
<i>Consent</i>	Permission given, generally by SOCA, for the carrying out of any action that would constitute a <i>money laundering</i> offence in the absence of that permission. The definition and ruling legislation for the giving of consent is in s335, <i>POCA</i> , which also deals with the passing of the consent from the <i>MLRO</i> to the <i>individual</i> concerned (s336).
<i>Credit institution</i>	Has the meaning given by Regulation 3(2), <i>2007 Regulations</i> .
<i>Criminal Conduct</i>	Conduct that is an offence in any part of the UK as well as conduct occurring elsewhere that would have been an offence if it had taken place in the UK. There are very limited exceptions to this for conduct which is both known to be legal in the country in which it is committed and which falls within the specific exceptions set out in orders made by the Secretary of State.
<i>Criminal Property</i>	The benefit of <i>criminal conduct</i> where the alleged offender knows or suspects that the property in question represents such a benefit (s340, <i>POCA</i> )
<i>Customer due diligence</i>	The process by which KYC information is gathered, and the identity of a <i>client</i> is established and verified, for both new and existing clients.
<i>Defined services</i>	Activities carried on, in the course of business by <i>businesses</i> or <i>individuals</i> as an auditor, <i>external accountant</i> , <i>insolvency practitioner</i> or <i>tax adviser</i> (Regulation 3(c), <i>2007 Regulations</i> ), or as trust and company service providers

(Regulation 3(e), *2007 Regulations*). It also includes persons providing services under the Designated Professional Body provisions of Part XX, s326 *FSMA 2000* or otherwise providing financial services under the oversight of their professional body.

<i>EEA</i>	European Economic Area countries, which are the European Union member states plus EFTA (European Free Trade Association) member states.
<i>Enhanced due diligence</i>	Additional due diligence steps that must be applied in situations where there is a higher risk of <i>money laundering</i> or <i>terrorist financing</i> and in a number of specific situations (Regulation 14), of which two are relevant to providers of <i>defined services</i> ; where the <i>client</i> has not been physically present for identification purposes, if a <i>business relationship</i> or occasional transaction is to be undertaken with a politically exposed person ( <i>PEP</i> ).
<i>External accountant</i>	Means a firm or sole practitioner who by way of business provides <i>accountancy services</i> to other persons, when providing such services (Regulation 3(7), <i>2007 Regulations</i> ).
<i>FATF</i>	Financial Action Task Force, created by G7 nations to fight money laundering.
<i>Financial institution</i>	Has the meaning given by Regulation 3(3), <i>2007 Regulations</i>
<i>FSA</i>	Financial Services Authority: statutory regulator of most financial services providers under the Financial Services and Markets Act 2000.
<i>FSMA 2000</i>	Financial Services and Markets Act 2000
<i>Guidance</i>	<p><i>Guidance</i> which is</p> <ul style="list-style-type: none"><li>(a) issued by a supervisory authority or any other appropriate body;</li><li>(b) approved by the Treasury; and</li><li>(c) published in a manner approved by the Treasury as suitable in their opinion to bring the <i>Guidance</i> to the attention of persons likely to be affected by it.</li></ul> <p>In this <i>Guidance</i>, the term has been used for <i>Guidance</i> for which Treasury approval has been applied, and is expected to be obtained, as well as that which already has Treasury approval. The circumstances in which Courts and others are required to take the <i>Guidance</i> into account in determining whether an offence has been committed are set out in <i>POCA</i> and the <i>2007 Regulations</i>.</p> <p>Any use of the term “guidance” outside this definition, has not been italicised in this <i>Guidance</i>.</p>
<i>Individuals</i>	Includes sole practitioners and the partners, directors, subcontractors, consultants and employees of <i>businesses</i> .
<i>Independent legal professional</i>	Provider of legal or notarial services as defined in Regulation 3(9) in the 2007 Regulations.
<i>Internal Report</i>	A report made to the <i>MLRO</i> in a <i>business</i> .
<i>Insolvency practitioner</i>	Means any person who acts as an <i>insolvency practitioner</i> within the meaning of s 388 Insolvency Act 1986 or Article 3 of the Insolvency (Northern Ireland) Order 1989 (Regulation 3(6), <i>2007 Regulations</i> ).
<i>JMLSG</i>	Joint Money Laundering Steering Group: body representing UK Trade Associations in the Financial Services Industry and aiming to promote good anti- <i>money laundering</i> practices and give relevant practical <i>Guidance</i> .
<i>Money</i>	For the purposes of this <i>Guidance</i> , <i>money laundering</i> is defined to include those offences relating to terrorist finance, which require to be <i>reported</i> under

<i>laundrying</i>	the <i>TA 2000</i> , as well as the <i>money laundrying offences</i> as defined in <i>POCA</i> .
<i>Money laundrying directive</i>	References in this <i>Guidance</i> are to the 3 <sup>rd</sup> Money Laundrying Directive (DIRECTIVE 2005/60/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundrying and terrorist financing) available from: <a href="http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l_309/l_30920051125en00150036.pdf">http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l_309/l_30920051125en00150036.pdf</a>
<i>MLRO</i>	Money Laundrying Reporting Officer. This term is used to describe the <i>nominated officer</i> appointed under Regulation 20(2)(d), <i>2007 Regulations</i> and as referred to in s331, <i>POCA</i> .
<i>Money Laundrying Reporting Officer</i>	see <i>MLRO</i> above
<i>Money laundrying offences</i>	One of the three <i>money laundrying offences</i> defined under ss327-329, <i>POCA</i> . In summary the offences comprise the following activities, where a person: <ul style="list-style-type: none"> <li>• <b>conceals</b>, disguises, converts or transfers <i>criminal property</i>, or removes <i>criminal property</i> from England and Wales, or from Scotland or from Northern Ireland (s327);</li> <li>• enters into or becomes concerned in an <b>arrangement</b> which he knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of <i>criminal property</i> by or on behalf of another person (s328); or</li> <li>• <b>acquires</b>, uses or has possession of <i>criminal property</i> except where adequate consideration was given for the property (s329).</li> </ul>
<i>Nominated Officer</i>	Office required to be appointed by <i>businesses</i> carrying on business in the <i>regulated sector</i> . See <i>MLRO</i> above.
<i>Overseas conduct exemption</i>	Exemption from reporting requirement where an act is reasonably believed to have taken place outside of the UK, and the act was known to be lawful when committed under the criminal law of the place where the act was committed, and the maximum sentence if the act had been committed in the UK would have been less than 12 months (except in the case of an act which would be an offence under the Gaming Act 1968, the Lotteries and Amusements Act 1976 or under ss23 or 25, <i>FSMA</i> ).
<i>PEPs</i>	Politically exposed persons, as defined in the <i>2007 Regulations</i> paragraph 14(5) and paragraph 4(1)(a) of Schedule 2. See also sections 5.27 to 5.29 above.
<i>POCA</i>	Proceeds of Crime Act 2002
<i>Prejudicing an investigation</i>	A ‘related’ <i>money laundrying</i> offence, defined under s342, <i>POCA</i> . In summary, it captures the making of any disclosure that is likely to prejudice an investigation or falsifying, concealing, or destroying, any documents that are relevant to a <i>money laundrying</i> investigation, or being complicit in such behaviour.
<i>Predicate offence</i>	Means the underlying offence or any <a href="#">offence</a> as a result of which <i>criminal property</i> has been generated.
<i>Privilege reporting exemption</i>	An exemption from reporting suspicions formed on the basis of information received in privileged circumstances (see Sections 7.26-7.46 of this <i>Guidance</i> ).
<i>Regulated investment</i>	Within the EEA, has the meaning given by point 14 of Article 4(1) of the Markets in Financial Instruments Directive (MiFID); and outside the EEA,

<i>market</i>	means a regulated financial market 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 obligations.
<i>Regulated Sector</i>	Defined in Proceeds of Crime Act Schedule 9 Part 1 (includes those who provide the <i>defined services</i> ).
<i>Relevant professional adviser</i>	An accountant, auditor or <i>tax adviser</i> who is a member of a professional body which is established for accountants, auditors or <i>tax advisers</i> (as the case may be); and which makes provision for (a) testing the competence of those seeking admission to membership of such a body as a condition for such admission; and (b) imposing and maintaining professional and ethical standards for its members, as well as imposing sanctions for non-compliance with those standards.
<i>Required Disclosure</i>	The identity of the suspect (if known), the information or other matter on which the knowledge or suspicion of <i>money laundering</i> (or reasonable grounds for such) is based and the whereabouts of the laundered property (if known).
<i>SAR</i>	Suspicious activity report made to SOCA
<i>SAR Glossary of Terms</i>	Glossary of terms used by SOCA to assist in relating/providing a theme to different SARs to increase effective mining of data by SOCA and Law Enforcement. The use of the terms is not mandatory.
<i>Shell bank</i>	means a <i>credit institution</i> , or an institution engaged in equivalent activities, incorporated in a jurisdiction in which it has no physical presence involving meaningful decision-making and management, and which is unaffiliated with a regulated financial group
<i>Simplified due diligence</i>	The phrase used in the <i>2007 Regulations</i> (Regulation 13) which means that a <i>business</i> is not required to apply the <i>customer due diligence</i> measures set out in Regulation 7 where the <i>business</i> has reasonable grounds for believing that a <i>client</i> falls into the relevant categories.
<i>SOCA</i>	Serious Organised Crime Agency. SOCA is an intelligence-led agency with law enforcement powers, responsible for reducing the social and individual harm of serious organised crime. Reports of known or suspected <i>money laundering</i> must be made to SOCA.
<i>SOCPA</i>	Serious Organised Crime and Police Act 2005
<i>Specified disclosure obligations</i>	See Annex A to the Glossary
<i>Specified interest</i>	<p>A vested interest which is:</p> <ul style="list-style-type: none"> <li>• in possession or in remainder or reversion (or, in Scotland, in fee); and</li> <li>• defeasible or indefeasible.</li> </ul> <p>A 'vested interest' is an interest which to which an entitlement already exists (whether immediately - 'in possession'; or in the future, following the ending of another interest - 'in remainder' or 'in reversion'). It is in contrast to an interest which is merely 'contingent'; a contingent interest is an interest which will only arise on the happening of a particular event, such as surviving to a particular date or surviving a particular person. Determining whether an interest is vested or contingent requires careful analysis. For example, if a trust provides that A has a life interest, and that B has an interest which takes effect on A's death, both A and B will have vested interests and, if B does not survive A, B's interest will devolve as part of B's estate; however, if B's interest is expressed to take effect on A's death only if he (B) is then living, B's interest (which will fail if he</p>

predeceases A) is merely contingent.

A defeasible interest is one which may be defeated, generally by the exercise of a power under the trust deed; an indefeasible interest is one which cannot be defeated. In the examples given above, A and B both have indefeasible interests. It is important that a defeasible vested interest is not mistaken for a contingent interest. A defeasible vested interest will take effect unless and until it is defeated; a contingent interest on the other hand will not take effect unless and until the event on which it is contingent arises.

<i>Suspicious Activity Report</i>	Otherwise known as a <i>SAR</i> . See <i>SAR above</i>
<i>TA 2000</i>	The Terrorism Act 2000 (as amended by the Anti-Terrorism, Crime and Security Act 2001 and the Terrorism Act 2006)
<i>TA 2006</i>	The Terrorism Act 2006
<i>Tax adviser</i>	Means a firm or sole practitioner who by way of business provides advice about the tax affairs of to persons, when providing such services (Regulation 3(8), <i>2007 Regulations</i> ). Tax compliance services, ie, assisting in the completion and submission of tax returns is, for the purpose of this <i>Guidance</i> , included within the term "advice about the tax affairs of another person".
<i>Terrorist financing</i>	Means an offence under (Regulation 2 <i>2007 Regulations</i> ): (a) s15 (fund raising), 16 (use and possession, 17 (funding arrangements), 18 (money laundering) or 63 (terrorist finance: jurisdiction), <i>TA 2000</i> ; (b) para 7(2) or (3), Schedule 3 to the Anti-Terrorism, Crime and Security Act 2001(a) (freezing orders); (c) article 7, 8 or 10 of the Terrorism (United Nations Measures) Order 2006(b); or (d) article 7, 8 or 10 of the Al-Qaida and Taliban (United Nations Measures) Order 2006(c).
<i>Terrorist offences</i>	The terrorist offences relate to fundraising (inviting another to provide money or other property with the intention or reasonable cause to suspect it is intended to be used for the purposes of terrorism), using or possessing terrorist funds (receiving or possessing money or other property with the intention or reasonable cause to suspect it is intended to be used for the purposes of terrorism), entering into funding arrangements (making arrangements as a result of which money or other property is or may be made available for the purposes of terrorism with the intention or reasonable cause to suspect it is intended to be used for the purposes of terrorism), money laundering, disclosing information relating to the commission of an offence (similar to <i>tipping off</i> ), or failing to make a disclosure in the regulated sector. (ss19 and 21A <i>TA 2000</i> (as amended))
<i>Terrorist property</i>	Means: (a) money or other property which is likely to be used for the purposes of terrorism (including any resources of a proscribed organisation), (b) proceeds of the commission of acts of terrorism, and (c) proceeds of acts carried out for the purposes of terrorism.
<i>Tipping off</i>	A 'related' <i>money laundering</i> offence, defined under s333, <i>POCA</i> for the non-regulated sector and (until the relevant statutory instrument abolishing this offence comes into force) in s 333A-D for the regulated sector.
<i>Transaction</i>	The provision of any advice by a <i>business</i> or <i>individual</i> to a <i>client</i> by way of

business, or the handling of the *client's* finances by way of business.

## Glossary Annex A – The Specified Disclosure Obligations

### DETAILS OF THE “SPECIFIED DISCLOSURE OBLIGATIONS” REFERRED TO IN REGULATION 13 (3) MLR2007 RE SIMPLIFIED DUE DILIGENCE

DIRECTIVE 2003/6/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 28 January 2003 on insider dealing and market manipulation (market abuse)

#### Article 6

1. Member States shall ensure that issuers of financial instruments inform the public as soon as possible of inside information which directly concerns the said issuers.

Without prejudice to any measures taken to comply with the provisions of the first subparagraph, Member States shall ensure that issuers, for an appropriate period, post on their Internet sites all inside information that they are required to disclose publicly.

2. An issuer may under his own responsibility delay the public disclosure of inside information, as referred to in paragraph 1, such as not to prejudice his legitimate interests provided that such omission would not be likely to mislead the public and provided that the issuer is able to ensure the confidentiality of that information. Member States may require that an issuer shall without delay inform the competent authority of the decision to delay the public disclosure of inside information.

3. Member States shall require that, whenever an issuer, or a person acting on his behalf or for his account, discloses any inside information to any third party in the normal exercise of his employment, profession or duties, as referred to in Article 3(a), he must make complete and effective public disclosure of that information, simultaneously in the case of an intentional disclosure and promptly in the case of a non-intentional disclosure.

The provisions of the first subparagraph shall not apply if the person receiving the information owes a duty of confidentiality, regardless of whether such duty is based on a law, on regulations, on articles of association or on a contract.

Member States shall require that issuers, or persons acting on their behalf or for their account, draw up a list of those persons working for them, under a contract of employment or otherwise, who have access to inside information. Issuers and persons acting on their behalf or for their account shall regularly update this list and transmit it to the competent authority whenever the latter requests it.

4. Persons discharging managerial responsibilities within an issuer of financial instruments and, where applicable, persons closely associated with them, shall, at least, notify to the competent authority the existence of transactions conducted on their own account relating to shares of the said issuer, or to derivatives or other financial instruments linked to them. Member States shall ensure that public access to information concerning such transactions, on at least an individual basis, is readily available as soon as possible.

DIRECTIVE 2003/71/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 4 November 2003 on the prospectus to be published when securities are offered to the public or admitted to trading and amending Directive 2001/34/EC

#### Article 3

Obligation to publish a prospectus

1. Member States shall not allow any offer of securities to be made to the public within their territories without prior publication of a prospectus.

2. The obligation to publish a prospectus shall not apply to the following types of offer:

(a) an offer of securities addressed solely to qualified investors; and/or  
(b) an offer of securities addressed to fewer than 100 natural or legal persons per Member State, other than qualified investors; and/or

(c) an offer of securities addressed to investors who acquire securities for a total consideration of at least EUR 50000 per investor, for each separate offer; and/or

(d) an offer of securities whose denomination per unit amounts to at least EUR 50000; and/or

(e) an offer of securities with a total consideration of less than EUR 100000, which limit shall be calculated over a period of 12 months.

However, any subsequent resale of securities which were previously the subject of one or more of the types of offer mentioned in this paragraph shall be regarded as a separate offer and the definition set out in Article 2(1)(d) shall apply for the purpose of deciding whether that resale is an offer of securities to the public. The placement of securities through financial intermediaries shall be subject to publication of a prospectus if none of the conditions (a) to (e) are met for the final placement.

3. Member States shall ensure that any admission of securities to trading on a regulated market situated or operating within their territories is subject to the publication of a prospectus.

#### Article 5

##### The prospectus

1. Without prejudice to Article 8(2), the prospectus shall contain all information which, according to the particular nature of the issuer and of the securities offered to the public or admitted to trading on a regulated market, is necessary to enable investors to make an informed assessment of the assets and liabilities, financial position, profit and losses, and prospects of the issuer and of any guarantor, and of the rights attaching to such securities. This information shall be presented in an easily analysable and comprehensible form.

2. The prospectus shall contain information concerning the issuer and the securities to be offered to the public or to be admitted to trading on a regulated market. It shall also include a summary. The summary shall, in a brief manner and in non-technical language, convey the essential characteristics and risks associated with the issuer, any guarantor and the securities, in the language in which the prospectus was originally drawn up. The summary shall also contain a warning that:

(a) it should be read as an introduction to the prospectus;

(b) any decision to invest in the securities should be based on consideration of the prospectus as a whole by the investor;

(c) where a claim relating to the information contained in a prospectus is brought before a court, the plaintiff investor might, under the national legislation of the Member States, have to bear the costs of translating the prospectus before the legal proceedings are initiated; and  
(d) civil liability attaches to those persons who have tabled the summary including any translation thereof, and applied for its notification, but only if the summary is misleading, inaccurate or inconsistent when read together with the other parts of the prospectus.

Where the prospectus relates to the admission to trading on a regulated market of non-equity securities having a denomination of at least EUR 50000, there shall be no requirement to provide a summary except when requested by a Member State as provided for in Article 19(4).

3. Subject to paragraph 4, the issuer, offeror or person asking for the admission to trading on a regulated market may draw up the prospectus as a single document or separate documents. A prospectus composed of separate documents shall divide the required information into a registration document, a securities note and a summary note. The registration document shall contain the information relating to the issuer. The securities note shall contain the information concerning the securities offered to the public or to be admitted to trading on a regulated market.

4. For the following types of securities, the prospectus can, at the choice of the issuer, offeror or person asking for the admission to trading on a regulated market consist of a base prospectus containing all relevant information concerning the issuer and the securities offered to the public or to be admitted to trading on a regulated market:

(a) non-equity securities, including warrants in any form, issued under an offering programme;

(b) non-equity securities issued in a continuous or repeated manner by credit institutions,

(i) where the sums deriving from the issue of the said securities, under national legislation, are placed in assets which provide sufficient coverage for the liability deriving from securities until their maturity date;

(ii) where, in the event of the insolvency of the related credit institution, the said sums are intended, as a priority, to repay the capital and interest falling due, without prejudice to the provisions of Directive 2001/24/EC of the European Parliament and of the Council of 4 April 2001 on the reorganisation and winding up of credit institutions(14).

The information given in the base prospectus shall be supplemented, if necessary, in accordance with Article 16, with updated information on the issuer and on the securities to be offered to the public or to be admitted to trading on a regulated market.

If the final terms of the offer are not included in either the base prospectus or a supplement, the final terms shall be provided to investors and filed with the competent authority when each public offer is made as soon as practicable and if possible in advance of the beginning of the offer. The provisions of Article 8(1)(a) shall be applicable in any such case.

5. In order to take account of technical developments on financial markets and to ensure uniform application of this Directive, the Commission shall, in accordance with the procedure referred to in Article 24(2), adopt implementing measures concerning the format of the prospectus or base prospectus and supplements.

#### Article 7

##### Minimum information

1. Detailed implementing measures regarding the specific information which must be included in a prospectus, avoiding duplication of information when a prospectus is composed of separate documents, shall be adopted by the Commission in accordance with the procedure referred to in Article 24(2). The first set of implementing measures shall be adopted by 1 July 2004.

2. In particular, for the elaboration of the various models of prospectuses, account shall be taken of the following:

(a) the various types of information needed by investors relating to equity securities as compared with non-equity securities; a consistent approach shall be taken with regard to information required in a prospectus for securities which have a similar economic rationale, notably derivative securities;

(b) the various types and characteristics of offers and admissions to trading on a regulated market of non-equity securities. The information required in a prospectus shall be appropriate from the point of view of the investors concerned for non-equity securities having a denomination per unit of at least EUR 50000;

(c) the format used and the information required in prospectuses relating to non-equity securities, including warrants in any form, issued under an offering programme;

(d) the format used and the information required in prospectuses relating to non-equity securities, in so far as these securities are not subordinated, convertible, exchangeable, subject to subscription or acquisition rights or linked to derivative instruments, issued in a continuous or repeated manner by entities authorised or regulated to operate in the financial markets within the European Economic Area;

(e) the various activities and size of the issuer, in particular SMEs. For such companies the information shall be adapted to their size and, where appropriate, to their shorter track record;

(f) if applicable, the public nature of the issuer.

3. The implementing measures referred to in paragraph 1 shall be based on the standards in the field of financial and non-financial information set out by international securities commission organisations, and in particular by IOSCO and on the indicative Annexes to this Directive.

#### Article 8

##### Omission of information

1. Member States shall ensure that where the final offer price and amount of securities which will be offered to the public cannot be included in the prospectus:

(a) the criteria, and/or the conditions in accordance with which the above elements will be determined or, in the case of price, the maximum price, are disclosed in the prospectus; or

(b) the acceptances of the purchase or subscription of securities may be withdrawn for not less than two working days after the final offer price and amount of securities which will be offered to the public have been filed.

The final offer price and amount of securities shall be filed with the competent authority of the home Member State and published in accordance with the arrangements provided for in Article 14(2).

2. The competent authority of the home Member State may authorise the omission from the prospectus of certain information provided for in this Directive or in the implementing measures referred to in Article 7(1), if it considers that:

(a) disclosure of such information would be contrary to the public interest; or

(b) disclosure of such information would be seriously detrimental to the issuer, provided that the omission would not be likely to mislead the public with regard to facts and circumstances essential for an informed assessment of the issuer, offeror or guarantor, if any, and of the rights attached to the securities to which the prospectus relates; or

(c) such information is of minor importance only for a specific offer or admission to trading on a regulated market and is not such as will influence the assessment of the financial position and prospects of the issuer, offeror or guarantor, if any.

3. Without prejudice to the adequate information of investors, where, exceptionally, certain information required by implementing measures referred to in Article 7(1) to be included in a prospectus is inappropriate to the issuer's sphere of activity or to the legal form of the issuer or to the securities to which the prospectus relates, the prospectus shall contain information equivalent to the required information. If there is no such information, this requirement shall not apply.

4. In order to take account of technical developments on financial markets and to ensure uniform application of this Directive, the Commission shall, in accordance with the procedure referred to in Article 24(2), adopt implementing measures concerning paragraph 2.

#### Article 10

##### Information

1. Issuers whose securities are admitted to trading on a regulated market shall at least annually provide a document that contains or refers to all information that they have published or made available to the public over the preceding 12 months in one or more Member States and in third countries in compliance with their obligations under Community and national laws and rules dealing with the regulation of securities, issuers of securities and securities markets. Issuers shall refer at least to the information required pursuant to company law directives, Directive 2001/34/EC and Regulation (EC) No 1606/2002 of the European Parliament and of the Council of 19 July 2002 on the application of international accounting standards(15).

2. The document shall be filed with the competent authority of the home Member State after the publication of the financial statement. Where the document refers to information, it shall be stated where the information can be obtained.

3. The obligation set out in paragraph 1 shall not apply to issuers of non-equity securities whose denomination per unit amounts to at least EUR 50000.

4. In order to take account of technical developments on financial markets and to ensure uniform application of this Directive, the Commission may, in accordance with the procedure referred to in Article 24(2), adopt implementing measures concerning paragraph 1. These measures will relate only to the method of publication of the disclosure requirements mentioned in paragraph 1 and will not entail new disclosure requirements. The first set of implementing measures shall be adopted by 1 July 2004.

#### Article 14

##### Publication of the prospectus

1. Once approved, the prospectus shall be filed with the competent authority of the home Member State and shall be made available to the public by the issuer, offeror or person asking for admission to trading on a regulated market as soon as practicable and in any case, at a reasonable time in advance of, and at the latest at the beginning of, the offer to the public or the admission to trading of the securities involved. In addition, in the case of an initial public offer of a class of shares not already admitted to trading on a regulated market that is to be admitted to trading for the first time, the prospectus shall be available at least six working days before the end of the offer.

2. The prospectus shall be deemed available to the public when published either:

(a) by insertion in one or more newspapers circulated throughout, or widely circulated in, the Member States in which the offer to the public is made or the admission to trading is sought; or

(b) in a printed form to be made available, free of charge, to the public at the offices of the market on which the securities are being admitted to trading, or at the registered office of the issuer and at the offices of the financial intermediaries placing or selling the securities, including paying agents; or

(c) in an electronic form on the issuer's website and, if applicable, on the website of the financial intermediaries placing or selling the securities, including paying agents; or

(d) in an electronic form on the website of the regulated market where the admission to trading is sought; or

(e) in electronic form on the website of the competent authority of the home Member State if the said authority has decided to offer this service.

A home Member State may require issuers which publish their prospectus in accordance with (a) or (b) also to publish their prospectus in an electronic form in accordance with (c).

3. In addition, a home Member State may require publication of a notice stating how the prospectus has been made available and where it can be obtained by the public.
4. The competent authority of the home Member State shall publish on its website over a period of 12 months, at its choice, all the prospectuses approved, or at least the list of prospectuses approved in accordance with Article 13, including, if applicable, a hyperlink to the prospectus published on the website of the issuer, or on the website of the regulated market.
5. In the case of a prospectus comprising several documents and/or incorporating information by reference, the documents and information making up the prospectus may be published and circulated separately provided that the said documents are made available, free of charge, to the public, in accordance with the arrangements established in paragraph 2. Each document shall indicate where the other constituent documents of the full prospectus may be obtained.
6. The text and the format of the prospectus, and/or the supplements to the prospectus, published or made available to the public, shall at all times be identical to the original version approved by the competent authority of the home Member State.
7. Where the prospectus is made available by publication in electronic form, a paper copy must nevertheless be delivered to the investor, upon his request and free of charge, by the issuer, the offeror, the person asking for admission to trading or the financial intermediaries placing or selling the securities.
8. In order to take account of technical developments on financial markets and to ensure uniform application of the Directive, the Commission shall, in accordance with the procedure referred to in Article 24(2), adopt implementing measures concerning paragraphs 1, 2, 3 and 4. The first set of implementing measures shall be adopted by 1 July 2004.

#### Article 16

##### Supplements to the prospectus

1. Every significant new factor, material mistake or inaccuracy relating to the information included in the prospectus which is capable of affecting the assessment of the securities and which arises or is noted between the time when the prospectus is approved and the final closing of the offer to the public or, as the case may be, the time when trading on a regulated market begins, shall be mentioned in a supplement to the prospectus. Such a supplement shall be approved in the same way in a maximum of seven working days and published in accordance with at least the same arrangements as were applied when the original prospectus was published. The summary, and any translations thereof, shall also be supplemented, if necessary to take into account the new information included in the supplement.
2. Investors who have already agreed to purchase or subscribe for the securities before the supplement is published shall have the right, exercisable within a time limit which shall not be shorter than two working days after the publication of the supplement, to withdraw their acceptances.

DIRECTIVE 2004/109/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL  
of 15 December 2004 on the harmonisation of transparency requirements in relation to  
information about issuers whose securities are admitted to trading on a regulated market  
and amending Directive 2001/34/EC

#### Article 4

##### Annual financial reports

1. The issuer shall make public its annual financial report at the latest four months after the end of each financial year and shall ensure that it remains publicly available for at least five years.
2. The annual financial report shall comprise:
  - (a) the audited financial statements;
  - (b) the management report; and
  - (c) statements made by the persons responsible within the issuer, whose names and functions shall be clearly indicated, to the effect that, to the best of their knowledge, the financial statements prepared in accordance with the applicable set of accounting standards give a true and fair view of the assets, liabilities, financial position and profit or loss of the issuer and the undertakings included in the consolidation taken as a whole and that the management report includes a fair review of the development and performance of the

business and the position of the issuer and the undertakings included in the consolidation taken as a whole, together with a description of the principal risks and uncertainties that they face.

3. Where the issuer is required to prepare consolidated accounts according to the Seventh Council Directive 83/349/EEC of 13 June 1983 on consolidated accounts [15], the audited financial statements shall comprise such consolidated accounts drawn up in accordance with Regulation (EC) No 1606/2002 and the annual accounts of the parent company drawn up in accordance with the national law of the Member State in which the parent company is incorporated.

Where the issuer is not required to prepare consolidated accounts, the audited financial statements shall comprise the accounts prepared in accordance with the national law of the Member State in which the company is incorporated.

4. The financial statements shall be audited in accordance with Articles 51 and 51a of the Fourth Council Directive 78/660/EEC of 25 July 1978 on the annual accounts of certain types of companies [16] and, if the issuer is required to prepare consolidated accounts, in accordance with Article 37 of Directive 83/349/EEC.

The audit report, signed by the person or persons responsible for auditing the financial statements, shall be disclosed in full to the public together with the annual financial report.

5. The management report shall be drawn up in accordance with Article 46 of Directive 78/660/EEC and, if the issuer is required to prepare consolidated accounts, in accordance with Article 36 of Directive 83/349/EEC.

6. The Commission shall, in accordance with the procedure referred to in Article 27(2), adopt implementing measures in order to take account of technical developments in financial markets and to ensure the uniform application of paragraph 1. The Commission shall in particular specify the technical conditions under which a published annual financial report, including the audit report, is to remain available to the public. Where appropriate, the Commission may also adapt the five-year period referred to in paragraph 1.

#### Article 5

##### Half-yearly financial reports

1. The issuer of shares or debt securities shall make public a half-yearly financial report covering the first six months of the financial year as soon as possible after the end of the relevant period, but at the latest two months thereafter. The issuer shall ensure that the half-yearly financial report remains available to the public for at least five years.

2. The half-yearly financial report shall comprise:

(a) the condensed set of financial statements;

(b) an interim management report; and

(c) statements made by the persons responsible within the issuer, whose names and functions shall be clearly indicated, to the effect that, to the best of their knowledge, the condensed set of financial statements which has been prepared in accordance with the applicable set of accounting standards gives a true and fair view of the assets, liabilities, financial position and profit or loss of the issuer, or the undertakings included in the consolidation as a whole as required under paragraph 3, and that the interim management report includes a fair review of the information required under paragraph 4.

3. Where the issuer is required to prepare consolidated accounts, the condensed set of financial statements shall be prepared in accordance with the international accounting standard applicable to the interim financial reporting adopted pursuant to the procedure provided for under Article 6 of Regulation (EC) No 1606/2002.

Where the issuer is not required to prepare consolidated accounts, the condensed set of financial statements shall at least contain a condensed balance sheet, a condensed profit and loss account and explanatory notes on these accounts. In preparing the condensed balance sheet and the condensed profit and loss account, the issuer shall follow the same principles for recognising and measuring as when preparing annual financial reports.

4. The interim management report shall include at least an indication of important events that have occurred during the first six months of the financial year, and their impact on the condensed set of financial statements, together with a description of the principal risks and uncertainties for the remaining six months of the financial year. For issuers of shares, the interim management report shall also include major related parties transactions.

5. If the half-yearly financial report has been audited, the audit report shall be reproduced in full. The same shall apply in the case of an auditors' review. If the half-yearly financial report

has not been audited or reviewed by auditors, the issuer shall make a statement to that effect in its report.

6. The Commission shall, in accordance with the procedure referred to in Article 27(2), adopt implementing measures in order to take account of technical developments on financial markets and to ensure the uniform application of paragraphs 1 to 5 of this Article.

The Commission shall, in particular:

- (a) specify the technical conditions under which a published half-yearly financial report, including the auditors' review, is to remain available to the public;
- (b) clarify the nature of the auditors' review;
- (c) specify the minimum content of the condensed balance sheet and profit and loss accounts and explanatory notes on these accounts, where they are not prepared in accordance with the international accounting standards adopted pursuant to the procedure provided for under Article 6 of Regulation (EC) No 1606/2002.

Where appropriate, the Commission may also adapt the five-year period referred to in paragraph 1.

#### Article 6

##### Interim management statements

1. Without prejudice to Article 6 of Directive 2003/6/EC, an issuer whose shares are admitted to trading on a regulated market shall make public a statement by its management during the first six-month period of the financial year and another statement by its management during the second six-month period of the financial year. Such statement shall be made in a period between ten weeks after the beginning and six weeks before the end of the relevant six-month period. It shall contain information covering the period between the beginning of the relevant six-month period and the date of publication of the statement. Such a statement shall provide:

- an explanation of material events and transactions that have taken place during the relevant period and their impact on the financial position of the issuer and its controlled undertakings, and
- a general description of the financial position and performance of the issuer and its controlled undertakings during the relevant period.

2. Issuers which, under either national legislation or the rules of the regulated market or of their own initiative, publish quarterly financial reports in accordance with such legislation or rules shall not be required to make public statements by the management provided for in paragraph 1.

3. The Commission shall provide a report to the European Parliament and the Council by 20 January 2010 on the transparency of quarterly financial reporting and statements by the management of issuers to examine whether the information provided meets the objective of allowing investors to make an informed assessment of the financial position of the issuer. Such a report shall include an impact assessment on areas where the Commission considers proposing amendments to this Article.

#### Article 14

1. Where an issuer of shares admitted to trading on a regulated market acquires or disposes of its own shares, either itself or through a person acting in his own name but on the issuer's behalf, the home Member State shall ensure that the issuer makes public the proportion of its own shares as soon as possible, but not later than four trading days following such acquisition or disposal where that proportion reaches, exceeds or falls below the thresholds of 5 % or 10 % of the voting rights. The proportion shall be calculated on the basis of the total number of shares to which voting rights are attached.

2. The Commission shall, in accordance with the procedure referred to in Article 27(2), adopt implementing measures in order to take account of technical developments in financial markets and to ensure the uniform application of paragraph 1.

#### Article 16

##### Additional information

1. The issuer of shares admitted to trading on a regulated market shall make public without delay any change in the rights attaching to the various classes of shares, including changes in the rights attaching to derivative securities issued by the issuer itself and giving access to the shares of that issuer.

2. The issuer of securities, other than shares admitted to trading on a regulated market, shall make public without delay any changes in the rights of holders of securities other than shares, including changes in the terms and conditions of these securities which could

indirectly affect those rights, resulting in particular from a change in loan terms or in interest rates.

3. The issuer of securities admitted to trading on a regulated market shall make public without delay of new loan issues and in particular of any guarantee or security in respect thereof. Without prejudice to Directive 2003/6/EC, this paragraph shall not apply to a public international body of which at least one Member State is member.

#### Article 17

Information requirements for issuers whose shares are admitted to trading on a regulated market

1. The issuer of shares admitted to trading on a regulated market shall ensure equal treatment for all holders of shares who are in the same position.

2. The issuer shall ensure that all the facilities and information necessary to enable holders of shares to exercise their rights are available in the home Member State and that the integrity of data is preserved. Shareholders shall not be prevented from exercising their rights by proxy, subject to the law of the country in which the issuer is incorporated. In particular, the issuer shall:

(a) provide information on the place, time and agenda of meetings, the total number of shares and voting rights and the rights of holders to participate in meetings;

(b) make available a proxy form, on paper or, where applicable, by electronic means, to each person entitled to vote at a shareholders' meeting, together with the notice concerning the meeting or, on request, after an announcement of the meeting;

(c) designate as its agent a financial institution through which shareholders may exercise their financial rights; and

(d) publish notices or distribute circulars concerning the allocation and payment of dividends and the issue of new shares, including information on any arrangements for allotment, subscription, cancellation or conversion.

3. For the purposes of conveying information to shareholders, the home Member State shall allow issuers the use of electronic means, provided such a decision is taken in a general meeting and meets at least the following conditions:

(a) the use of electronic means shall in no way depend upon the location of the seat or residence of the shareholder or, in the cases referred to in Article 10(a) to (h), of the natural persons or legal entities;

(b) identification arrangements shall be put in place so that the shareholders, or the natural persons or legal entities entitled to exercise or to direct the exercise of voting rights, are effectively informed;

(c) shareholders, or in the cases referred to in Article 10(a) to (e) the natural persons or legal entities entitled to acquire, dispose of or exercise voting rights, shall be contacted in writing to request their consent for the use of electronic means for conveying information and, if they do not object within a reasonable period of time, their consent shall be deemed to be given. They shall be able to request, at any time in the future, that information be conveyed in writing, and

(d) any apportionment of the costs entailed in the conveyance of such information by electronic means shall be determined by the issuer in compliance with the principle of equal treatment laid down in paragraph 1.

4. The Commission shall, in accordance with the procedure provided for in Article 27(2), adopt implementing measures in order to take account of technical developments in financial markets, to take account of developments in information and communication technology and to ensure the uniform application of paragraphs 1, 2 and 3. It shall, in particular, specify the types of financial institution through which a shareholder may exercise the financial rights provided for in paragraph 2(c).

#### Article 18

Information requirements for issuers whose debt securities are admitted to trading on a regulated market

1. The issuer of debt securities admitted to trading on a regulated market shall ensure that all holders of debt securities ranking *pari passu* are given equal treatment in respect of all the rights attaching to those debt securities.

2. The issuer shall ensure that all the facilities and information necessary to enable debt securities holders to exercise their rights are publicly available in the home Member State and that the integrity of data is preserved. Debt securities holders shall not be prevented

from exercising their rights by proxy, subject to the law of country in which the issuer is incorporated. In particular, the issuer shall:

(a) publish notices, or distribute circulars, concerning the place, time and agenda of meetings of debt securities holders, the payment of interest, the exercise of any conversion, exchange, subscription or cancellation rights, and repayment, as well as the right of those holders to participate therein;

(b) make available a proxy form on paper or, where applicable, by electronic means, to each person entitled to vote at a meeting of debt securities holders, together with the notice concerning the meeting or, on request, after an announcement of the meeting; and

(c) designate as its agent a financial institution through which debt securities holders may exercise their financial rights.

3. If only holders of debt securities whose denomination per unit amounts to at least EUR 50000 or, in the case of debt securities denominated in a currency other than Euro whose denomination per unit is, at the date of the issue, equivalent to at least EUR 50000, are to be invited to a meeting, the issuer may choose as venue any Member State, provided that all the facilities and information necessary to enable such holders to exercise their rights are made available in that Member State.

4. For the purposes of conveying information to debt securities holders, the home Member State, or the Member State chosen by the issuer pursuant to paragraph 3, shall allow issuers the use of electronic means, provided such a decision is taken in a general meeting and meets at least the following conditions:

(a) the use of electronic means shall in no way depend upon the location of the seat or residence of the debt security holder or of a proxy representing that holder;

(b) identification arrangements shall be put in place so that debt securities holders are effectively informed;

(c) debt securities holders shall be contacted in writing to request their consent for the use of electronic means for conveying information and if they do not object within a reasonable period of time, their consent shall be deemed to be given. They shall be able to request, at any time in the future, that information be conveyed in writing; and

(d) any apportionment of the costs entailed in the conveyance of information by electronic means shall be determined by the issuer in compliance with the principle of equal treatment laid down in paragraph 1.

5. The Commission shall, in accordance with the procedure provided for in Article 27(2), adopt implementing measures in order to take account of technical developments in financial markets, to take account of developments in information and communication technology and to ensure the uniform application of paragraphs 1 to 4. It shall, in particular, specify the types of financial institution through which a debt security holder may exercise the financial rights provided for in paragraph 2(c).

#### Article 19

##### Home Member State control

1. Whenever the issuer, or any person having requested, without the issuer's consent, the admission of its securities to trading on a regulated market, discloses regulated information, it shall at the same time file that information with the competent authority of its home Member State. That competent authority may decide to publish such filed information on its Internet site.

Where an issuer proposes to amend its instrument of incorporation or statutes, it shall communicate the draft amendment to the competent authority of the home Member State and to the regulated market to which its securities have been admitted to trading. Such communication shall be effected without delay, but at the latest on the date of calling the general meeting which is to vote on, or be informed of, the amendment.

2. The home Member State may exempt an issuer from the requirement under paragraph 1 in respect of information disclosed in accordance with Article 6 of Directive 2003/6/EC or Article 12(6) of this Directive.

3. Information to be notified to the issuer in accordance with Articles 9, 10, 12 and 13 shall at the same time be filed with the competent authority of the home Member State.

4. In order to ensure the uniform application of paragraphs 1, 2 and 3, the Commission shall, in accordance with the procedure referred to in Article 27(2), adopt implementing measures. The Commission shall, in particular, specify the procedure in accordance with which an issuer, a holder of shares or other financial instruments, or a person or entity referred to in

Article 10, is to file information with the competent authority of the home Member State under paragraphs 1 or 3, respectively, in order to:

- (a) enable filing by electronic means in the home Member State;
- (b) coordinate the filing of the annual financial report referred to in Article 4 of this Directive with the filing of the annual information referred to in Article 10 of Directive 2003/71/EC.

Article 30

Transitional provisions

1. By way of derogation from Article 5(3) of this Directive, the home Member State may exempt from disclosing financial statements in accordance with Regulation (EC) No 1606/2002 issuers referred to in Article 9 of that Regulation for the financial year starting on or after 1 January 2006.

2. Notwithstanding Article 12(2), a shareholder shall notify the issuer at the latest two months after the date in Article 31(1) of the proportion of voting rights and capital it holds, in accordance with Articles 9, 10 and 13, with issuers at that date, unless it has already made a notification containing equivalent information before that date.

Notwithstanding Article 12(6), an issuer shall in turn disclose the information received in those notifications no later than three months after the date in Article 31(1).

3. Where an issuer is incorporated in a third country, the home Member State may exempt such issuer only in respect of those debt securities which have already been admitted to trading on a regulated market in the Community prior to 1 January 2005 from drawing up its financial statements in accordance with Article 4(3) and its management report in accordance with Article 4(5) as long as

(a) the competent authority of the home Member State acknowledges that annual financial statements prepared by issuers from such a third country give a true and fair view of the issuer's assets and liabilities, financial position and results;

(b) the third country where the issuer is incorporated has not made mandatory the application of international accounting standards referred to in Article 2 of Regulation (EC) No 1606/2002; and

(c) the Commission has not taken any decision in accordance with Article 23(4)(ii) as to whether there is an equivalence between the abovementioned accounting standards and

- the accounting standards laid down in the law, regulations or administrative provisions of the third country where the issuer is incorporated, or
- the accounting standards of a third country such an issuer has elected to comply with.

4. The home Member State may exempt issuers only in respect of those debt securities which have already been admitted to trading on a regulated market in the Community prior to 1 January 2005 from disclosing half-yearly financial report in accordance with Article 5 for 10 years following 1 January 2005, provided that the home Member State had decided to allow such issuers to benefit from the provisions of Article 27 of Directive 2001/34/EC at the point of admission of those debt securities.