HM Revenue & Customs

http://www.hmrc.gov.uk

Notice MLR8

Preventing money laundering and terrorist financing

August 2008

This notice cancels and replaces Notice MLR7 (January 2004) and Notice MSB2 (October 2004). Details of any changes to the previous version can be found in paragraph 1.1 of this notice.

Further help and advice

If you need general advice or more copies of HM Revenue & Customs notices, please ring our advice service on **0845 010 9000**. **You can call between 8:00 am and 8:00 pm, Monday to Friday**.

If you have **hearing difficulties**, please ring the **Textphone** service on **0845 000 0200**.

If you would like to speak to someone in **Welsh,** please ring
0845 010 0300, between 8:00 am and 6:00 pm, Monday to Friday.

Other notices on this or related subjects:

Notice MLR9 *Money Laundering Regulations 2007: Registration*

Contents

Notice MLR8 ..... **1**

1. Introduction **5**

1.1 Who is this guidance for? 5
1.2 Purpose of this guidance 5
1.3 Status of the guidance 6
1.4 Contents of this guidance 6

2. Background and legislation **7**

2.1 What is money laundering? 7
2.2 Legislation on money laundering and terrorist financing 7

3. Money Laundering Regulations 2007: General obligations **9**

3.1 Policies and procedures 9
3.2 Sanctions for non-compliance 9

4. Senior management responsibility **10**

4.1 Adoption of policy in relation to financial crime prevention 10
4.2 What should a policy statement include? 10
4.3 Liability for offences by bodies corporate 10
4.4 Application of AML/CTF policies outside the European Economic Area (EEA) 10

5. Internal Control **12**

5.1 Internal Controls and communication 12
5.2 Compliance management 13

6. A risk-based approach **14**

6.1 What is a risk-based approach? 14
6.2 Risk-assessment 14
6.3 Risk monitoring 15
6.4 Managing and mitigating the risk 15
6.5 Monitoring and improving the effectiveness of controls 16
6.6 Recording what has been done and why 16

7. Customer due diligence (CDD) **17**

7.1 Introduction 17
7.2 Why is it necessary to apply CDD measures? 17
7.3 What is customer due diligence? 17
7.4 When must these due diligence measures be applied? 17
7.5 Determining the extent of customer due diligence measures 17
7.6 Timing of verification of identity 18
7.7 Non-compliance with customer due diligence measures 18
7.8 Identifying the beneficial owner 18
7.9 Obtaining information on the purpose and intended nature of a business relationship 20
7.10 Occasional transactions 20
7.11 Simplified due diligence (SDD) 21
7.12 Enhanced due diligence (EDD) 21
7.13 Reliance on third parties to apply customer due diligence measures 23
7.14 Persons that businesses must not accept as customers 24

8. Identity and verification **26**

8.1 Introduction 26
8.2 Nature and extent of evidence 26
8.3 Documentary evidence 26
8.4 Electronic evidence 27
8.5 Nature of electronic checks 27
8.6 Criteria for use of an electronic provider 27

9. Ongoing monitoring of customers in a business relationship **28**

9.1 The requirement to monitor customers' activities 28
9.2 What is monitoring? 28
9.3 Manual or automated? 28

9.4 Staff awareness....29
9.5 Customer information....29

10. Suspicious Activity reporting to the Serious Organised Crime Agency (SOCA)....30

10.1 General legal and regulatory obligations....30
10.2 The meaning of knowledge, suspicion and reasonable grounds for knowledge or suspicion....30
10.3 Making disclosures to the Serious Organised Crime Agency (SOCA)....30
10.4 Internal reporting procedures....30
10.5 SARs completed by agents....31
10.6 Consent under PoCA....31
10.7 Tipping-off....31
10.8 Suspicion indicators....32

11. Staff awareness and training....33

11.1 General legal obligations....33
11.2 Who should be trained?....33
11.3 What should training cover?....33
11.4 How often should training be given?....33

12. Record-keeping....34

12.1 General legal requirements....34
12.2 The records that must be kept....34
12.3 Persons who are relied on by another person to apply any customer due diligence measures....34
12.4 Businesses which rely on another person to apply customer due diligence measures....34
12.5 How long must the customer keep due diligence records?....34
12.6 In what format must the records be kept?....35
12.7 Penalties for failure to keep records....35

13. APPENDIX 1: Criminal offences and penalties for money laundering and terrorist financing....36

13.1 The Proceeds of Crime Act 2002 (PoCA) Part 7....36
13.2 The Terrorism Act 2000 Part 3....36

14. APPENDIX 2: Sanctions for failure to comply with the Money Laundering Regulations 2007....38

14.1 Civil penalties....38
14.2 Criminal offences....38

15. APPENDIX 3: template for policy statement and risk assessment....39

15.1 Policy statement....39
15.2 Risk assessment....39
15.3 Customer profile....39
15.4 Risk identification....40
15.5 Risk factors and response....40
15.6 Customer due diligence: policy on acceptable ID and satisfactory verification....42
15.7 Customer due diligence: business relationships....42
15.8 Ongoing monitoring of business relationships....43
15.9 Monitoring the risk....43
15.10 Internal controls and communication....43
15.11 Monitoring and managing compliance....44
15.12 Suspicious Activity Reporting....44
15.13 Record-keeping....44
15.14 Training....44

16. APPENDIX 4: Summary of customer due diligence and ongoing monitoring....45

17. APPENDIX 5: Acceptable evidence of identity....47

17.1 Private individuals....47
17.2 Customers other than private individuals (such as companies, trusts or charities)....51

18. APPENDIX 6: Supplementary guidance for High Value Dealers....53

18.1 Overview of the sector....53
18.2 What are the money laundering risks faced by HVDs?....53
18.3 Managing the risk....53
18.4 Suspicion indicators....54

19. APPENDIX 7 55

19.1 Introduction and sector overview 55
19.2 What are the money laundering risks faced by Bureaux De Change? 55
19.3 Managing the risk 56
19.4 Identification issues 56
19.5 Linked transactions 57
19.6 HM Treasury Consolidated List of Financial Sanctions Targets 57
19.7 Training 57
19.8 Suspicion indicators 57

20. APPENDIX 8: Supplementary guidance for Money Transmission Businesses 58

20.1 Overview of the sector 58
20.2 What does the risk-based approach mean for money transmission businesses? 58
20.3 How should the risk-based approach be implemented? 58
20.4 What are the money laundering risks in the industry? 59
20.5 EC Regulation 1781/2006 on information on the payer accompanying transfers of funds (commonly known as the Payments Regulation or the Wire Transfer Regulation) 60
20.6 Verification of identity 62
20.7 Nature and purpose of the business relationship 63
20.8 Ongoing monitoring of business relationships 64
20.9 Customers who are Money Transmission Businesses 64
20.10 Use of agents 64
20.11 Enhanced Due Diligence 64
20.12 Suspicious activity reporting 65
20.13 HM Treasury consolidated sanctions list 65
20.14 Typologies 65
20.15 Training 65

APPENDIX 9: Supplementary guidance for cheque encashment businesses (CEBs) 66

20.16 Overview of the sector 66
20.17 What are the money laundering risks faced by Cheque Encashment Businesses? 66
20.18 Managing the risks 67
20.19 Identification issues 67
20.20 Linked transactions 68
20.21 Training 68
20.22 Suspicion indicators 68

21. APPENDIX 10: Supplementary guidance for trust or company service providers 70

21.1 Overview of the sector 70
21.2 What are the money laundering risks faced by businesses in the TCSP sectors? 70
21.3 Factors that may increase the risk of money laundering 70

Client-related 70

Service/transaction-related 71

Geographic areas of operation of the business or clients 71

21.4 The Risk-Based Approach 71
21.5 Customer Due Diligence 71
21.6 Ongoing monitoring of business relationships 74
21.7 Enhanced due diligence and ongoing monitoring 74
21.8 Suspicion indicators 74

22. Glossary of terms 76

1. Introduction

1.1 Who is this guidance for?

This guidance is addressed to proprietors, directors, managers, employees and Nominated Officers of the following businesses that are the subject of the Money Laundering Regulations 2007 (MLR 2007) and for whom HM Revenue & Customs (HMRC) is the supervisory authority:

- Money Service Businesses (MSBs)
- High Value Dealers (HVDs)
- Trust or Company Service Providers (TCSPs).

For further information on the businesses that fall into the categories above the relevant supervisory authorities and the registration requirements and processes, please go to Notice MLR9 *Registration.*

All auditors, insolvency practitioners, external accountants and tax advisers, including those that are supervised by HMRC, should follow the guidance published by the Consultative Committee of Accountancy Bodies (CCAB).

Trust or company service providers that are supervised by HMRC should follow this guidance but may also find the CCAB guidance useful.

Businesses that provide both accountancy services and trust or company services and are supervised by HMRC should follow the CCAB guidance but also have regard for the guidance for Trust or Company Service Providers in Appendix 10 of this guidance when carrying out those services.

This guidance revises and updates the guidance previously set out in Notice MSB2 *Anti money laundering guide* and Notice MLR7 *Anti money laundering guide for High Value Dealers*, to reflect the changes to the prevention of money laundering and combating terrorist financing measures brought about by the Money Laundering Regulations 2007, which came into force on 15 December 2007. These changes include the introduction of a risk-based approach to preventing money laundering and terrorist financing and new customer due diligence measures.

This guidance is based on, and, where appropriate, replicates the guidance produced by the Joint Money Laundering Steering Group (JMLSG) for businesses that are supervised by the Financial Services Authority (FSA).

1.2 Purpose of this guidance

The purpose of this guidance is to provide relevant businesses that are supervised by HMRC with comprehensive guidance on implementing the legal requirements for measures designed to deter, detect and disrupt money laundering and terrorist financing. It also includes industry sector specific guidance for:

- High Value Dealers
- Bureaux De Change
- Money Transmission Businesses
- Cheque Encashment Businesses, and
- Trust or Company Service Providers.

The guidance:

- Outlines the legislation on anti-money laundering (AML) and combating terrorist financing (CTF) measures
- Explains the requirements of the Money Laundering Regulations 2007 and how these should be applied in practice
- Assists businesses in designing and putting in place the systems and controls necessary to lower the risk of their business being used by criminals to launder money or finance terrorism
- Provides industry specific good practice guidance on AML/CTF procedures.

1.3 Status of the guidance

This guidance is 'relevant guidance' which is approved by the Treasury, for the purposes of **MLR 2007 Regulations 42(3) and 45(2), and Regulation 14(3) of the Transfer of Funds (Information on the Payer) Regulations 2007.** The extent to which a business can demonstrate that this guidance has been followed will be taken into account by HMRC and a court when they decide whether or not there has been a failure to comply with the MLR 2007 or the EC Wire Transfer/Payments Regulation.

It is also 'relevant guidance' for the purposes of the **Proceeds of Crime Act 2002 Sections 330 (8) and 331(7)**, which require courts to consider whether this guidance has been followed in deciding if a person in the regulated sector has committed an offence of failure to disclose.

Similarly, the **Terrorism Act 2000 Section 21A** requires a court to take account of such approved guidance when considering whether a person within the financial sector has failed to report under that Act.

Where the term 'must' is used in this guidance it indicates a legal or regulatory requirement. The term 'should' is used to indicate the recommended way to meet the regulatory requirements. Businesses may decide to act in a different way than recommended if they wish but may be called upon to demonstrate that they have met the same standards.

1.4 Contents of this guidance

The guidance includes:

- A definition of money laundering and terrorist financing
- The main pieces of UK legislation concerning AML/CTF
- The main legal obligations on relevant businesses under MLR 2007
- The role of senior management in taking responsibility for effectively managing the money laundering and terrorist financing risks faced by the business
- Information on the risk-based approach to the prevention of money laundering and terrorist financing
- The customer due diligence measures
- The evidence of identity requirements
- Methods for ongoing monitoring of business relationships
- Procedures for reporting suspicious activity
- Staff awareness and training requirements
- Record keeping requirements
- Details of criminal offences and penalties relating to money laundering and terrorist financing
- The sanctions for failure to comply with the Money Laundering Regulations 2007
- Business sector specific material, which has been prepared principally by practitioners in the relevant sectors.

2. Background and legislation

2.1 What is money laundering?

Money laundering is the process by which criminally obtained money or other assets (criminal property) are exchanged for 'clean' money or other assets with no obvious link to their criminal origins.

Criminal property may take any form, including money or money's worth, securities, tangible property and intangible property. It also covers money, however come by, which is used to fund terrorism.

Money laundering activity includes:

- Acquiring, using or possessing criminal property
- Handling the proceeds of crimes such as theft, fraud and tax evasion
- Being knowingly involved in any way with criminal or terrorist property
- Entering into arrangements to facilitate laundering criminal or terrorist property
- Investing the proceeds of crimes in other financial products
- Investing the proceeds of crimes through the acquisition of property/assets
- Transferring criminal property.

Terrorism is 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.

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.

There are no 'de minimis' exceptions in relation to either money laundering or terrorist financing offences.

The UK legislation on money laundering applies to the proceeds of conduct that is an offence in the UK and most conduct occurring elsewhere that would have been an offence if it had taken place in the UK.

2.2 Legislation on money laundering and terrorist financing

The main pieces of UK legislation concerning the prevention of money laundering and combating terrorist financing are summarised in this section. The criminal offences and penalties for money laundering and terrorist financing are listed in Appendix 1.

2.2.1 The Proceeds of Crime Act 2002 (PoCA) as amended by the Serious Organised Crime and Police Act 2005

PoCA:

- Establishes a series of criminal offences in connection with money laundering, failing to report knowledge or suspicions or reasonable grounds for knowledge or suspicions, tipping off a person to the fact that a report has been made, and prejudicing an investigation
- Sets out penalties for the various offences established under PoCA
- Establishes the Assets Recovery Agency (which will shortly merge with the Serious Organised Crime Agency (SOCA)), with power to investigate whether a person holds criminal assets, and if so, their location
- Creates five investigative powers for law enforcement.

2.2.2 The Terrorism Act 2000 (TA2000) as amended by the Anti-Terrorism, Crime and Security Act 2001

This Act:

- Establishes offences relating to involvement in facilitating, raising, possessing or using funds for terrorist purposes and for failing to report suspicions, tipping off and prejudicing an investigation
- Empowers authorities to make Orders on financial institutions in connection with terrorist investigations
- Establishes a list of proscribed organisations with which financial services firms may not deal.

2.2.3 The Money Laundering Regulations 2007 (MLR 2007)

These Regulations:

- Require firms to take measures to identity their customers
- Specify the policies and procedures that financial institutions and other relevant businesses must put in place in order to prevent and identify activities relating to money laundering and terrorist financing
- Require businesses in the regulated sector to appoint a Nominated Officer to receive internal reports from staff with knowledge or suspicion of money laundering or terrorist financing
- Set out the supervision and registration arrangements. Further information on the role of HMRC as a supervisory authority is available in MLR9 *Registration*.

2.2.4 Regulation EC 1781/2006 on information on the payer accompanying transfers of funds (commonly known as the Payments Regulation or the Wire Transfer Regulation)

The Regulation:

- Is directly applicable in the UK. Supervisory and enforcement provisions and the creation of civil and criminal penalties are contained in the Transfer of Funds (Information on the Payer) Regulations 2007
- Applies to Payment Service Providers (PSPs), principally banks (supervised by the FSA), and money service businesses (supervised by HMRC)
- Aims to ensure that basic information on the originator of wire transfers is immediately available to law enforcement agencies to assist them in detecting and tracing the assets of terrorists or other criminals
- Applies to transfers of funds which are sent or received by a Payment Service Provider in the European Community
- Requires that transfers of funds are accompanied by information on the payer.

2.2.5 HM Treasury consolidated list of persons designated as being subject to financial restrictions

This includes targets listed by the United Nations, European Union and United Kingdom under legislation relating to current financial restrictions regimes. The purpose of the HM Treasury list is to draw together in one place all the names of designated persons from the various financial restrictions regimes effective in the UK. Criminal penalties apply to breaches of the restrictions. Section 7.14 contains further guidance on financial restrictions.

3. Money Laundering Regulations 2007: General obligations

3.1 Policies and procedures

MLR 2007 Regulation 20 sets out the requirement for relevant businesses to establish and maintain appropriate and risk-sensitive policies and procedures relating to:

- Customer due diligence and ongoing monitoring
- Reporting
- Record keeping
- Internal Control
- Risk assessment and management
- The monitoring and management of compliance, and
- The internal communication of such policies and procedures,

in order to prevent activities related to money laundering and terrorist financing.

These policies and procedures must include policies and procedures that:

- Identify and scrutinise:
  - complex or unusually large transactions
  - unusual patterns of transactions which have no apparent economic or visible lawful purpose
  - any other activity which could be considered to be related to money laundering or terrorist financing
- Specify the additional measures that will be taken to prevent the use of products and transactions that favour anonymity for money laundering or terrorist financing
- Determine whether a customer is a politically exposed person (see section 7.12.3 for definition and further guidance)
- Nominate an individual in the organisation to receive disclosures under Part 7 of PoCA and Part 3 of TA2000
- Ensure employees report suspicious activity to the Nominated Officer, and
- Ensure the Nominated Officer considers such internal reports in the light of available information and determines whether they give rise to knowledge or suspicion or reasonable grounds for knowledge or suspicion of money laundering or terrorist financing.

Financial institutions (which include Bureaux De Change, money transmitters and cheque cashers) must, additionally:

- Establish and maintain systems which enable a full and rapid response to enquiries from law enforcement agencies, and
- Communicate the policies and procedures to branches and subsidiary undertakings which are located outside the UK.

3.2 Sanctions for non-compliance

The civil and criminal sanctions for failure to comply with the MLR 2007 are explained in Appendix 2.

4. Senior management responsibility

4.1 Adoption of policy in relation to financial crime prevention

Senior managers are responsible for ensuring that the business's policies and procedures are designed and operate effectively to manage the risk of the business being used for financial crime and to fully meet the requirements of the MLR 2007.

Senior manager means a director, manager, secretary, chief executive, member of the committee of management, or a person purporting to act in that capacity, any partner in a partnership, or a sole proprietor.

A statement of the business's AML/CTF policy and the procedures to implement it will clarify how the business's senior management intends to discharge its responsibility for the prevention of money laundering and terrorist financing. This will provide a framework of direction to the business and its staff and will identify named individuals and functions responsible for implementing particular aspects of the policy.

The policy statement will set out how senior management undertakes its assessment of the risks the firm faces and how these risks are to be managed. Even in a small business, a summary of its high-level AML/CTF policy will focus the minds of staff on the need to be constantly aware of the risks and how they are to be managed.

4.2 What should a policy statement include?

The policy statement could include:

Guiding principles – including:

- The culture and values to be adopted and promoted within the business towards the prevention of money laundering and terrorist financing
- A commitment to ensuring all relevant staff are trained and made aware of the law and their obligations under it, and to establishing procedures to implement these requirements in line with **MLR 2007 Regulations 20 and 21**
- Recognition of the importance of staff promptly reporting their suspicions internally.

Risk mitigation approach:

- A summary of the firms approach to assessing and managing its money laundering and terrorist financing risks
- Allocation of responsibilities to specific persons and functions
- A summary of the firms procedures for carrying out appropriate identification, verification, customer due diligence, and monitoring checks on the basis of their risk-based approach
- A summary of the appropriate monitoring arrangements in place to ensure that the firm's policies and procedures are being carried out.

4.3 Liability for offences by bodies corporate

Under MLR 2007 Regulation 47, an officer in a body corporate (i.e. a director, manager, secretary, chief executive, member of the committee of management, or a person purporting to act in that capacity), or any partner in a partnership of any business covered by the MLR 2007, who consents to or is involved in committing offences under the Regulations, or where any such offence is due to any neglect on his part, will be individually liable to prosecution for the offence as well as the body corporate**.** Partners of partnerships and officers of unincorporated associations covered by the MLR 2007 are in a similar position. **Failure of senior managers to comply with the MLR 2007 obligations may result in financial penalties or a prison term of up to two years and/or an unlimited fine.** However, provided the assessment of the risks and the selection of mitigating procedures have been approached in a considered way, all the relevant decisions are properly recorded and the firm's procedures are followed, the risk of contravention should be small.

4.4 Application of AML/CTF policies outside the European Economic Area (EEA)

Under MLR 2007 Regulation 15, credit or financial institutions must require their branches and subsidiary undertakings (which has its Companies Act 2006 meaning) which are situated in a non-EEA state to apply AML and CTF measures and keep records at least to the standards required by the MLR 2007. Higher standards should be applied if required by the host country.

Regulation 20(5) requires that credit or financial institutions communicate where relevant the policies and procedures it establishes and maintains to branches and subsidiaries outside the UK.

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

5. Internal Control

5.1 Internal Controls and communication

5.1.1 Why are internal controls and communication necessary?

MLR 2007 Regulation 20 requires businesses to have appropriate systems of internal control and communication in order to prevent activities related to money laundering and terrorist financing.
In simple terms this means that businesses must ensure that management controls are put in place that will alert the relevant people in the business to the possibility that criminals may be attempting to use the business to launder money or fund terrorism, so as to enable them to take appropriate action to prevent or report it.

Systems of internal control and communication must be capable of identifying unusual or suspicious transactions or customer activity, and quickly reporting the details to the Nominated Officer/Money Laundering Reporting Officer (see section 10), or to the owner of the business, who is responsible for making a disclosure to SOCA under the terms of the PoCA 2002 or the TA 2000.

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

- The degree of risk associated with each area of its operation
- The nature, scale and complexity of the business
- The type of products, customers, and activities involved
- The diversity of operations, including geographical diversity
- Distribution channels
- The volume and size of transactions.

5.1.2 What controls are necessary?

Systems of internal control should include:

- Identification of senior management responsibilities
- Provision of regular and timely information to senior management on money laundering and terrorist financing risks
- Training of relevant employees on the legal and regulatory responsibilities for money laundering and terrorist financing controls and measures
- Documentation of the business's AML/CTF risk management policies and procedures
- Measures to ensure that money laundering and terrorist financing risks are taken into account in the day-to-day operation of the business.

5.1.3 Use of agents

Where relevant businesses offer their products and services through agents that they have listed within their entry on the MLR register, the principal business is responsible for their agents' compliance with the MLR 2007 and liable to sanctions arising from their non-compliance. The risks of money laundering or terrorist financing through these premises must be actively managed in line with the risk-based approach. This includes:

- Producing risk assessments and profiles
- Ensuring that agents have satisfactory AML/CTF systems and procedures in place
- Monitoring compliance with these procedures and
- Reviewing and updating risks and controls so that policies and procedures continue to effectively manage the risks.

Agents are not the subject of a 'fit and proper test' under **MLR 2007 Regulation 28** unless they are required to be registered in their own right. However, it is in the interests of registered businesses to ensure that their agents meet the same standards so that, under the risk-based approach, they can reasonably be relied on to comply with the MLR 2007 when undertaking business for the registered business, subject to appropriate, risk-based levels of risk and compliance management.

It is recommended that businesses:

- Require responsible people (proprietors, partners, directors, major shareholders (above 25%) and, if appropriate, Nominated Officers of their agents) to make a declaration that they satisfy the Fit and Proper criteria laid down in Regulation 28 of MLR 2007. (This can be done by adapting the downloadable HMRC Fit and Proper application form from our website **www.hmrc.gov.uk**)
- Conduct commercial investigations, e.g. on credit worthiness, on all agents
- Conduct a programme of site visits to agents
- Undertake transaction monitoring and testing to confirm the business's AML/CTF policies and procedures are being complied with by agents
- Keep records of these declarations and checks to support risk management and internal control policies and procedures.

5.2 Compliance management

Businesses must carry out regular assessments of the adequacy of their systems and controls to ensure that they manage the money laundering and terrorist financing risks effectively and are compliant with the MLR 2007. Businesses must therefore ensure that appropriate monitoring processes and procedures are established and maintained to regularly review and test the effectiveness of their policies and procedures.

Businesses must test the effectiveness of the checks they make and also the areas and indicators of risk that they have identified. A review should include consideration of the following areas:

- Are there any areas of weakness in the business where appropriate risk-sensitive checks may not be being carried out in accordance with the MLR 2007 requirements and the business's policies and procedures?
- Are correct records kept in respect of evidence of ID taken and other customer due diligence and ongoing monitoring measures?
- Are there any new products, services or procedures that require risk assessment, appropriate due diligence checks and internal controls putting in place?

Further information on the monitoring and review of risk policy, programmes and procedures can be found in section 6 of this guidance.

6. A risk-based approach

6.1 What is a risk-based approach?

MLR 2007 Regulations 20(1), 7(3) and 8(3) require firms to adopt a risk-based approach to the application of measures to prevent money laundering and terrorist financing.

A risk-based approach requires a number of steps to be taken 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 steps are to:

- Identify the money laundering and terrorist financing risks that are relevant to the business
- Assess the risks presented by the particular

  - Customers – types and behaviour

  - Products and services

  - Delivery channels, e.g. cash over the counter, electronic, wire transfer, cheque

  - Geographical areas of operation, e.g. location of business premises, source or destination of customers' funds
- Design and implement controls to manage and mitigate these assessed risks
- Monitor and improve the effective operation of these controls, and
- Record appropriately what has been done, and why.

A risk-based approach should balance the costs to the business and its customers with a realistic assessment of the risk of the business being used for money laundering or terrorist financing. It focuses effort where it is needed and will have most impact.

Businesses can decide for themselves how to carry out their risk-assessment, which may be simple or sophisticated in accordance with the business they operate. Where the business is simple, involving few products, with most customers falling into similar categories, a simple approach may be appropriate for most customers, with the focus being on those customers that fall outside the norm.

Businesses with predominantly retail customers will be able to put standard AML/CTF procedures in place. In more complex business relationships, risk-assessment, mitigation and ongoing monitoring will be more involved.

A risk-assessment will often result in a stylised categorisation of risk, e.g. high, medium and low. Criteria will be attached to each category to assist in allocating customers and products to risk categories, in order to determine the level of identification, verification, additional customer information and ongoing monitoring, in a way that minimises complexity.

6.2 Risk-assessment

A risk-based approach starts with the identification and assessment of the risk that has to be managed. The supplementary guidance in Appendices 6 to 10 includes further information on the risks that may be present within the different business sectors and appropriate controls and counter measures that can be applied to deter, detect and disrupt money laundering and terrorist financing in those circumstances. Appendix 3 provides a template for a policy statement and risk-assessment that some businesses may find useful.

The business should consider the following questions:

What risk is posed by the customers?

For example by:

- Brand new customers carrying out large one-off transactions
- Customers that are not local to the business
- Customers engaged in a business which involves significant amounts of cash
- Complex business ownership structures with the potential to conceal underlying beneficiaries
- A customer or group of customers making frequent transactions to the same individual/group of individuals
- An individual (or an immediate relative of his) holding a public position and/or situated in a location which carries a risk of exposure to the possibility of corruption

- Customers based in, or conducting business in or through, a high risk jurisdiction, or a jurisdiction with known higher levels of corruption, organised crime or drug production/distribution. For information on high-risk countries go to the Financial Action Task Force website **www.fatf-gafi.org**
- Transactions that do not make commercial sense.

Is a risk posed by a customer's behaviour?

For example:

- An unwillingness to produce evidence of ID or the production of unsatisfactory evidence of ID
- Where the customer is, or appears to be, acting on behalf of another person, an unwillingness to give the name(s) of the person(s) they represent
- A willingness to bear very high or un-commercial penalties or charges
- Situations where the source of funds cannot be easily verified.

How does the way the customer comes to the business affect the risk?

- Occasional or one-off transactions as opposed to business relationships
- Introduced business, depending on the effectiveness of the due diligence carried out by the introducer
- Non face-to-face transactions.

What risk is posed by the products/services the customer is using?

For example:

- Do the products allow/facilitate payments to third parties?
- Is there a risk of inappropriate assets being placed with, or moving through the business?

N.B. These lists are not exhaustive. Your risk assessment should include any other risks that apply in your business.

6.3 Risk monitoring

Risk assessment must also include the review and monitoring of the money laundering and terrorist financing risks to the business. The risk-based approach by the business will be informed by the monitoring of patterns of business, for example:

- A sudden increase in business from an existing customer
- Uncharacteristic transactions which are not in keeping with the customer's known activities
- Peaks of activity at particular locations or at particular times
- Unfamiliar or untypical types of customer or transaction.

6.4 Managing and mitigating the risk

Once the business has identified and assessed the risks it faces of being used for money laundering or terrorist financing, it must ensure that appropriate controls are put in place to lessen these risks and prevent the business from being used for money laundering or terrorist financing.

Managing and mitigating the risks will involve:

- Applying customer due diligence measures to verify the identity of customers and any beneficial owners
- Obtaining additional information on higher-risk customers
- Conducting ongoing monitoring of the transactions and activity of customers with whom there is a business relationship, and
- Having systems to identify and scrutinise unusual transactions and activity to determine whether there are reasonable grounds for knowing or suspecting that money laundering or terrorist financing may be taking place.

These requirements are explained in more detail in further sections of this guidance.

MLR 2007 Regulations 7(3) and 8(3) state that businesses must determine the extent of their customer due diligence measures and ongoing monitoring procedures on a risk-sensitive basis, depending on the type of customer, business relationship, product or transaction.

Examples of risk-based control procedures may include:

- Introducing customer identification and verification procedures at a lower monetary level than the minimum set out for occasional transactions in the Money Laundering Regulations (15,000 euro), in circumstances where the customer or other characteristics of the transaction are in a higher risk category
- Requiring ID evidence – whether it be documentary, electronic or third party assurance – to be of a certain standard
- Requiring additional evidence of identity in higher risk situations
- More extensive due diligence checks, e.g. on source of funds, for higher risk customers
- Varying the level of monitoring of customer transactions and activities according to identified risk to identify transactions or activities that may be unusual or suspicious.

This list of suggested controls is not exhaustive. Business managers must decide what checks and controls are appropriate to address the risks that they have identified within their business activities.

Identifying a customer or transaction as being of a higher risk does not automatically mean that the customer/transaction is involved with money laundering or terrorist financing. Similarly, a customer/transaction seen as low risk does not mean that the customer/transaction is not involved with money laundering or terrorist financing. Employees of the business therefore need to be vigilant, and use their experience and common sense when applying the business's risk based criteria and rules.

6.5 Monitoring and improving the effectiveness of controls

The business should have some means of assessing whether its risk mitigation procedures and controls are working effectively, and if not, where they need to be improved. Its policies and procedures will therefore need to be kept under regular review.

Aspects of the risk-based approach that should be considered for monitoring and review include:

- Procedures to identify changes in customer characteristics or behaviour
- The ways in which products and services may be used for money laundering or terrorist financing, recognising how these ways can change, with reference to information and typologies supplied by law enforcement feedback
- The adequacy of staff training and awareness
- Compliance monitoring arrangements, e.g. internal audit/quality assurance processes or external reviews
- The balance between technology-based and people-based systems
- Capturing appropriate management information
- Upward reporting and accountability
- Internal communication
- Effectiveness of the liaison with regulatory and law enforcement agencies.

6.6 Recording what has been done and why

Businesses should keep relevant documents relating to the risk-assessment and management procedures and processes discussed in this section. That will enable businesses to be able to demonstrate to HMRC that the extent of customer due diligence measures and ongoing monitoring procedures are appropriate in view of the risks of money laundering and terrorist financing, as required by **MLR 2007 Regulation 7(3)(b) and 8(3).** The records that must be kept in respect of customer due diligence measures and ongoing monitoring of business relationships are set out in section 12.

7. Customer due diligence (CDD)

7.1 Introduction

This section sets out and explains the legal definitions and requirements for customer due diligence under MLR 2007. A summary of these customer due diligence requirements is also provided in Appendix 4. Section 8 explains the principles and criteria to be applied to obtaining and verifying evidence of customers' identity. Details of the specific documents and other evidence of identity that are acceptable are set out in Appendix 5.

7.2 Why is it necessary to apply CDD measures?

The customer due diligence obligations on relevant businesses under the MLR 2007 are designed to make it more difficult for businesses in the regulated sector to be used by criminals for money laundering or terrorist financing.

Businesses also need to guard against fraud, including impersonation fraud, and the risks of committing offences under the Proceeds of Crime Act and the Terrorism Act relating to money laundering or terrorist financing.

Where there is a business relationship, customer due diligence measures must involve more than just determining the customer's identity. It will also be necessary to ascertain the intended nature and purpose of the business relationship and to collect information on the customer, his business and risk profile to allow ongoing monitoring of the business relationship to ensure that transactions undertaken are consistent with that knowledge.

7.3 What is customer due diligence?

The meaning and application of customer due diligence are set out in **MLR 2007 Regulations 5 and 7**.

These regulations require businesses to:

- Identify their customers and verify their identity
- Identify, where applicable, the 'beneficial owner' involved in the business or transaction (where someone is acting on behalf of another person, or to establish the ownership of corporate bodies or other entities – see section 7.8 for further guidance) and take risk-based and adequate measures to verify their identity
- For business relationships, obtain information on the purpose and intended nature of the business relationship (e.g. on the source of funds and purpose of transactions – see section 7.9 for further guidance).

7.4 When must these due diligence measures be applied?

Customer due diligence measures must be applied:

- When establishing a business relationship (see section 7.9)
- When carrying out an occasional transaction (i.e. involving 15,000 euro (or the equivalent in sterling) or more - see section 7.10)
- Where there is a suspicion of money laundering or terrorist financing
- Where there are doubts about previously obtained customer identification information
- At appropriate times to existing customers on a risk-sensitive basis.

Money transmission businesses should also note that the European Council Regulation EC 1781/2006 requires them to obtain information on customers to accompany every transfer of funds. The information must be verified where the amount exceeds 1,000 euro (or the equivalent in sterling). The Money Transmission Businesses sector guidance in Appendix 8 provides more information on these obligations.

7.5 Determining the extent of customer due diligence measures

MLR 2007 Regulation 7(3) requires that the extent of customer due diligence measures must be decided on a risk-sensitive basis, depending on the type of customer, business relationship, product or transaction.

Businesses must be able to demonstrate to HMRC that the due diligence measures that have been applied are appropriate in view of the risk of money laundering and terrorist financing faced by each business.

Section 6 provides guidance on risk-assessment. Section 8 and Appendix 5 provide more information on risk-based identification and verification procedures.

7.6 Timing of verification of identity

Under MLR 2007 Regulation 9(1), the verification of the identity of the customer, and, where applicable, the beneficial owner, must take place before the establishment of a business relationship or the carrying out of an occasional transaction.

However, if it is necessary not to interrupt the normal conduct of business and there is little risk of money laundering or terrorist financing occurring, then verification may take place during the establishment of the business relationship, provided that it is done as soon as is practicable after contact is first established **(Regulation 9(2)).**

7.7 Non-compliance with customer due diligence measures

MLR 2007 Regulation 11 requires that where a business is unable to comply with the required CDD measures in relation to a customer, then the business must:

- not carry out a transaction with or for the customer through a bank account
- not establish a business relationship
- not carry out an occasional transaction with the customer
- terminate any existing business relationship with the customer
- consider making a report to the Serious Organised Crime Agency (see section 10).

If the problem is caused by the customer not having the 'right' documents or information, perhaps because the person is financially excluded, consideration should be given to whether there are any other ways of being reasonably satisfied as to the customer's identity (see Appendix 5 for details).

If there are no grounds for making a report to SOCA, the business should return the funds, ideally in a way that minimises the risk of the returned funds being effectively laundered in the process.

If the business decides that the circumstances give reasonable grounds for knowledge or suspicion of money laundering or terrorist financing, the firm must retain the funds until consent from SOCA has been obtained to return them.

7.8 Identifying the beneficial owner

7.8.1 General legal requirements

MLR 2007 Regulation 5(b) requires businesses to identify any 'beneficial owner' of the customer and take risk-based and adequate measures to verify his identity. The verification obligation is slightly different from the obligation to verify the identity of customers in that there is no requirement, when identifying beneficial owners, for verification to be done on the basis of documents, data or information obtained from a *reliable* and *independent* source. The business must only take *risk-based* and *adequate* measures with the objective of satisfying itself that it knows who the beneficial owner is.

In many cases the obligation to identify a 'beneficial owner' will not arise because the customer will be an individual acting for himself when he enters into the business relationship or undertakes the transaction. The obligation arises where a customer is acting on behalf of another person, or where the customer is a legal entity such as a company or a trust that involves one or more individual who meets the definition of beneficial owner.

Section 8 and Appendix 5 include guidance on identification and verification procedures for beneficial owners.

7.8.2 Who is a beneficial owner?

Regulation 6 defines who the beneficial owners are for common entities such as companies, partnerships and trusts. As a general rule, 'beneficial owners' are the individuals (or individual) behind the customer who ultimately own or control the customer or on whose behalf a transaction or activity is being conducted.

In deciding who the beneficial owner is in relation to a customer who is not a private individual (e.g. a company or trust) businesses should aim to find out who has ownership of or control over the funds and/or forms the controlling mind and/or management of the entity involved in the transaction or relationship. This should take account of the number of individuals, the nature and distribution of their interests in the entity, and the nature and extent of any business, contractual or family relationship between them.

7.8.3 Corporate bodies

The beneficial owners of companies are the individuals who:

- Ultimately own or control (whether through direct or indirect ownership or control, including through bearer shareholdings) more than 25% of the shares or voting rights in the company. N.B. This test is not used for companies whose shares are listed on a regulated market, or
- Otherwise exercises control over the management of the company.

As well as companies incorporated under the Companies Acts, limited liability partnerships (LLPs), industrial and provident societies and some charities (often companies limited by guarantee or incorporated by Act of Parliament or Royal Charter) are bodies corporate.

7.8.4 Partnerships (other than LLPs)

The beneficial owners of partnerships are the individuals who:

- Are entitled to or controls more than a 25% share of the capital or profits of the partnership or more than 25% of the voting rights, or
- Otherwise exercises control over the management of the partnership.

7.8.5 Trusts

The beneficial owners of trusts are:

- Any individual who is entitled to a specified vested interest in at least 25% of the capital of the trust property
- The class of persons in whose main interest the trust is set up or operates. The class should be described, e.g. ‘A’s children and grandchildren’ or ‘B’s family’ or ‘poor and homeless persons in Greater London’
- Any individual who has control over the trust.

A ‘vested interest’, in this context, means an interest that a person is currently entitled to, without any pre-conditions needing to be fulfilled.

Where an individual is the beneficial owner of a body corporate which is entitled to a specific vested interest in the capital of the trust property or has control over the trust, the individual is to be regarded as entitled to the interest or having control over the trust, or as benefiting from or exercising control over the property of the entity.

Control means a power (whether exercisable alone, jointly with another person or with the consent of another person) under the trust instrument or by law to:

- Dispose of, advance, lend, invest, pay or apply trust property
- Vary the trusts
- Add or remove a person as a beneficiary or to or from a class of beneficiaries
- Appoint or remove trustees
- Direct, withhold consent to or veto the exercise of any of the above powers.

Four forms of control are specifically excluded from the definition of ‘control’. These are listed in MLR 2007 Regulation 6(5)(b).

There is a special rule for estates of deceased persons: the executor, personal representative or administrator is the beneficial owner until administration is complete: **MLR 2007 6(8).**

Further information on the customer due diligence requirements in relation to trusts can be found in the customer due diligence guidance produced by the Law Society.

7.8.6 Other legal entities or legal arrangements that administer and distribute funds

Examples of such entities may include trust-like foreign entities
such as foundations or anstalts. The beneficial owners of these entities are:

- Where the individuals who benefit from the entity or arrangement have been determined, any individual who benefits from at least 25% of the property of the entity or the arrangement
- Where the individuals who benefit from the entity or arrangement have yet to be determined, the class of persons in whose main interests the entity or arrangement is set up or operates
- An individual who controls at least 25% of the property of the entity or arrangement.

Where an individual is the beneficial owner of a body corporate which benefits from or exercises control over the property of the entity or arrangement, the individual is to be regarded as entitled to the interest or having control over the trust, or as benefiting from or exercising control over the property of the entity.

7.8.7 Other cases (e.g. agents)

In all other cases, the beneficial owner will be the individual who ultimately owns or controls the customer or on whose behalf the transaction is being conducted. A common example of this is where the customer is acting as agent for another person (his principal).

7.9 Obtaining information on the purpose and intended nature of a business relationship

7.9.1 What is a business relationship?

A business relationship is defined as a business, professional or commercial relationship between a relevant person (i.e. a business regulated under the MLR 2007) and a customer, which is expected by the relevant person, at the time when contact is established, to have an element of duration (**see MLR 2007 Regulation 2(1))**.

It is an arrangement between the business and the customer that anticipates an ongoing relationship between the two parties. This can be a formal or an informal arrangement.

In general, it is for the business to decide what type of relationship it has with its customers, i.e. whether they establish a business relationship or whether a customer is carrying out separate one-off transactions, even though they may be doing so on a regular basis. However, the following circumstances would indicate that a business relationship exists:

- A customer account is set up
- A loyalty card is issued
- Preferential rates or services are given
- Any other arrangement is put in place that facilitates an ongoing business relationship or repeated contact.

7.9.2 What information is required?

Depending on the business's risk assessment of the situation, information that might be relevant to obtain to understand the purpose and intended nature of the relationship may include some or all of the following:

- Details of the customer's business or employment
- The expected source and origin of the funds to be used in the relationship
- Copies of recent and current financial statements
- The nature and purpose of relationships between signatories and underlying beneficial owners
- The anticipated level and nature of the activity that is to be undertaken through the relationship.

7.10 Occasional transactions

7.10.1 General legal requirements

MLR 2007 Regulation 7 requires that customer due diligence measures must be applied when a business carries out occasional transactions. As defined in MLR 2007, occasional transaction means a transaction (carried out other than as part of an ongoing business relationship) amounting to 15,000 euro (or the equivalent in sterling) or more, whether the transaction is carried out in a single operation or several operations which appear to be linked.

7.10.2 Linked transactions

As part of the risk-assessment and management requirements set out in **MLR 2007 Regulation 20,** businesses must have adequate systems in place to identify transactions exceeding 15,000 euro that have been broken down into a number of separate operations with the possible aim of avoiding identification or other due diligence checks.

In deciding whether there is a risk that transactions are being deliberately split into separate operations, the business needs to consider the circumstances of the transactions. For example:

- Are a number of transactions carried out by the same customer within a short space of time?
- Could a number of customers be carrying out transactions on behalf of the same individual or group of individuals?

- In the case of money transmission, are a number of customers sending payments to the same individual?

Businesses must be able to demonstrate to HMRC that they have adequate checks and controls in place to pick up on such indicators where there is a risk of occasional transactions (i.e. transactions over 15,000 euro) being disguised as smaller transactions.

These checks may also identify the need to make enquiries to establish if there is a beneficial owner involved, and/or result in the need to send a Suspicious Activity Report to SOCA (see section 10).

The controls and checks could include IT systems-based transaction controls and monitoring and/or obtaining information on the source of funds and the purpose of the transactions from customers.

The indicators of risk and the appropriate enquiries to be made should be specified in the business's risk profiles, policies and procedures (see section 6 The risk-based approach).

Businesses should refer to the guidance on risk factors, risk management measures and linked transactions in the relevant industry section in the appendices of this guidance and ensure they keep up-to-date with information on risks and trends provided by industry bodies.

7.11 Simplified due diligence (SDD)

Simplified due diligence is an exception to the obligation to apply the customer due diligence measures set out in MLR 2007 Regulation 5.

MLR 2007 Regulation 13 provides that businesses are not required to apply the customer due diligence measures where they have reasonable grounds for believing that the customer is:

- A credit or financial institution which is subject to the requirements of the Money Laundering Directive, or, if situated in a non-EEA state, is subject to equivalent requirements and is supervised for compliance with those requirements. This category includes Money Service Businesses
- A company whose securities are listed on a regulated EEA market or equivalent overseas subject to specified disclosure obligations
- A UK public authority or a public authority in the EU/EEA subject to certain conditions concerning appropriate check and balance procedures being in place to ensure control of the authority's activity (see MLR 2007 Schedule 2 paragraph 2).

Information on the countries that meet the 'equivalent requirements' test for the purposes of MLR 2007 Regulation 13 is available on the websites of HM Treasury: **www.hm-treasury.gov.uk** and the JMLSG: **www.jmlsg.org.uk**.

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

However, businesses should remember that full customer due diligence measures must be applied even to these customers when there is a suspicion of money laundering or terrorist financing.

Further, the requirement to conduct ongoing monitoring of the business relationship is also fully applicable (see section 9) even in situations where SDD applies.

7.12 Enhanced due diligence (EDD)

7.12.1 General legal requirements

MLR 2007 Regulation 14 requires businesses to apply enhanced due diligence measures on a risk-sensitive basis:

- When the customer has not been physically present for identification purposes
- In respect of a business relationship or occasional transaction with a 'politically exposed person' (PEP) (see section 7.12.3)
- In any other situation which by its nature can presents a higher risk of money laundering.

With the exception of PEPs, the MLR 2007 do not specify what these enhanced due diligence measures must comprise. Instead, businesses should consider applying the EDD measures that are given as examples in **Regulation 14(2)** for customers that are not physically present to be identified or consider the risk and circumstances of each situation and apply an additional measure or measures tailored to that risk.

7.12.2 Non face-to-face customers

Regulation 14 (2) requires that where the customer has not been physically present for identification purposes, specific and adequate measures must be taken to compensate for the higher risk, for example by applying one or more of the following measures:

- Obtaining additional documents, data or information to establish the customer's identity
- Applying supplementary measures to verify or certify the documents supplied or requiring certification by a credit or financial institution
- Ensuring that the first payment of the operations is carried out through an account opened in the customer's name with a credit institution.

7.12.3 Politically exposed persons (PEPs)

What is a PEP?

Under the definition in **MLR 2007 Regulation 14(5),** a politically exposed person is a person who:

- Is or has, at any time in the preceding year, been entrusted with a prominent public function by:
  - (i) a state other than the UK
  - (ii) a Community institution (e.g. the European Parliament), or
  - (iii) an international body (e.g. the U.N.) or
- Is an immediate family member or a 'known close associate' of such a person.

Prominent public functions include:

- Heads of state or government, ministers and deputy or assistant ministers
- Members of parliaments
- Members of supreme or constitutional courts, or other high level judicial bodies
- Members of courts of auditors or the board of central banks
- Ambassadors, charges d'affaires and high-ranking officers in the armed forces and
- Members of the administrative, management or supervisory bodies of State-owned enterprises.

An 'immediate family member' includes:

- A spouse or civil partner
- A partner
- Children and their spouses, or partners, and
- Parents.

A 'known close associate' includes:

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

How can a PEP be identified?

Under **Regulation 20 (2)** businesses must have risk-sensitive policies and procedures in place that can identify when a customer with whom they propose to have a business relationship or carry out an occasional transaction (i.e. of 15,000 euro or more) is a PEP. Where there is a risk that such a customer may be a PEP, businesses should make appropriate enquiries by, for example, asking the customer for background information, researching publicly available information via the internet, or, if the risk is substantial, consulting a commercial website listing PEPs. If there is doubt about whether the customer is a PEP, the customer should be treated as high-risk.

In deciding whether a person is a known close associate of a PEP businesses need only have regard to information that they hold or is publicly known **(Regulation 14(6)).**

What customer due diligence measures must be applied to PEPs?

MLR 2007 Regulation 14(4) requires that businesses that propose to have a business relationship with, or conduct occasional transactions with a politically exposed person must apply enhanced due diligence measures on a risk-sensitive basis. **Regulation 14(4)** specifies that they must:

- Have senior management approval for establishing a business relationship with such a person
- Take adequate measures to establish the source of wealth and source of the funds involved
- Conduct enhanced ongoing monitoring of the business relationship.

7.12.4 Other higher risk situations

MLR 2007 Regulation 14(1) requires enhanced due diligence to be applied in situations which by their nature can present a higher risk of money laundering or terrorist financing. Section 6.2 gives examples of risk indicators. Business's risk assessment and management systems must be capable of identifying such situations and appropriate enhanced due diligence measures must be applied to mitigate the risk involved. For example, enhance due diligence measures could include:

- Obtaining details of the source of the customer's funds and the purpose of the transactions
- Obtaining additional evidence of identity
- Applying supplementary measures to verify or certify the documents supplied or requiring certification by a credit or financial institution
- Ensuring that the first payment of the operations is carried out through an account opened in the customer's name with a credit institution.

In addition, the Treasury may, from time to time, issue advice about high risk situations to the regulated sector. Such advice may include advice about dealing with customers in or receiving funds from countries that present a high risk of money laundering or terrorist financing. Advisory notices have been issued about Iran, Nauru and Antigua & Barbuda following concerns expressed by the Financial Action Task Force. Such advice is published on the Treasury's website at **www.hm-treasury.gov.uk**

7.13 Reliance on third parties to apply customer due diligence measures

MLR 2007 Regulation 17 allows businesses to rely on certain other regulated persons to apply any of the customer due diligence measures provided that they consent to being relied on. However, where the business has relied on a third party, the business remains liable for any failure to apply such measures.

This regulation does not prevent a business applying customer due diligence measures itself by means of an outsourcing service provider or agent.

The persons that may be relied upon are:

In the UK

- A credit or financial institution which is authorised by the FSA
- An auditor, insolvency practitioner, external accountant, tax advisor or independent legal professional who is supervised for the purposes of the MLR 2007 by one of the following professional bodies
    - Association of Chartered Certified Accountants
    - Council for Licensed Conveyancers
    - Faculty of Advocates
    - General Council of the Bar
    - General Council of the Bar of Northern Ireland
    - Institute of Chartered Accountants in England and Wales
    - Institute of Chartered Accountants in Ireland
    - Institute of Chartered Accountants of Scotland
    - Law Society
    - Law Society of Scotland
    - Law Society of Northern Ireland.

In EEA states

- A credit or financial institution, auditor, insolvency practitioner, external accountant, tax advisor or independent legal professional who is:

- Subject to mandatory professional registration recognised by law, and
- Supervised for compliance with the requirements of the money laundering directive.

In a non-EEA state

- A credit or financial institution (or equivalent institution), auditor, insolvency practitioner, external accountant, tax advisor or independent legal professional who is:
  - Subject to mandatory professional registration recognised by law
  - Subject to requirements equivalent to those laid down in the money laundering directive and
  - Supervised for compliance in a manner equivalent to the standards set out in section 2 of chapter V of the money laundering directive.

In Regulation 17, 'financial institution' excludes money service businesses.

Information on the countries that meet the 'equivalent requirements' test for the purposes of MLR 2007 Regulation 17 is available on the websites of HM Treasury: **www.hm-treasury.gov.uk** and the JMLSG: **www.jmlsg.org.uk**.

Policy and decisions on whether to rely on third parties should be part of the risk-assessment and include the obtaining and consideration of relevant information on the status and background of the third party.

The business must put appropriate procedures in place to ensure that the customer due diligence checks are carried out correctly and must take steps to ensure that that the third party will, if requested, provide any information on the customer (and any beneficial owner) which the third party obtained when they applied the customer due diligence measures. Section 12 of this guidance provides further information on these record-keeping requirements.

Businesses can find further information on reliance on third parties in the JMLSG guidance.

7.14 Persons that businesses must not accept as customers

7.14.1 General legal requirements

The UK imposes financial restrictions on persons and entities following their designation at the UN and/or EC. The UK also operates a domestic counter-terrorism regime, where the Government decides to impose financial restrictions on certain persons and entities.

Financial restrictions in the UK are governed by various pieces of legislation. In all circumstances where an asset freeze is imposed, it is unlawful to make payments to or allow payments to be made to designated persons.

A list of all financial restrictions currently in force in the UK is maintained by the Treasury's Asset Freezing Unit. The Consolidated List of persons designated as being subject to financial restrictions can be found on the HM Treasury website at: **www.hm-treasury.gov.uk/financialsanctions**

Further information on financial sanctions can also be found onthis website.

There are specific financial restrictions targeted at the Al-Qaida network and terrorism.

Under the relevant legislation it is a criminal offence for any natural or legal person to:

(a) Deal with the funds of designated persons

(b) Make funds and economic resources, and in the case of Terrorism financial services, available, directly or indirectly to or for the benefit of designated persons, or

(c) Knowingly and intentionally participate in activities that would directly or indirectly circumvent the financial restrictions or enable or facilitate the commission of an offence relating to (a) and (b) above.

'Deal with' means:

(a) In respect of funds:

- Use, alter, move, allow access to or transfer
- Deal with in any other way that would result in any change in volume, amount, location, ownership, possession, character or destination, or
- Make any other change that would enable use, including portfolio management, and

(b) In respect of economic resources:

- Use to obtain funds, goods or services in any way, including (but not limited to) by selling, hiring or mortgaging the resources.

The purpose of this legislation imposing financial restrictions is primarily to prevent the diversion of funds to terrorism and terrorist purposes.

HM Treasury has the power to grant licences exempting certain transactions from the financial restrictions. Requests to dis-apply the financial restrictions in relation to a designated person are considered by the Treasury on a case-by-case basis to ensure that there is no risk of funds being diverted to terrorism. To apply for a licence, please contact the Asset Freezing Unit using the contact details below.

7.14.2 Action by relevant businesses

Businesses need to have appropriate policies and procedures in place to monitor transactions in order to prevent breaches of the financial restrictions legislation.

For manual checking, businesses can register with the Asset Freezing Unit update service (directly or via a third party).

If checking is automated, businesses will need to ensure that the relevant software includes checks against the latest consolidated list.

The Asset Freezing Unit may also be contacted to provide guidance and to assist with any concerns regarding financial sanctions at:

Asset Freezing Unit

Phone: **020 7270 5664/5454**

Fax: **020 7451 7677**

Email: **assetfreezingunit@hm-treasury.gov.uk**

In the event that a customer or a payee is identified as a designated individual following receipt of money, e.g. during a money transmission process, the transaction must not proceed unless a licence is granted by the Treasury, as this would be a breach of the financial restrictions. The Treasury should be informed immediately and the transaction suspended pending their advice. No funds should be returned to the designated person. The firm may also need to consider whether there is an obligation also to report to SOCA under the Proceeds of Crime Act 2002 or the Terrorism Act 2000.

Further guidance on reporting to SOCA can be found in Section 10 of this guidance.

Written reports can also be made to the Asset Freezing Unit at:

The Asset Freezing Unit
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ

7.14.3 HM Treasury action against breaches of financial sanctions

There are criminal penalties which apply in relation to breaches of the financial restrictions. However, in line with the principles set out in the Code for Crown Prosecutors, prosecution of a firm suspected to be in breach of the financial restrictions regime in the UK would be likely only where the prosecuting authorities consider this to be in the public interest, and where they believe that there is enough evidence to provide a realistic prospect of conviction.

Appendices 7 and 8 include guidance on industry good practice on compliance with the financial restrictions requirements for Bureaux De Change and Money Transmission Businesses.

Firms should ensure that they act in accordance with appropriate and evidenced risk-based policies and procedures.

8. Identity and verification

8.1 Introduction

This section explains the principles and criteria to be applied to obtaining and verifying evidence of the identity of customers and their beneficial owners. The specific legal requirements for customer due diligence, including those in relation to beneficial owners, are set out in section 7. Details of the documents and other evidence of identity that are acceptable are set out in Appendix 5.

8.2 Nature and extent of evidence

8.2.1 Customers

Identifying a customer is a two part process. The business first identifies the customer by obtaining a range of information, such as their name, address and date of birth. The second part is verifying this information through the use of reliable, independent source documents, data or information.

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

Evidence of identity can take a number of forms. For individuals, the easiest way of being reasonably satisfied as to someone's identity is through identity documents such as passports and photo card driving licences.

It is also possible to be reasonably satisfied as to a customer's identity based on other forms of confirmation, including, in appropriate circumstances, written or otherwise documented assurances from independent and reliable persons or organisations that have dealt with the customer for some time.

How much identity information or evidence to ask for, and what to verify, in order to be reasonably satisfied as to a customers identity, are for the judgement of the business, based on their risk-based identification and verification procedures. These procedures should take into account factors such as:

- The type of product or service sought by the customer
- The nature and length of any existing or previous relationship with the customer
- Whether the customer is physically present.

Evidence of identity can be documentary or electronic, or a combination of both. A record must be kept of the evidence taken of the customer's identity and the supporting documents relating to the due diligence checks made.

There is no requirement to take a copy of the evidence seen to identify the customer. It is sufficient to record and hold details of the identification seen, e.g. the passport issuing authority and reference number, provided it is robust enough to enable law enforcement officers to trace the original document at a later date.

8.2.2 Beneficial owners

The Risk-Based Approach should also be applied to verifying the identity of beneficial owners. The customer due diligence requirement is that the business must take risk-based and adequate measures so that it is satisfied that it knows the identity of any beneficial owner(s).

Where a private individual is acting for another individual who is the beneficial owner, in normal circumstances, the identity of the beneficial owner should be verified in the same way as it would be for a direct customer (see section 17.1 in Appendix 5).

In the case of trusts, companies and other legal entities, the business must be satisfied that the ownership and control structures are understood. Further guidance on identifying the beneficial owners of companies, trusts etc. is provided in section 17.2 in Appendix 5.

8.3 Documentary evidence

Documentary evidence of a person's identity differs in reliability and independence. Some documents are issued after in-depth checks on an individual's identity have been undertaken others are issued on request without any checks being carried out. There is a broad hierarchy of documents:

- Documents issued by government departments and agencies, or by a court, then
- Documents issued by other public sector bodies or local authorities, then
- Documents issued by regulated firms in the financial services sector, then
- Those issued by other firms subject to the MLR 2007 or to comparable legislation, then

- Those issued by other organisations.

Any documentary item with an expiry date or expiry dates should only be accepted as evidence before any expiry date has been reached.

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

Businesses will need to be prepared to accept a range of documents, and they may wish also to employ electronic checks, either on their own or in tandem with documentary evidence.

8.4 Electronic evidence

Most customers, who live in the UK, will have built up an electronic 'footprint', i.e. a profile of checks that have been made, for example by utility providers, telephone companies, credit agencies, banks etc. Over time, individuals build up a score which is based on the number of checks made, the range of sources the information has been verified from etc. It is the score that determines the reliability of the electronic information held.

Businesses can access these records, either directly or through an independent third party organisation, and use them as a way of confirming customers' details. This can provide a useful basis for having confidence in a customer's identity. N.B. Checks made for this purpose don't require the customer's permission but they must be informed that the check is to take place.

8.5 Nature of electronic checks

For an electronic check to provide satisfactory evidence of identity on its own, it must use data from multiple sources collected over a period of time, or incorporate checks that assess the strength of the information supplied. An electronic check that accesses data from a single source (e.g. a single check against the electoral roll) is not enough on its own to provide satisfactory evidence of identity.

A number of commercial agencies which access many data sources are accessible online to businesses and can provide a comprehensive level of verification. Such agencies use databases of both positive and negative information, and many also access data sources that can identify high-risk conditions, e.g. known identity frauds or inclusion on a sanctions list.

8.6 Criteria for use of an electronic provider

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

- It is recognised through registration with the Information Commissioners Office to store personal data
- It uses a range of positive information sources that can be called upon to link the customer to both current and previous circumstances
- It accesses negative information sources such as databases relating to identity fraud and deceased persons
- It accesses a wide range of alert data sources, and
- It has transparent processes that enable the firm to know what checks were carried out, what the results of these checks were, and what they mean in terms of how much certainty they give as to the identity of the subject.

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

9. Ongoing monitoring of customers in a business relationship

9.1 The requirement to monitor customers' activities

Businesses must conduct ongoing monitoring of their business relationships with their customers. **MLR 2007 Regulation 8** states that ongoing monitoring of business relationships means:

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

The extent to which scrutiny of transactions and knowledge of customer enquiries are undertaken should be determined using the risk-based approach and must be applied in accordance with the risks that are assessed to be present in relation to the customer, products, transactions, delivery channels and geographical locations involved.

Monitoring customer activity helps to identify unusual activity. If unusual events cannot be rationally explained, they may involve money laundering or terrorist financing. Monitoring customer activity and transactions throughout a relationship helps give greater assurance that the business is not being used for the purposes of money laundering or terrorist financing.

9.2 What is monitoring?

The basic requirements of a monitoring system are that:

- It flags up transactions and/or activities for further examination
- These reports are reviewed promptly by the right person(s), and
- Appropriate action is taken on the findings of any further examination.

Monitoring can be either:

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

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

In designing monitoring arrangements, it is important that appropriate account is taken of the frequency, volume and size of transactions carried out by customers, and the risks that are present in respect of the customer and the product.

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

9.3 Manual or automated?

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

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

The effectiveness of a monitoring system, automated or manual, in identifying unusual activity will depend on the quality of the parameters which determine what alerts it makes, and the ability
of staff to assess and act as appropriate on these outputs.

9.4 Staff awareness

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

9.5 Customer information

MLR 2007 Regulation 8(2)(b) states that monitoring must involve keeping the documents data or information obtained for the purpose of applying customer due diligence measures up-to-date. This obligation also applies where a business has relied on another relevant business to apply CDD measures under **Regulation 17**.

10. Suspicious Activity reporting to the Serious Organised Crime Agency (SOCA)

10.1 General legal and regulatory obligations

Under **Part 7 of the Proceeds of Crime Act and Part 3 of the Terrorism Act**, businesses in the regulated sectors and their employees are required to disclose information to SOCA in circumstances where they:

- Know or suspect, or
- Have reasonable grounds for knowing or suspecting

that another person is engaged in money laundering or terrorist financing.

MLR 2007 Regulation 20(2) requires that businesses in the regulated sectors must have policies and procedures under which:

- An individual in the organisation is appointed as a Nominated Officer who is responsible for receiving disclosures of information concerning suspicions of money laundering, made under the requirements of Part 7 of the Proceeds of Crime Act and Part 3 of the Terrorism Act
- Employees report suspicious activity to the Nominated Officer, and
- The Nominated Officer considers disclosures in the light of any relevant information which is available to the business and determines whether it gives rise to knowledge or suspicion or reasonable grounds for knowledge or suspicion of money laundering or terrorist financing.

In some businesses, the Nominated Officer is called the Money Laundering Reporting Officer (MLRO).

'In the organisation' means from within the same business, business group, or corporate structure.

Sole proprietors who have no members of staff do not need to appoint a Nominated Officer because they are directly responsible for making disclosures under PoCA and Terrorism Act.

The failure of any person to disclose such information is an offence under Part 7 of the PoCA or Part 3 of the Terrorism Act.

10.2 The meaning of knowledge, suspicion and reasonable grounds for knowledge or suspicion

For the purposes of the PoCA and the TA, **knowledge** means knowledge of money laundering activity based on information that came to the member of staff or Nominated Officer in the course of the business in the regulated sector.

Suspicion is an opinion held that is based on information or circumstances but without certainty or proof. Unusual transactions are not necessarily suspicious, however, **MLR 2007 Regulation 20** requires that unusual transactions and any other activity that is regarded as particularly likely by its nature to be related to money laundering or terrorist must be identified and scrutinised, which could result in suspicion requiring disclosure.

Reasonable grounds for knowledge or suspicion arise where the facts or circumstances, if viewed objectively, would lead to an expectation that a reasonable person working in the relevant business would know or suspect that someone was engaged in money laundering or terrorist financing.

10.3 Making disclosures to the Serious Organised Crime Agency (SOCA)

Disclosures are made by submitting a Suspicious Activity Report (SAR).

The preferred means of making reports to SOCA is electronically through the SARS online system at **www.soca.gov.uk**

Where this route is not practicable, reports should be made either electronically through encrypted email links approved by SOCA, or by fax, first class post, or courier. Where reports are submitted in paper format they should be typed or word-processed on the standard forms.

The basis for the knowledge or suspicion of money laundering or terrorist financing should be set out in a clear and concise manner.

The SAR should contain as much relevant information about the customer, transaction or activity as possible.

The Nominated Officer must report suspicious approaches or proposed transactions or activity, even if no transaction or activity takes place.

10.4 Internal reporting procedures

All relevant businesses must maintain internal procedures which ensure employees report suspicious activity to the Nominated Officer.

A report must be made as soon as a decision is made that there are reasonable grounds to suspect money laundering. Suspicion may arise before or after a transaction takes place.

Before deciding to make a report to SOCA, the Nominated Officer will need access to all the business's relevant records. The business must therefore, take reasonable steps to ensure its Nominated Officer has access to such information. This may include:

- The financial circumstances of the customer or a person on whose behalf the customer is acting, and
- The features of the transaction.

In addition, the Nominated Officer should:

- Consider the level of identity information held on the customer and any information held on his personal circumstances that might be available to the business, and
- Review other transaction patterns and volumes through the account and any other accounts in the same name.

The Nominated Officer should also take into consideration any additional risks where the customer is located outside the UK, particularly if the customer is located in a high-risk jurisdiction.

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

10.5 SARs completed by agents

The Nominated Officer of the registered business has an important role to play in deciding whether or not a report from within the business results in reasonable grounds for suspicion. Principals and agents should agree on a procedure that ensures the report reaches SOCA as soon as possible with as much relevant information as possible. This can be achieved in one of two ways:

- The agent sends the SAR direct to SOCA copying in the Principal, or
- The agent routes the SAR to the Principal who sends it to SOCA or decides a SAR is not appropriate.

If SARs are sent direct to SOCA they should be endorsed to the effect that a copy has gone to the Nominated Officer, in order to reduce the scope for duplication or confusion.

10.6 Consent under PoCA

Where a customer's transaction or activity request raises grounds for suspicion of potential money laundering or terrorist financing activity, consent must be sought from SOCA before the transaction is completed, unless it is not practicable to do so (see below).

In urgent cases, SOCA can be contacted by telephone to respond to requests for consent. SOCA will notify a decision as soon as possible.

It is an offence for a Nominated Officer or sole trader to proceed with a transaction if consent has been requested, but not yet granted, within seven working days. The seven working days begin the day after SOCA receives the report. If a response has not been received from SOCA after seven working days, the transaction can proceed, although good practice should include further contact with SOCA to ensure a notice of refusal hasn't been sent.

If it is not possible to suspend a transaction in order to obtain prior consent, for personal safety reasons or to avoid tipping-off the customer that a report is being made, a suspicious activity report must be submitted as soon as possible after the transaction is completed. You will need to demonstrate that you have a good reason for not seeking prior consent to the transaction. If you are unable to provide adequate justification for not seeking consent you may be liable to prosecution under the PoCA.

10.7 Tipping-off

It is a criminal offence under **PoCA Part 7** for anyone, following a disclosure to a Nominated Officer or to SOCA, to do or say anything that might either 'tip off' another person that a disclosure has been made or prejudice an investigation. The Terrorism Acts contain similar offences.

This means that businesses must not tell a customer:

- That a transaction was/is being delayed because consent from SOCA has been requested
- That details of their transactions or activities will be/have been reported to SOCA
- That they are being investigated by law enforcement.

Reasonable enquiries of a customer concerning the background to a business or transaction, as part of customer due diligence checks will not give rise to a tipping-off offence.

10.8 Suspicion indicators

The following lists are not exhaustive but set out some of the main indications that a transaction is suspicious.

10.8.1 New customers and occasional or 'one-off' transactions:

- Checking identity is proving difficult
- The customer is reluctant to provide details of their identity
- There is no genuine reason for the customer using the services of an MSB
- A cash transaction is unusually large
- The cash is in used notes and/or small denominations
- The customer requests currency in large denomination notes
- The customer will not disclose the source of cash
- The explanation for the business and/or the amounts involved are not credible
- A series of transactions are structured just below the regulatory threshold for due diligence identity checks
- The customer has made an unusual request for collection or delivery
- Transactions having no apparent purpose or which make no obvious financial sense, or which seem to involve unnecessary complexity
- Unnecessary routing of funds through third parties.

10.8.2 Regular and established customers

- The transaction is different from the normal business of the customer
- The size or frequency of the transaction is not consistent with the normal activities of the customer
- The pattern of transactions has changed since the business relationship was established
- Money transfers to high-risk jurisdictions without reasonable explanation, which are not consistent with the customer's usual foreign business dealings
- Sudden increases in the frequency/value of transactions of a particular customer without reasonable explanation.

10.8.3 Examples where customer identification issues have potential to indicate suspicious activity

- The customer refuses or appears reluctant to provide information requested
- There appears to be inconsistencies in the information provided by the customer
- The customer's area of residence is inconsistent with other profile details such as employment
- An address appears vague or unusual
- The supporting documentation does not add validity to the other information provided by the customer
- The customer is in a hurry to rush a transaction through, with promises to provide the information later.

10.8.4 Examples of activity that might suggest to staff that there could be potential terrorist activity

- The customer is unable to satisfactorily explain the source of income
- Frequent address changes
- Media reports on suspected or arrested terrorists or groups.

11. Staff awareness and training

11.1 General legal obligations

MLR 2007 Regulation 21 requires businesses to take appropriate measures so that all relevant employees are:

- Made aware of the law relating to money laundering or terrorist financing, and
- Regularly given training in how to recognise and deal with transactions and other activities which may be related to money laundering or terrorist financing.

11.2 Who should be trained?

Employees should be trained in what they need to do to carry out their particular roles in the organisation. All customer-facing staff will require training in relation to recognising and handling suspicious transactions. Nominated Officer/MLROs, senior managers and others involved in ongoing monitoring of business relationships and other internal control procedures will need different training, tailored to their particular functions.

11.3 What should training cover?

Businesses must ensure that relevant employees are made aware of their responsibilities under the Proceeds of Crime Act and the Terrorism Act to report knowledge or suspicion to the Nominated Officer and the requirements under MLR 2007 for the business to apply customer due diligence measures.

Training to enable employees to recognise and deal with suspicious transactions should include:

- The identity and responsibilities of the Nominated Officer (or MLRO)
- The potential effect of any breach of the law on the firm, its employees personally and its clients
- The risks of money laundering and terrorist financing that the business faces
- The vulnerabilities of the business's products and services
- The policies and procedures that have been put in place to reduce and manage the risks
- Customer due diligence measures, and, where relevant, procedures for monitoring customers' transactions
- How to recognise potential suspicious activity
- The procedures for making a report to the Nominated Officer
- The circumstances when consent is to be sought and the procedure to follow
- Reference to industry guidance and other sources of information, e.g. SOCA, FATF.

11.4 How often should training be given?

Businesses should ensure that the frequency of training is sufficient to maintain the knowledge and competence of staff to apply customer due diligence measures appropriately and in accordance with the business's risk assessments of the products or services they offer.

It is important, as part of ongoing staff training, to make staff aware of changing behaviour and practices amongst money launderers and those financing terrorism. A range of information on this can be found on the internet and through the media, for example, the website of the Financial Action Task Force **www.fatf-gafi.org** Training methods and assessment should be determined by the individual business according to the size and complexity of the business.

12. Record-keeping

12.1 General legal requirements

The purpose of **MLR 2007 Regulation 19** on record-keeping is to require a business to be able to demonstrate its compliance with the MLR 2007, through keeping evidence and records of due diligence checks made and information held on customers and transactions. These records may be crucial in any subsequent investigation by SOCA, the police or HMRC. They will enable the business to produce a sound defence against any suspicion of involvement in money laundering or terrorist financing, or charges of failure to comply with the Regulations.

12.2 The records that must be kept

The records that must be kept are:

- A copy of, or the references to, the evidence of the customer's identity obtained under the customer due diligence requirements in the Regulations
- The supporting records in respect of business relationship or occasional transactions which are the subject of customer due diligence measures or ongoing monitoring.

In relation to the evidence of a customer's identity, businesses must keep the following records:

- A copy of the identification documents accepted and verification evidence obtained, or
- References to the evidence of customer's identity.

Transaction and business relationship records (e.g. account files, relevant business correspondence, daily log books, receipts, cheques etc.) should be maintained in a form from which a satisfactory audit trail may be compiled, and which may establish a financial profile of any suspect account or customer.

12.3 Persons who are relied on by another person to apply any customer due diligence measures

Where a person is relied on by another business to apply customer due diligence measures on their behalf under the arrangements set out in section 7.13 of this guidance, he must keep the records specified above for five years beginning from the date on which he is relied on in relation to any business relationship or transaction.

A person who is relied on must, if requested by the person relying on him within the time specified above:

- As soon as reasonably practicable make available to the person who is relying on him any information about the customer (and any beneficial owner) which he obtained when applying customer due diligence measures and
- As soon as reasonably practicable forward to the person who is relying on him copies of any identification and verification data and any other relevant documents on the identity of the customer (and any beneficial owner) which he obtained when applying the measure.

12.4 Businesses which rely on another person to apply customer due diligence measures

Where a business relies on another person to apply any customer due diligence measures on their behalf, it must take steps to ensure that the third party will, if requested within the time specified above:

- As soon as reasonably practicable make available to him any information about the customer (and any beneficial owner) which the third party obtained when applying customer due diligence measures, and
- As soon as reasonably practicable forward to him copies of any identification and verification data and other relevant documents on the identity of the customer (and any beneficial owner) which the third party obtained when applying
  those measures.

These requirements do not apply where the business applies customer due diligence measures by means of an outsourcing service provider or agent, although, because the business is responsible for applying CDD and storing its records, it would be prudent for it to be in a position to ensure that it receives or can quickly access customer identification records where any of these services (or records storage) are outsourced.

12.5 How long must the customer keep due diligence records?

Evidence of customer's identity records must be kept for five years beginning on the date on which the occasional transaction is completed or the business relationship ends.

Records of transactions (whether undertaken as occasional transactions or part of a business relationship) must be kept for five years beginning on the date on which the transaction is completed.

All other records must be kept for five years beginning on the date on which the business relationship ends.

12.6 In what format must the records be kept?

Most businesses want to keep to a minimum the volume and density of records which need to be kept whilst still complying with the Regulations. Records may therefore be kept:

- By way of original documents
- By way of good photocopies of original documents
- On microfiche
- In scanned form
- In computerised or electronic form.

12.7 Penalties for failure to keep records

Where the record keeping obligations under the MLR 2007 are not observed, a business or person is open to financial penalties or potentially prosecution including imprisonment for up to two years.

13. APPENDIX 1: Criminal offences and penalties for money laundering and terrorist financing

13.1 The Proceeds of Crime Act 2002 (PoCA) Part 7

This sets out the primary offences relating to money laundering, which includes the laundering of terrorist funds. There are six separate offences in Part 7 of SOCA. The main three offences are:

1. Concealing, disguising, converting, transferring and/or removing criminal property from the UK: **section 327**
2. Entering into or becoming involved in an arrangement which facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person: **section 328**
3. The acquisition, use and/or possession of criminal property: **section 329**.

Conviction for offences 1-3 above can result in imprisonment for up to 14 years and/or an unlimited fine.

4. The fourth offence applies to individuals working in the regulated sector (including MSBs, TCSPs and HVDs). This includes all individuals, at whatever level (employee, manager, director etc.) who work in a business activity in the regulated sector. The scope of the regulated sector is set out in Schedule 9 to PoCA (and consists of the same businesses caught by regulations 3 and 4 of the Money Laundering Regulations 2007). This offence is: Failing to disclose knowledge or suspicion, or reasonable grounds for knowledge or suspicion of money laundering as soon as is reasonably practicable to the Nominated Officer or SOCA (see section 10 for the role of the Nominated Officer in reporting suspicious activity) **section 330**.
5. The fifth offence applies to the Nominated Officer for the business, or the sole proprietor: Failing to disclose knowledge or suspicion or reasonable grounds for knowledge or suspicion of money laundering as soon as is reasonably practicable to SOCA **section 331**.

Conviction for offences 4 - 5 can incur up to five years' imprisonment and/or an unlimited fine.

The final offence in Part 7 of PoCA is:

6. Tipping off, i.e. revealing that a disclosure of suspicion of money laundering has been made or that an investigation into money laundering offences is being carried out, or contemplated, where this is likely to prejudice an investigation: **section 333A** (inserted by The Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulation 2007). N.B. There are certain exceptions in relation to disclosures within and between regulated businesses, supervisory authorities, investigators and legal or professional advisors.

Conviction for tipping off offences can incur up to five years' imprisonment and/or an unlimited fine.

In addition, **Section 342 of PoCA** makes it an offence to make a disclosure which is likely to prejudice a money laundering investigation or falsify, conceal, destroy or otherwise dispose of documents which are relevant to the investigation. Conviction for these offences can incur up to five years' to imprisonment and/or an unlimited fine.

Where criminal proceeds have already arisen, **Section 340(11) of PoCA** includes within the definition of money laundering any attempt, conspiracy or incitement to commit an offence under Sections 327 - 329 of PoCA as well as aiding, abetting, counselling or procuring an offence under Sections 327 - 329 of PoCA.

13.2 The Terrorism Act 2000 Part 3

This sets out the primary offences relating to the funding of terrorism, which are:

- Fund raising for the purpose of terrorism: **section 15**
- Using or possessing money for the purpose of terrorism: **section 16**
- Involvement in funding arrangements: **section 17** and
- Money laundering (facilitating the retention or control of money which is destined for, or is the proceeds of terrorism): **section 18.**

It is an offence to attempt to commit an offence under sections 15 - 18 of the TA 2000 even if terrorist property has not come into being, e.g. under **Section 15(1) of the TA 2000** where the invitation to provide money or other property for terrorist financing is in itself an offence.

An act done outside the UK that would be an offence under sections 15 to 18 if done in the UK is also an offence: **section 63**.

Conviction for any of the above offences can incur up to 14 years' imprisonment and/or an unlimited fine.

There are also offences in relation to:

- Failure to disclosure the belief or suspicion that someone has committed, or attempted to commit, any of the above offences: **section 21A**.

Conviction for this offence can incur up to five years' imprisonment and/or an unlimited fine.

- Tipping off, i.e. revealing that a disclosure of suspicion of terrorist funding has been made or that an investigation into terrorist funding offences is being carried out, or contemplated, where this is likely to prejudice an investigation: **section 21D** (introduced by The Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulation 2007). N.B. This section applies to persons working in a business in the regulated sector.

Conviction for this offence can incur up to two years' imprisonment and/or an unlimited fine.

14. APPENDIX 2: Sanctions for failure to comply with the Money Laundering Regulations 2007

14.1 Civil penalties

Regulation 42 gives HMRC the power to impose civil penalties on businesses that fail to comply with the requirements of the Regulations in respect of:

- Notification and registration requirements
- Customer due diligence measures
- Ongoing monitoring of a business relationship
- Enhanced customer due diligence and ongoing monitoring
- Record-keeping
- Policies and procedures to prevent money laundering and terrorist financing
- Appointing a Nominated Officer and internal reporting procedures
- Training of employees.

There is no upper limit in Regulation 42 on the amount of penalties. Penalties will be for an amount that is considered appropriate for the purposes of being effective, proportionate and dissuasive.

Businesses can ask HMRC to review the decision to impose a penalty, or of the amount of the penalty, and decisions to refuse or cancel registration. Penalty and registration decisions can also be appealed to the VAT and Duties Tribunal.

14.2 Criminal offences

MLR 2007 Regulation 45 sets out the offence of failing to comply with the MLR 2007 obligations, including those relating to registration, customer due diligence measures, record-keeping, training, and adequate and appropriate systems, policies and procedures to prevent money laundering and terrorist financing.

Conviction under the MLR 2007 can incur up to two years' imprisonment and/or an unlimited fine.

15. APPENDIX 3: template for policy statement and risk assessment

The Risk-Based Approach to the prevention of money laundering and terrorist financing

15.1 Policy statement

This section should include a general statement on the business's recognition of its legal obligations to have procedures and controls in place to deter, disrupt and detect money laundering and terrorist financing.

This section could also include comments on:

- The culture and values to be adopted and promoted within the business towards the prevention of money laundering and terrorist financing
- A commitment to ensuring all relevant staff are made aware of the law and their obligations under it and are regularly trained in how to recognise suspicious activity
- Recognition of the importance of staff promptly reporting suspicious activity
- A summary of the firm's approach to assessing and managing its money laundering and terrorist financing risk
- Allocation of responsibilities to specific persons
- A summary of the firm's procedures for carrying out appropriate identification, verification, customer due diligence, and monitoring checks on the basis of their risk-based approach
- A summary of the appropriate monitoring arrangements in place to ensure that the firm's policies and procedures are being carried out.

15.2 Risk assessment

Date of risk assessment	

15.3 Customer profile

Include relevant customer profile information, for example:

Number/ % age of customers:	
In a business relationship, (See section 7.9.1)	
Regular customers doing one-off transactions	
Passing trade	

How are customers introduced to the business?	
Through recommendation/word of mouth from existing customers	
Through advertising	
Off the street passing trade	
Other sources	
Are there any non face-to-face customers? If so, estimate the number and value of transactions	
Any potential Politically Exposed Persons? (See section 7.12.3)	
General description of usual types of customer	

and purpose of transactions, e.g. regular small amounts of money sent to family overseas	
Any significant customers outside the normal customer profiles?	
What is the value or % age of cash transactions?	

15.4 Risk identification

Explain the risks inherent in the industry and faced by this particular business, for example:

- A high volume of cash transactions creates an opportunity for placement of criminal cash, including through 'smurfing' (see Glossary for definition)
- Remittance of funds to countries with high levels of organised crime or drug production/distribution
- Making funds available to persons designated as subject to financial sanctions
- Customers who are in a public position and/or location which carries a risk of exposure to the possibility of corruption
- Customers with complex business ownership structures with the potential to conceal underlying beneficiaries
- Non face-to-face customers increases the risk of impersonation fraud
- Transmission of money from or to individuals, organisations or locations that may be linked to terrorist activity.

15.5 Risk factors and response

Risk should be assessed in relation to:

- Customers – types and behaviours
- Products and services
- Delivery channels, e.g. cash over the counter, electronic, wire transfer, cheque
- Geographical areas of operation, e.g. location of business premises, source or destination of customers' funds.

List and explain the risk factors that are relevant to the business and document the actions that will be taken to mitigate these risks as they arise, i.e. the types of customer due diligence and ongoing monitoring measures that will be applied, or the management controls in place within the business. A summary of the customer due diligence and ongoing monitoring requirements is provided in Appendix 4.

The table below includes examples of the types of risk factors that may be relevant. **N.B. This list is not exhaustive. Businesses will need to add any other relevant risk factors.**

Risk factors	Explain how the risk factor applies	What procedures are in place to manage and mitigate the risks, e.g. internal control procedures additional ID documents/checks for higher risk transactions above a specified amount source of funds enquiries in specified or unusual circumstances transaction monitoring to identify suspicious activity?
Customer types and behaviour		
Customers with businesses that handle large amounts of cash		
Customers with complex business ownership		

structures with the potential to conceal underlying beneficiaries		
Customers who are in a public position which could create a risk of exposure to the possibility of corruption (PEPs – see section 7.12.3)		
Customers based in or conducting business in, or through, a high risk jurisdiction, or a jurisdiction with known higher levels of corruption, organised crime or drug production/ distribution		
Customers who are not local to the business		
New customers carrying out large transactions		
Customers carrying out regular large transactions		
A number of transactions below the amount requiring ID checks carried out by the same customer within a short space of time		
A number of customers sending payments to the same individual		
Non face-to-face customers		
Situations where the source of funds cannot be easily verified		
Products/transaction types		
Complex or unusually large transactions		
Unusual patterns of transactions which have no apparent economic or visible lawful purpose		
Uncharacteristic transactions which are not in keeping with the customer's known activities		
A sudden increase in business from an existing customer		
A high level of transactions for amounts just below the amount requiring ID checks		
Peaks of activity at particular locations or at particular times		

Delivery channels		
Large cash transactions		
Occasional or one-off transactions as opposed to business relationships		
Business organisation/ geographical area of operation		
Large number of branches		
Large number of agents		
Geographical locations of operation		
Number of employees and turnover of staff		
Money sent to or received from areas known to have high levels of criminality or terrorist activity		

Attach or refer to employee instructions for customer due diligence checks.

15.6 Customer due diligence: policy on acceptable ID and satisfactory verification

Include, for example:

- How and when are ID documents verified?
- What forms of identity are acceptable?
- What checks are carried out on the documents?
- How are the checks recorded?
- Are customer files set up to hold records of ID?
- Are business ID cards issued to customers?
- Do the cards include a photograph?
- Is there a risk that these cards could be used by someone else?
- How is that risk addressed?
- In what circumstances are checks made to the Consolidated List of persons designated as being subject to financial restrictions on HM Treasury's website?

Attach or refer to relevant employee instructions.

15.7 Customer due diligence: business relationships

15.7.1 Customer due diligence when establishing a business relationship

Explain the business's policy and procedures in respect of recognising when it is about to enter into a business relationship.

What information is obtained in respect of the purpose and intended nature of the business relationship?

What information on the customer's identity is obtained?

What verification is carried out?

How are customers assessed for risk? What criteria are used?

Attach or refer to relevant internal guidance and procedural instructions.

15.8 Ongoing monitoring of business relationships

Give details of the procedures and processes for conducting ongoing monitoring, including the application of trigger event systems to prompt scrutiny of transactions and/or the policy and method of reviewing customer files to monitor activity.

Explain the risk indicators that are used and the procedures for making appropriate enquiries concerning the source of funds and the customer's business activities.

Include details of who in the business is responsible for making such enquiries and reviewing the results of the enquiries.

How does the business ensure that that documents and information are up-to-date?

What systems of enhanced ongoing monitoring of transactions and customer activity are in place for high-risk customers?

For politically exposed persons (see section 7.12.3), is senior management approval obtained before establishing a business relationship?

Attach or refer to relevant internal guidance and procedural instructions.

15.9 Monitoring the risk

What analysis is carried out in respect of:	
Number and size of transactions	
Customer profiles	
Patterns and fluctuations in trade	
Suspicious activity	
Any other factors?	

Attach or refer to reports on risk monitoring.

List details of changes to the risk assessment

Date Risk Assessment reviewed	Change made (e.g. new product, new risk factor or change in status to significant or high)	Comments (e.g. sudden jump in sales, change to customer profile)

15.10 Internal controls and communication

Explain how the systems of internal control and communication are managed. This section could include, for example:

- Senior management responsibilities
- Provision of regular and timely information to senior management on money laundering and terrorist financing risks
- Training of relevant employees on their legal responsibilities for preventing money laundering and terrorist financing and reporting suspicious activity
- Ensuring that agents have satisfactory systems and procedures in place for undertaking customer due diligence measures and reporting suspicious activity
- Reviewing and updating risks and controls so that policies and procedures continue to effectively manage the risks
- Communicating relevant information to employees on matters concerning the business's policies or procedures, e.g. risk alerts.

Attach or refer to relevant internal guidance and procedural instructions.

15.11 Monitoring and managing compliance

Explain what action is taken to check that the business is complying with its legal obligations concerning customer due diligence, ongoing monitoring of business relationships and reporting suspicious activity through, for example:

- Ensuring that appropriate monitoring processes and procedures are established and maintained
- Conducting regular audits or exercises that test that procedures are adhered to throughout the business.

Attach or refer to relevant internal guidance and procedural instructions.

15.12 Suspicious Activity Reporting

Include details of the Nominated Officer.

Explain the internal reporting procedures.

How are situations requiring consent managed?

What analysis or monitoring of transactions is undertaken to detect suspicious transactions or customer activity?

Attach or refer to employee instructions on identifying and reporting suspicious activity and procedures for monitoring transactions.

15.13 Record-keeping

Explain how transaction, payment and customer information is recorded and held.

Attach or refer to relevant internal guidance and procedural instructions

15.14 Training

Explain the policy and practice on training, for example:

When and how are new employees trained?

What does the training cover?

How often is training given?

Attach or refer to relevant internal guidance and procedural instructions.

16. APPENDIX 4: Summary of customer due diligence and ongoing monitoring

A full explanation of the customer due diligence (CDD) and enhanced customer due diligence (EDD) requirements is provided in section 7. Further guidance on identification and verification is provided in section 8. Money Transmission Businesses must also follow the requirements of the EC Wire Transfer/Payments Regulation which requires verification of customers' identity for all transactions over 1,000 euro (or the equivalent in sterling). These requirements are explained in Appendix 8. Ongoing monitoring (OM) is explained in section 9. Businesses must determine the appropriate customer due diligence and ongoing monitoring measures to apply on a risk-sensitive basis, according to the risks relating to:

- Customers – type and behaviour
- Products and services
- Delivery Channels, e.g. cash over the counter, electronic, wire transfer, cheque
- Geographical locations, e.g. source or destination of funds or goods.

References to the relevant Regulations and sections of the guidance are included in the table.

Comment [71]: Can the table be widened to the width of the page?

MLR 2007	Type of customer activity	Customer due diligence and ongoing monitoring required
Reg. 7 (CDD)	Establishing a business relationship (S.7.9.1).	Obtain and verify ID documents, data or information (S.8 and Appendix 5). Where appropriate, identify and verify details of the beneficial owner (S.7.8).
Reg. 8 (OM)	Transactions undertaken throughout the course of a business relationship.	Obtain information on the purpose and intended nature of the business relationship (S.7.9). Carry out ongoing monitoring. This means: • Scrutiny of transactions, including, where necessary, the source of funds and • Keeping documents and information on the customer up to date (S9).
Reg. 7 (CDD)	Occasional transactions (where there is no business relationship) of 15,000 euro or over, where there are no significantly higher than usual risk factors present (S.7.10).	Obtain and verify ID documents, data or information (S.8 and Appendix 5). Where appropriate, identify and verify details of the beneficial owner (S7.8)
Reg. 14 (EDD)	This section applies to customers with whom there is a business relationship **and** those doing transactions that fall into the following categories: Non face to face customers (S7.12.2). Politically exposed persons (S.7.12.3).	In addition to obtaining and verifying the ID of the customer, (S.8 and Appendix 5), and, where appropriate, the beneficial owner (S7.8), take risk-based enhanced due diligence measures (S7.12). Where the customer is not physically present for identification purposes, or there is a risk of impersonation fraud, obtain additional evidence of identification and/or apply

	Any other situation which, by its nature can present a higher risk of money laundering or terrorist financing, including where transactions are below 15,000 euro (7.12.4)	supplementary measures to verify the documents supplied (S7.12.1). For non face to face: customers consider undertaking the first transaction through a bank account in the customer's name (S7.12.2). For PEPs: carry out enhanced due diligence as considered appropriate and reasonable, e.g. for occasional transactions (over 15,000 euro), obtain details of the source of funds and purpose of transactions (S7.12).

17. APPENDIX 5: Acceptable evidence of identity

17.1 Private individuals

17.1.1 Standard evidence

This section sets out the standard identification requirements for customers who are private individuals. This is likely to be sufficient for most situations. If, however, the customer or transaction is assessed as presenting a higher money laundering or terrorist financing risk, the business will need to decide whether it should require additional identity information to be provided and increase the level of verification.

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

Businesses may also need to follow this guidance when identifying, and verifying the identity of beneficial owners and any other relevant individuals associated with the relationship or the transaction. Again, however, in situations where there is a higher risk of money laundering or terrorist financing, additional evidence of identification and level of verification will be more appropriate.

The business should obtain the following information from customers who are private individuals:

Full name
Current residential address
Date of birth

Money transmission businesses should be aware that for the purposes of **Regulation EC 1781/2006 on information on the payer accompanying transfers of funds (commonly known as the Payments Regulation or the Wire Transfer Regulation),** for amounts under 15,000 euro evidence of address need not necessarily be obtained if the transmitter opts to hold only the customer's name and unique identification number as the Complete Information on the Payer. Consideration should, nevertheless, be given to obtaining and verifying evidence of the customer's address and possibly other additional information where there is a risk of impersonation fraud. (Where additional information is held for verification purposes, the information sent with the transfer may still be restricted to the name and customer unique identification number.) Guidance on this Regulation can be found in Appendix 8: Money Transmission Businesses.

17.1.2 Verification of identity

Verification of the information obtained must be done using reliable and independent sources. These could be a document or documents provided by the customer, or data accessed electronically, or a combination of both. Where identification is done face-to-face, originals of any documents involved in the verification should be seen.

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

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

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

Either a government issued document which incorporates:

- The customer's full name and photograph, and

  - either his residential address

  - or his date of birth.

Government-issued documents with a photograph include:

Valid passport
Valid photocard driving licence (full or provisional)
National ID card (for non UK nationals)
Firearms certificate or shotgun licence
ID card issued by the electoral office for Northern Ireland

Or a government issued document (without a photograph) which incorporates the customers full name, **supported by** secondary evidence of ID, either government-issued or issued by a judicial authority, a public sector body or authority, a regulated utility company, or another FSA regulated firm in the UK financial services sector, or in a comparable jurisdiction, which incorporates:

- The customers full name, and

  - either his residential address

  - or his date of birth.

Government issued documents without a photograph include:

Valid old style full UK driving licence
Recent evidence of entitlement to a state or local authority-funded benefit, tax credit, pension, educational or other grant

Other documents include:

Instrument of a court appointment
Current council tax demand letter or statement
Current bank or credit/debit card statements (but not ones printed off the internet)
Utility bills (but not ones printed off the internet)

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

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

When accepting evidence of identity from a customer, it is important that the business makes sufficient checks on the evidence provided to satisfy them of the customer's identity, and keeps a record of the checks made.

Checks on photo ID may include:

- Visual likeness against the customer
- Does the date of birth on the evidence match the apparent age of the customer?
- Is the ID valid?
- Is the spelling of names the same as other documents provided by the customer?

Checks on secondary evidence of ID may include:

- Do the addresses match the address given on the photo ID?
- Does the name of the customer match with the name on the photo ID?

Consideration should be given as to whether the documents relied upon may be forged. In addition, if a business chooses to accept documents that are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity.

17.1.3 Electronic verification

If identity is verified electronically, checks should use the customer's full name, address and date of birth as a basis. They can be carried out either directly by the business, or through a commercial agency which meets the criteria in section 8.6 that provide a reasonable assurance that the customer is who he says he is.

Electronic verification should meet a standard level of confirmation before it can be relied upon. In circumstances that do not give rise to suspicion or significant risk of impersonation fraud, the standard level of confirmation is:

- One match on an individuals full name and current address, **and**
- A second match on the full name and **either** his current address **or** his date of birth.

Where the customer is present, businesses may wish to mitigate the risk of impersonation fraud by asking the customer to verify additional information held electronically.

Where the customer is not physically present for identification purposes, additional measures are required to mitigate the risk, which may include obtaining additional evidence of identity and/or supplementary measures to verify the information supplied.

Commercial agencies that provide electronic verification use various methods of displaying results – for example, by the number of documents checked or through scoring mechanisms. **It is important that the business fully understands the system they are using, and are satisfied that the sources of the underlying data meet the standard level of confirmation set out above.**

17.1.4 Customers who cannot provide the standard evidence

Some customers may not be able to produce identification information to meet the standard requirement, e.g. migrant workers, refugees and asylum seekers, dependent spouses/partners or minors. In these cases the business will need an approach that compensates for the difficulties that such customers may face in providing the standard evidence of identity.

Businesses must establish and document why the standard requirements cannot reasonably be applied.

The following table provides examples of documents that provide evidence of identity for some types of financially excluded customers. The list is not exhaustive. A proportionate and risk-based approach will be needed to determine whether the evidence available gives reasonable confidence as to the identity of a customer.

Customer	**Document(s)**
Economic migrants	National Passport, or National Identity Card (nationals of EEA and Switzerland)
Refugees (those that are not on benefit)	Immigration Status Document with Residence Permit, or IND travel document (i.e. *Blue* Convention Travel doc, or *Red* Stateless Persons doc, or *Brown* Certificate of Identity doc)
Asylum seekers	IND Application Registration Card (ARC) N.B. This document shows the status of the individual and does not confirm their identity.

Where a business decides that a customer cannot reasonably meet the standard identification requirement, and the provisions in the table above cannot be met, it may accept as identification evidence a letter or statement from an appropriate person who knows the individual, that indicates that the person is who he says he is.

Some categories of financially excluded customers may represent a higher risk of money laundering. Businesses should consider enhanced monitoring of transactions conducted through such business relationships.

17.1.5 Non face-to-face customers

Non face-to-face customers present an inherent risk of impersonation fraud which businesses should also take account of in their internal policies and procedures. **Regulation 14(2) of the MLR 2007** requires that businesses apply enhanced due diligence measures, on a risk-sensitive basis, when they don't physically meet their customers (see section 7.12).

Therefore, businesses must apply additional verification checks to mitigate the risk of impersonation fraud. These checks may include:

- Requiring additional documents, data or information to verify the customer's identity
- Applying supplementary measures to verify the documents supplied
- Requiring the first transaction to be carried out through an account in the customers name with a UK or EU regulated bank or one from a comparable jurisdiction
- Telephone contact with the customer at a home or business number which has already been verified, using it to verify additional aspects of personal identity information provided during the application process
- Communicating with the customer at an address which has already been verified, for example by letter
- Internet sign-on where the customer uses security codes, tokens, and/or other passwords which have been set up during the application process and provided by mail to the named individual at an independently verified address.

Photocopied identity documents can be accepted as evidence of ID provided that each copy document has an original certification by an appropriate person to confirm that the person is who they claim to be.

An appropriate person is an independent professional person who is not already a friend or relative of the applicant. For example:

- Family GP
- Accountant
- Civil Servant
- Teacher
- Solicitor
- Notary
- Post Office branch employee
- Employer.

In addition to providing a written certification on the copy document to confirm the identification of the applicant, the certifying individual should also provide their business contact details.

17.2 Customers other than private individuals (such as companies, trusts or charities)

17.2.1 General obligations

Customers

Certain information about the entity should be obtained as a standard requirement (see section 17.2.2 below for companies, and the relevant guidance referred to in section 17.2.3 for other entities).

The business should then assess the risks of money laundering or terrorist financing, based on a combination of factors relating to the customer, business relationship, products, services, or transactions involved. The business must then decide the extent to which the identity of the entity should be verified, using reliable, independent source documents, data or information.

Beneficial owners

As part of the standard evidence, the business must know the names of all individual beneficial owners who own or control more than 25% of the assets or voting rights, or who otherwise exert control, even where these interests are held indirectly. Sections 7.8 and 8.2.2 provide more information on beneficial owners.

Following the assessment of the money laundering and terrorist financing risks presented by the customer, the business must also decide what information should be obtained and verified for some of the individuals behind or connected to the customer, for the purpose of being satisfied that it knows who the 'beneficial owners' of the entity are.

There is no specific requirement for the identity of beneficial owners to be verified using an independent source. Businesses may therefore decide, based on risk, when it is appropriate to rely on information provided by their customers, and when they need to obtain or verify information from another source.

Where there are difficulties verifying information provided on beneficial owners, e.g. where the customer is from a jurisdiction where there is no requirement to file information about the persons who own or control a company, businesses should review the information provided by the customer and seek further evidence, where considered necessary. A decision should then be made, based on the information provided on the beneficial owner(s), the rationale for the transactions and the risks involved, as to whether the evidence of identity of the beneficial owner is satisfactory to enable the business relationship to be established or the occasional transaction to be carried out.

17.2.2 Corporate customers

Standard evidence

To the extent consistent with the risk assessment carried out, a business must ensure that it understands the company's legal form, structure and ownership.

The business should obtain the following information as standard in relation to companies:

Full name
Registered number
Registered office in country of incorporation
Business address

And, additionally, for private or unlisted companies:

Names of all directors
Names of beneficial owners who hold or control over 25% of the shares or voting rights or otherwise exercise control over the management of the company (see section 7.8)

Basic verification

The business should verify the identity of the company from:

- Either a search of the relevant company registry
- Or, in the case of a publicly owned and listed company, confirmation of the company's listing on the regulated market
- Or a copy of the company's certificate of incorporation.

The identity of any beneficial owners should be verified in accordance with the guidance in section 17.2.1 above. N.B. the beneficial owner provisions do not apply to companies whose securities are listed on a regulated market.

For UK companies, a registry search will confirm that the company has not been, or is not in the process of being, dissolved, struck off or wound up. For non-UK companies, similar search enquiries should be made through the registry in the country of incorporation. Decisions on the extent of verification should take into account the accessibility and reliability of information from particular jurisdictions.

Additional verification to address identified risk

The standard evidence and basic verification requirements are likely to be sufficient to verify the identity of most corporate customers. If, however, any of the circumstances relating to the customer, products, services or transactions are assessed to present a higher risk of money laundering or terrorist financing, then the business will need to decide what additional information must be obtained in order to be satisfied as to the customer's identity and to enable a thorough and effective risk assessment.

The verification processes for private companies, and for public companies that are not listed on the stock exchange or other regulated market, should take into account the availability of public information on the company.

Verification may include, where appropriate, verifying the identity of one or more of the directors, the beneficial owners, or other representatives of the company by obtaining evidence of name, address and dates of birth in the same way as would be done for a private individual, e.g. the production of a passport.

The business may also need to obtain additional information on the nature of the company's business, the reasons for seeking the product or service, and the source of funds.

A visit to the customer's premises could be useful to verify the information provided on the company's business activities.

Information on identifying risk is provided in section 6 of this guidance and also in each of the sector specific Appendices 6 - 10.

Simplified due diligence for companies listed on a regulated market

Businesses are not required to verify the identity of companies whose securities are listed on a regulated EEA market or equivalent overseas which is subject to specified disclosure obligations. This exemption from the customer due diligence requirements is due to the fact that these companies are publicly owned and generally accountable. The exemption also applies to companies that are majority-owned and consolidated subsidiaries of such companies.

Section 5.3.133 of the JMLSG guidance for FSA regulated firms provides further information on the relevant disclosure obligations.

If the regulated market is located within the EEA there is no requirement to undertake checks on the market itself. If it is outside the EEA, sections 5.3.134 and 5.3.135 of the JMLSG guidance should be followed.

17.2.3 Other legal entities

Further guidance on verifying the identity of a range of non-personal entities is provided in the JMLSG Anti-money laundering guidance. That guidance provides more detailed information concerning:

- Charities, church bodies and places of worship
- Other trusts, foundations and similar entities
- Other firms subject to the MLR 2007
- Partnerships and other unincorporated businesses
- Clubs and societies
- Public sector bodies, governments, state owned companies.

18. APPENDIX 6: Supplementary guidance for High Value Dealers

Please note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance in sections 1 to 12.

18.1 Overview of the sector

The HVD population is disparate, consisting of retailers and wholesalers of goods who accept cash payments equivalent to 15,000 euro or more. Types of HVD include jewellers, car dealers, art dealers and auctioneers. Cash means notes, coins or travellers' cheques in any currency.

18.2 What are the money laundering risks faced by HVDs?

18.2.1 Large cash transactions

Cash is the mainstay of much organised criminal activity. For the criminal, it has the obvious advantage of leaving no discernable audit trail and is their most reliable and flexible method of payment. Cash is also a weakness for criminals. Whilst they hold cash they are more at risk of being traced to the predicate offence. Cash seizure powers also mean they are more at risk of having the money taken away by law enforcement. They will therefore often seek to dispose of cash into high value goods. The objective of the first stage of money laundering, i.e. placement, is to move the criminal cash into the financial system. Money launderers normally want to move funds quickly in order to avoid detection. This is more easily done in large one-off transactions.

18.2.2 High value goods

The purchase of high value goods, paid for in cash, with good portability represents an attractive area for money launderers. Goods purchased with cash that can easily be sold on (even for a loss) for 'clean money' are especially attractive. High value goods are also a useful store of value and may form part of a criminal lifestyle. Goods purchased would generally be luxury items that could be potentially sold on through the black market e.g. jewellery, art, antiques, high performance cars.

18.2.3 Goods that are purchased and subsequently returned

Returning high value goods paid for in cash and obtaining a refund by way of a cheque enables the laundering of the 'dirty money' by exchanging it for a legitimate retailer's cheque.

18.2.4 Customers' behaviour

Risk can be indicated by a customer's behaviour, for example where a customer initially proposes to pay for goods over 15,000 euro value by credit card/cheque and then at the last minute presents cash as the means of payment prior to taking ownership of the goods.

18.3 Managing the risk

Businesses should have a system to record all cash transactions of 15,000 euro or more on their accounting system and make them identifiable.

Businesses must have policies and procedures in place concerning the acceptance of these large transactions to ensure that appropriate risk-assessment, customer due diligence and internal reporting requirements are met.

In order to effectively mitigate and manage the risks inherent in large cash payments, HVDs may wish to consider routing all high value cash transactions through one specialist outlet or branch. This offers the combined benefits of:

- Concentrating risk in one area
- Focusing anti money laundering expertise within a limited number of staff improving effectiveness through greater experience
- Reducing training costs
- Limiting the size of the MLR registration fee.

The Nominated Officer of the business could consider using a 'till alert' so as to alert them to a potential HVD transaction or consider having a policy of only the Nominated Officer or other specified members of staff dealing with HVD transactions.

Cash payment should not be accepted until appropriate enquiries have been made, e.g. concerning the reasons for cash payments, the source of the funds etc.

The identity of couriers, intermediaries, or persons who pay for goods overseas through cash deposit and bank transfer should be established. If such information is not provided and/or the sale becomes suspicious, a report should be made to SOCA and consideration given to refusing the transaction.

Businesses must have systems in place that are capable of identifying where transactions of 15,000 euro or more are split so that smaller cash payments are made to avoid the need for customer identification checks.

18.4 Suspicion indicators

- There are no genuine reasons for paying large sums of money in cash
- The goods purchased, and/or the payment arrangements are not consistent with normal practice for the type of business concerned
- Businesses where the level of cash activity is higher than the underlying business would justify
- The customer is paying in used notes or in small denominations
- The customer is buying from an unusual location in comparison to their location
- The method of delivery is unusual, e.g. a request for immediate delivery, delivery to an address other than the customer's address, or the loading of high volume/bulky goods immediately into the customers own transport
- There are large numbers of Scottish bank notes within the payment
- Cash payment is only mentioned by the customer at the conclusion of the transaction
- Instruction on the form of payment changes suddenly just before the transaction goes through.

In the case of refunds:

- The customer enquires about the business's refund policy
- The customer seeks a refund for spurious reasons
- The customer seeks the repayment in the form of a cheque.

19. APPENDIX 7

Supplementary guidance for Bureaux De Change (referred to as currency exchange offices in the definition of money service business in MLR 2007 Regulation 2(1)).

Please note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance in sections 1 to 12.

19.1 Introduction and sector overview

Bureau De Change operations represent the provision of foreign exchange products to both personal and business customers. It covers a wide range of services from the provision of currency for travel purposes to complex currency dealing operations.

In many instances the Bureau De Change will be selling products on behalf of a product provider, for example travellers' cheques, stored value cards/pre-paid cards. For many firms, operations are based on a relatively low value mass consumer/business basis that normally involves rapid, infrequent, or one-off customer contact for transactions that are well below the requirements for customer due diligence identification checks.

Transactions can be undertaken in a variety of locations including airports, high streets, implants within other organisations such as travel agents, and on a non face-to-face basis, using the internet or telephone.

In this section, Bureau De Change activities do not include money transmission products, which are dealt with in a separate section. However, such products are normally supplied on an agency basis and it is important to ensure that Bureaux establish AML related accountabilities with the product provider and ensure that these are clearly defined and documented.

19.2 What are the money laundering risks faced by Bureaux De Change?

There is a high risk that the proceeds of crime will pass through Bureaux at all stages of the money laundering process. However, many millions of foreign exchange transactions are conducted each month and the likelihood of a particular transaction actually involving the proceeds of crime is very low.

A firm's risk-based approach must be designed to ensure that it places an emphasis within its strategy on deterring, detecting and disclosing in the areas of greatest perceived vulnerability. Firms should target their resources where they feel they will make the most difference in fighting crime.

The provision of currency and the ability to convert currencies is a particular area of risk associated with Bureau De Change activities. Most customers both personal and business will have a legitimate need to convert currency. However, the risk is in failing to identify customers or situations where the level of foreign exchange activity is higher than one would expect from that particular segment of the business or unusual or inconsistent in some other way. In such circumstances there is justification for looking more closely at whether the customer may be laundering money or financing terrorism.

19.2.1 Factors that may increase the money laundering risk

Size of transactions and product types:

- **Cash transactions**: Cash is the mainstay of much organised criminal activity. For the criminal, it has the obvious advantage of leaving no discernible audit trail and is their most reliable and flexible method of payment. Cash is also a weakness for criminals. Whilst they hold cash they are more at risk of being traced to the predicate offence. Cash seizure powers also mean they are more at risk of having the money taken away by law enforcement. The objective of the first stage of money laundering, i.e. placement, is to move the criminal cash into the financial system. They will therefore often seek to exchange cash in one currency for foreign currency (or vice versa). This may involve exchanging small denominations of one currency for large denominations of another currency. This is considered to be the most difficult and risky part of the money laundering cycle for criminals.
- **Speed and size of the transaction**: Money launderers normally want to move funds quickly in order to avoid detection or seizure. This is more easily done in large one-off transactions.
- **Split transactions**: The more sophisticated money launderer will look to split a large transaction into several smaller ones with the intention of avoiding AML related controls. Such splitting can occur within one location, across branches or across organisations. This is known as 'smurfing' – when a number of people who each exchange small amounts of cash. The funds eventually end up back with the criminal.

- **The product is easily transported across jurisdictions** and can easily be transferred to another person without leaving an audit trail. This may be particularly pertinent when a product can be transported to high-risk jurisdictions. Currency smugglers will look to move products into countries with no exchange control and lax AML/CTF legislation.
- **Buy backs and refunds:** Amounts of foreign currency may be presented by launderers for exchange into sterling in cash, draft, travel cheques or other instrument. This could be either an attempt at placement or part of the layering process.
- **Swaps through a third currency:** Amounts of currency could be presented for exchange into a third currency, an example would be dollars are exchanged into euro through sterling, possibly from small denominations into easily transported large notes. This would be part of the layering process.

Customer related:

- The customer operates within a high risk sector. Some money launderers will be proprietors of cash-based businesses such as restaurants, pubs, casinos, taxi firms, beauty salons and amusement arcades. The aim here is to mix 'dirty' money with 'clean' and so muddy the trail
- The customer is operates a Money Service Business
- The customer undertakes transactions that make no commercial sense or do not match the profile of the customer. This also includes significant and unusual changes to a customer's established pattern of behaviour
- The customer is not the beneficial owner of the funds and carries out transactions on behalf of third party or parties

Geographical factors:

- Transactions linked to customers connected with countries that are known to have lax AML controls
- Transactions may also straddle jurisdictions, with funds moving from well regulated countries to those with poor regulatory regimes
- The bureau operates within a geographical area where it has previously identified a higher than average number of potential money laundering cases.

19.2.2 Factors that may reduce the money laundering risk

- The product is funded by an instrument drawn on the client's own account at an EU regulated (or equivalent) financial institution. For example, debit/credit card, cheque, CHAPS payment
- Transactions are conducted for a customer on a regular basis and the client is known to the organisation.

19.3 Managing the risk

To assist in managing the risk of their business being used as a vehicle for money laundering, Bureau De Change operators should develop adequate policy and procedure documents that set out the steps the firm takes to meet the requirements of the Regulations in relation to training, identification and verification procedures, risk assessment and management, the monitoring of business relationships, suspicious activity reporting, internal systems and controls and compliance monitoring and management.

19.4 Identification issues

19.4.1 Industry recommended thresholds

As part of a risk-based approach, it is recommended by industry representatives that foreign exchange businesses should adopt a lower threshold of £5,000.

19.4.2 Evidence of identification

The amount of information to be obtained and the level of verification required should be determined by the business according to the risks presented by the customer, product, delivery channel or geographical location. Factors to be taken into account to form business policy in this area may be based on:

- Method of payment, e.g. cash
- Transaction type, e.g. type of currency
- Source of funds.

19.4.3 Financial exclusion

Each foreign exchange business must establish, through risk assessment of its own business, an approach to dealing with customers who may face difficulties in providing the standard evidence of identity due to financial exclusion issues. Appendix 5 includes guidance on verifying the identity of customers who cannot provide the standard evidence of identity.

19.5 Linked transactions

Businesses must put in place a process to monitor repeat transactions with customers whose identity has been obtained, in order to identify customers who may be attempting to split large transactions into several smaller, less conspicuous amounts, which could indicate 'smurfing' activity (see Glossary for definition). It is deemed good practice to monitor for repeat business over the preceding 90 days from the date of the most recent transaction, using risk indicators and profiles that are appropriate to the business. Unusual or suspicious transactions or patterns of activity should be reported to the Nominated Officer.

19.6 HM Treasury Consolidated List of Financial Sanctions Targets

Bureaux De Change must have regard for the guidance in section 7.14.

To reduce the risk of breaching obligations under financial restrictions regimes, bureaux are likely to focus their resources on areas of their business that carry a greater likelihood of involvement with targets or their agents. Within this approach, bureaux are likely to focus their prevention and detection procedures on higher value transactions rather than the vast majority of transactions that are of very low value with no identification documents being presented or recorded. The risk factors that necessitate a check against the Consolidated List should be documented and relevant staff trained in the appropriate procedures to follow.

Relevant sources of information should be consulted to build up appropriate risk-profiles based on customer types and behaviour and knowledge of locations with high levels of drug or other organised crime or terrorist activity. Information on high risk jurisdictions and locations is available from the Financial Action Task Force website **www.fatf-gafi.org** and other internet sources.

If a check produces a positive match, the transaction must not proceed and a report should be submitted to HM Treasury. The firm may also need to consider whether the firm has an obligation to report to SOCA under PoCA or the Terrorism Act (see section 7.14 for further information).

19.7 Training

In accordance with the guidance in section 11 of this guidance, foreign exchange businesses should undertake to train all relevant staff:

- When appointed to an MSB role
- At least once every two years thereafter.

Each business will assess, as part of its business risk analysis process, if training needs to be given more frequently than stated above. This will be detailed as part of each business' internal policy on training.

19.8 Suspicion indicators

- Businesses where the level of cash activity is higher than the underlying business would justify
- The customer is paying in used notes or in small denominations
- The customer is buying from an unusual location in comparison to their own location
- The customer is happy with a poor rate
- The customer is buying currency that does not fit with what the business knows about the customer's destination.

20. APPENDIX 8: Supplementary guidance for Money Transmission Businesses

Please note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance in sections 1 to 12.

20.1 Overview of the sector

Money Transmission Businesses (MTBs) transfer funds between UK and overseas customers. Such transfers are called remittance transactions. Nearly 30,000 registered premises in the UK carry out remittance transactions for customers. MTBs send about £2.3 billion in remittances from the UK each year. MTBs generally fall into one of two categories: those which focus on smaller value remittances carried out mostly on behalf of migrant workers, and those which remit larger values on behalf of customers involved in specific transactions abroad, such as property purchases.

The structure of MTBs varies: larger companies use a wide network of agents in the UK and abroad, while many smaller companies are family businesses that provide tailored remittance services to a specific country or area.

MTBs carry out most transactions either directly, face-to-face with the customer at the MTB's high street premises, or through agents, although a growing number of transactions are now carried out via the internet.

The 10 most popular countries to which remittances are sent are:

1) Pakistan

2) India

3) Nigeria

4) Bangladesh

5) The Philippines

6) Zimbabwe

7) Sri Lanka

8) Colombia

9) Iran

10) Gambia

20.2 What does the risk-based approach mean for money transmission businesses?

A risk-based approach differs from a 'checklist' type of approach in that it lets businesses decide which areas of their operations pose the greatest risk of money laundering or terrorist financing, and to invest resources accordingly to counter them in the most effective way. Each business is expected to successfully manage its risks of money laundering and terrorist financing, ensuring as far as reasonably possible that it deters, detects and discloses money laundering or terrorist financing activity. Under a risk-based approach, if money laundering does occur, the business must be able to justify that the approach it has taken to managing the risk was reasonable in the circumstances.

The principles and detailed requirements of the risk-based approach are explained in section 6 of this guidance.

20.3 How should the risk-based approach be implemented?

To successfully implement the risk-based approach and comply with the MLR 2007, money transmission businesses must take steps to manage the risk of their business being used as a vehicle for money laundering or terrorist financing.

The first step in applying this approach is to identify and assess the nature and extent of the risks that are to be managed.

The business must then ensure that procedures are put in place that effectively mitigate and manage the risks that have been identified. Customer due diligence measures and ongoing monitoring of business relationships must be applied in a way that is appropriate to the risks identified.

The policies and procedures must be communicated and managed effectively. Relevant staff must be trained to recognise risk and suspicious activity and to respond appropriately to mitigate risk and report suspicious activity. Records must be kept of the customer due diligence checks made and evidence obtained in respect of customer identity and other information on business relationships and occasional transactions.

The business must monitor and evaluate the application of the customer due diligence procedures to ensure that the controls operated are consistent with the policies and processes that have been developed and documented. If the money transmission business decides to depart from any of these processes, the process that is applied should be documented for the transactions, and an explanation should be provided.

On a regular basis, the money transmission business should review its risk-assessment and management policies and procedures and decide whether it needs to update them to take into account any product or business changes, or any money laundering related incidents or knowledge acquired.

A template for a policy statement and risk assessment is provided in Appendix 3, which some businesses may find useful in developing their risk-based approach.

20.4 What are the money laundering risks in the industry?

In general, money transmission businesses are faced with a high risk that they will be used to launder the proceeds of crime or transfer monies that finance terrorism. The risk will vary for each business according to the range and types of products supplied, their customers, delivery channels and geographical destination of funds.

The risk factors can be divided up into a number of categories, as set out below. The list is not exhaustive, and money transmission businesses may be aware of particular factors that apply to their own businesses that are not included here.

20.4.1 Factors that increase risk

- Factors that relate to the product itself, including:

  - High value remittances

  - Cash funding and cash pay-outs.

- The countries in which the product operates may give rise to a higher risk of money laundering because of a generally higher crime rate or likelihood of money laundering or terrorist financing
- Factors that relate to the nature of the business arrangement, including:

- The existence of an agency relationship, where the money transmission business is dependent on an agent for customer contact. The determining factor here is how much communication exists between the money transmission business and the agent

- The level of control or comfort regarding the entity delivering the funds in the receiving country

- Non face-to-face transactions
- New customers with no previous relationship with the money transmission business, looking to undertake larger transactions
- Lack of knowledge regarding the origin or destination of funds
- Lack of a meaningful purpose for the transaction.

20.4.2 Factors that decrease risk

- Factors that relate to the product itself, including:

- The product is designed and mainly used for low value remittances

- Funding from and payment into bank accounts.

- The using of accounts to keep track of customer transactions

- The ability to track linked transactions and identify transaction patterns

- Visibility of transactions conducted at other locations by agents of the same or a related money transmission business

- The ability to freeze transactions after they have been initiated

- The countries in which the product operates are regarded as having a lower risk of crime, money laundering or terrorist financing
- Knowledge of the recipient as well as of the sender of funds
- Factors relating to the nature of the business arrangement, including:

- The money transmission business is a single operation without agent relationships and hence with direct customer contact

- Control or comfort regarding the entity delivering the funds in the receiving country.

- Face-to-face contact with the customer
- An ongoing relationship with the customer
- Knowledge of the origin of funds
- A stated purpose for the transaction, confirmed by the features of the transaction.

20.5 EC Regulation 1781/2006 on information on the payer accompanying transfers of funds (commonly known as the Payments Regulation or the Wire Transfer Regulation)

20.5.1 General Legal Requirements

In addition to the customer due diligence measures that must be applied under the Money Laundering Regulations, money transmission businesses must also comply with the EC Payments/ Wire Transfer Regulation and Transfer of Funds (Information on the Payer) Regulations 2007 (which set out the UK's supervision and enforcement provisions).

Payment service providers (which include MTBs) must ensure that transfers of funds are accompanied by information on the payer.
They must obtain specified information on the payer and verify the information where the amount exceeds 1,000 euro (or the equivalent in sterling) in a single transaction, or a series of transactions that appear to be linked.

The purpose of the Payments/Wire Transfer Regulation is to prevent terrorists and other criminals from using wire transfers for moving their funds and to enable detection of such misuse when it occurs.
It aims to ensure that basic information on the originator of wire transfers (the payer) is immediately available to law enforcement agencies to assist them in detecting and tracing the assets of terrorists or other criminals.

The Regulation applies to all transfers of funds, in any currency, which are sent or received by a payment service provider in the European Community, with certain exceptions, for example, relating to transfers of funds carried out using electronic money amounting to 1,000 euro or less and mobile phones or other digital or IT devices. Full details of the exemptions are set out in Article 3 of
the Regulation.

20.5.2 Definitions

Payment Service Provider

For the purposes of this notice, a payment service provider means a Money Transfer Business.

Payer

The Payer is the customer wishing to carry out a transfer of funds.

Payee

The Payee is the beneficiary of a transfer of funds.

Intermediary Payment Service Provider

An Intermediary Payment Service Provider is a Money Transfer Business who carries out transfers on behalf of the PSP of the Payer.

20.5.3 Obligations on payment service providers (PSPs)

The Regulation sets out the obligations on each type of payment service provider when they are involved in sending or receiving funds.

The PSP for the payer must:

- Obtain complete information on the payer (see section 20.5.4 below) from all customers wanting to conduct a money transfer
- Verify the Complete Payer Information on the basis of documents, data or information from a reliable and independent source where the transaction is over 1,000 euros whether carried out as one operation or in several operations that appear to be linked and together exceed 1,000 euros
- If the payer does not have an account number, allocate the transaction a unique identifier number which allows the transaction to be traced back to the payer
- Keep records of the details of the transaction, including the complete information on the payer, for five years

- If the payment service provider for the payee is situated in the European Community, ensure that the transfer of funds is accompanied by the account number of the payer, or a unique identifier allowing the transaction to be traced back to the payer
- For intra EC transfers, if requested by the PSP of the payee, make available the complete information on the payer, within three working days
- If the payment service provider for the payee is outside the EU, ensure that complete information on the payer is sent to the payment service provider of the payee.

The PSP for the payee must:

- Detect if the complete information on the payer is missing
- In the case of missing or incomplete information on the payer, reject the transfer or ask for the missing information
- Where there is a regular failure to supply the required information on the payer, take steps such as warning letters and deadlines, before either rejecting future transfers from the payment service provider or deciding whether or not to restrict or terminate its business relationship with that payment service provider
- Where information is missing or incomplete, consider whether the transfer of funds, or any related transaction is suspicious, and if so, submit a suspicious activity report (SAR) to the Serious Organised Crime Agency (SOCA)
- Keep records of all such instances detailing the reasons for Complete Information on the Payer not being provided, your decision as to whether or not to carry out future transactions with the PSP and, if appropriate, details of any reports made to SOCA, and
- Keep records of any information received on the payer for five years.

The IPSP must:

- Ensure that all information received on the payer that accompanies a transfer of funds is kept with the transfer.

20.5.4 Complete information on the payer (CIP)

CIP consists of:

- The payer's name
- The payer's full postal address including postcode
- The payer's account number or, where the payer does not have an account number, a unique identifier which allows the transaction to be traced back to the payer.

As an alternative to the address, one of the following may be substituted:

- The payer's date and place of birth or
- The payer's customer identification number or
- The payer's national identity number (e.g. passport number).

Customer's identification number

This is a number that the payment service provider allocates to the payer. It must be capable of providing a link to the transaction and to any verification checks made. The customer identification number and the unique identifier can be one and the same when the transaction is a one-off transaction. For the purposes of this section, 'one-off' means a transaction that is not carried out for a customer with an account.

20.5.5 Questions concerning the sending of complete information on the payer

Q. Who do I send information on the Payer to if the transaction goes through an IPSP?

A. If the IPSP is responsible for arranging the transfer of funds then you should send the complete information on the Payer to that IPSP. (If you do not do this then the payment from the IPSP may be blocked when the payment goes through the banking system.)

Q. Can I send the information on the Payer direct to the PSP of the Payee instead?

A. Yes. You can send the information on the Payer together with Payee details direct to the overseas PSP. However if you do this you should give your IPSP written confirmation of what you are doing as there is a risk that without full information on the Payer the payment may be blocked in the banking system. The IPSP therefore needs to agree to the arrangement as he is taking the risk of delays.

Q. If I am an IPSP do I need to send the information on each Payer to the PSP of the Payee or can I just send details of the PSP that is my customer?

A. Unless you have a written agreement with the PSP who is your customer (see details below) you should send the information on the Payer for each individual transaction to the person paying the money to the Payee.

For example your customer is a PSP who wants to send four separate amounts of money to different Payees in the same city/location. You should obtain information on the Payer for each payment and send that information to the PSP of the payee.

Q. If I am an IPSP and the PSP of the Payer wishes to send information on the Payer direct to the overseas PSP what am I required to do?

A. You must decide if you are content with the arrangement. If not you should insist on receiving the information on the Payer. If you are content you should obtain written confirmation from the PSP that they are sending the information on the Payer direct to the overseas PSP. Record the PSP as the Payer with your transmission.

Q. If as a PSP or IPSP I have sent the information on the Payer to the PSP of the Payee do I also need to send it to my bank/IPSP when I arrange for a payment covering several separate money transmission arrangements?

A. No: the bank/IPSP will regard you as the Payer and will therefore only need your details.

Q. If I am a PSP of a Payer but I do not deal with the PSP of the Payee (for example I have a bank account in the overseas country and instruct my bank to transfer funds to the Payee's account or I use a non-business representative* to withdraw money from my overseas account and distribute it to Payees) to whom do I send the information on the Payer?

A. If there is no overseas PSP you must send the complete information on the Payer to the overseas bank where you are transmitting the payment.

Q. Does the information need to be sent in any particular format?

A. Yes. It needs to be sent in such a way that there is a retrievable record of the information that was sent, when it was sent and to whom. The CPI also needs to be traceable back to the individual transactions to which they relate. Examples may include:

- Copies of emails
- Copies of faxes
- Computer records.

20.5.6 Sanctions for non-compliance

The EC Payments/Wire Transfer Regulation came into effect on the 1 January 2007. The UK's supervision and enforcement provisions are set out in the Transfer of Funds (Information on the Payer) Regulations 2007.

With effect from 15 December 2007, businesses that are found to be non-compliant may be liable to financial penalties or prosecution.

In addition, under the MLR 2007, which came into force on 15 December 2007, HMRC will have powers to cancel the registration of MTBs where they are found to be consistently non-compliant with the Payments Regulation. For more information about HMRC's powers to cancel registrations, please refer to Notice MLR9 *Registration*.

20.6 Verification of identity

20.6.1 General legal requirements

Both the MLR 2007 and EC Regulation 1781/2006 on information on the payer accompanying transfers of funds (Payments Regulation/Wire Transfer Regulation) require verification of customers' identities **'on the basis of documents, data or information obtained from a reliable and independent source'.** The documents, data and information that are necessary to fulfil these requirements are set out in Section 8 and Appendix 5.

MLR 2007 Regulation 7(3) requires that a relevant person must:

(a) determine the extent of customer due diligence measures on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction

(b) be able to demonstrate to his supervisory authority that the extent of the measures is appropriate in view of the risks of money laundering and terrorist financing.

Where there is a higher risk of false identity documents or information, there may be a need to obtain additional evidence of identity. There may also be specific intelligence which throws doubt on a particular piece of evidence. Business's procedures should set out the circumstances when increased evidence is required.

When using electronically sourced evidence to verify identity, businesses must make sure that they have an adequate understanding of the data sources relied on by the external agencies who supply the information. Section 8 contains guidance on the standards and criteria for electronic verification.

Where a business relationship exists and the customer's information and evidence of verification is held in a customer account file, it is not necessary to repeat the verification for each transaction but businesses must have procedures to ensure the documents, data or information held is kept up-to-date **(MLR 2007 Regulation 7(2).**

20.6.2 Alternative means of verification

Appendix 5 sets out the forms of evidence that can be used to verify customers' identities, including in circumstances where customers may be financially excluded and so not able to produce standard documentation, e.g. some refugees and migrant workers.

20.6.3 Beneficial owners

The MLR 2007 require that businesses have procedures in place to enable them to identify where a beneficial owner is involved when establishing a business relationship or carrying out an occasional transaction. This would include identifying the directors and significant shareholders of a company, or the person whose money it was if they had asked another person to make the remittance. Section 7.8 provides further guidance on identifying beneficial owners.

20.6.4 Pooled funds

Sometimes customers will pool their funds and make a single transfer to a destination in order to minimize the overall cost of the remittance.

For occasional transactions of 15,000 euro (or the equivalent in sterling) or more, money transmission businesses must identify the beneficial owners on whose behalf the transaction is being carried out and take risk-based measures to verify their identity. Similarly, risk-based scrutiny of transactions carried out within a business relationship should identify, as appropriate, where such beneficial owners exist.

20.7 Nature and purpose of the business relationship

The purpose of obtaining information on the customer is to build a base-line of knowledge of the customer and his business. Understanding the purpose of the transactions, the source and destination of the remitted funds, and the nature of the customer's business, enables the money transmission business to have some expectation regarding the size and frequency of transactions. The money transmission business can then identify unusual transactions that require scrutiny to decide whether further customer due diligence measures or suspicious activity reporting action is necessary.

Useful information could include:

- The customer's line of business or work
- The purpose of the transactions
- The expected frequency of transactions
- The nature of the payer's relationship with the payee
- Other general circumstances of the customer.

For business customers, further information includes:

- Turnover of the business, its size, and its number of employees
- Length of establishment.

As the nature of this information is likely to change over time, the law requires a process of review and updating of information about the nature and purpose of the relationship where this changes over time.

20.8 Ongoing monitoring of business relationships

Section 9 provides guidance on the requirement for ongoing monitoring of business relationships under MLR 2007 Regulation 8.

The purpose of ongoing monitoring is to identify unusual transactions or changes to the pattern of transactions that may signal suspicious activity.

The focus of ongoing monitoring is therefore on transactions (their value, frequency, destination, purpose etc.) rather than on the identity of the customer, which is unlikely to change once it has been verified.

20.9 Customers who are Money Transmission Businesses

Regulation 13 of MLR 2007 allows simplified due diligence for MSB customers, which means that money transmission businesses are not required to apply the customer due diligence measures concerning verifying the identity of the customer and beneficial owner, or obtaining information on the purpose and intended nature of the business relationship.

However, **businesses must conduct ongoing monitoring of the business relationship**. Section 9 provides further guidance on methods of ongoing monitoring.

For customers that are money transmission businesses, it will be necessary to obtain information that is sufficient to identify the risks that are presented by the customer's operations and to put in place appropriate monitoring arrangements that will trigger scrutiny of any unusual, high-risk or suspicious activity through the customer's account. The policy and procedures that are to be followed for MTB customers should be set out in the policy and risk management documents (see section 6 and Appendix 3).

Ongoing monitoring should be carried out through customer account reviews and transaction monitoring. The number and volume of transactions going through the account of an MSB customer should be monitored and individual transactions scrutinised according to identified risk parameters.

In order to satisfy this requirement, the wholesale MTB should obtain information on the source of funds that is sufficient to identify potential risks of money laundering or terrorist financing. In normal circumstances, basic information, e.g. unique customer numbers and size of individual transactions will be sufficient and it will not be necessary to ask for further information on end customers, or the purpose of individual transactions processed by the MSB customer. However, further enquiries on source of funds and end customer details will be necessary where transactions are unusually large or give rise to suspicions of money laundering or terrorist financing.

20.10 Use of agents

Where a principal MTB transacts with a customer through an agent, the business contracting with the customer is responsible for applying the customer due diligence measures relating to that customer. The principal must therefore ensure that the agent complies with the business's AML/CTF policies and procedures. Section 5.1.3 includes guidance on the controls that are recommended to manage the risks where business is conducted through agents.

20.11 Enhanced Due Diligence

20.11.1 Non face-to-face customers

Guidance on the enhanced due diligence measures that must be applied when the customer is not physically present for identification purposes is in section 7.12.2 and Appendix 5.

20.11.2 Politically Exposed Persons (PEPs)

Businesses must have risk-based procedures in place to determine when a customer who is seeking to enter into a business relationship or carry out an occasional transaction is a politically exposed person, and to apply the enhanced due diligence measures that are specified in **Regulation 14(4) of the MLR 2007**. Further guidance on customer due diligence measures for PEP customers is provided in section 7.12.3

20.11.3 Other higher risk situations

To comply with **Regulations 14(1)(b) and 20(1) of the MLR 2007**, money transmission businesses must have systems and procedures in place to monitor customers and transactions to identify higher-risk situations and to apply enhanced due diligence measures in order to deter and detect suspicious activity.

Section 6.2 gives example of risk indicators.

Section 7.12 gives examples of the types of enhanced due diligence measures that can be applied to mitigate the higher risk of money laundering or terrorist financing.

20.12 Suspicious activity reporting

See section 10 for guidance on reporting suspicious activity under Part 3 of the Proceeds of Crime Act and Part 7 of the Terrorism Act, including examples of circumstances that should arouse suspicion.

20.12.1 Linked transactions

Businesses should put in place a process to monitor repeat transactions from customers whose identity has been obtained, in order to identify customers who may be attempting to split large transactions into several smaller, less conspicuous amounts, which could indicate money laundering or terrorist financing activity. It is deemed good practice for businesses to monitor for repeat transactions that exceed £10,000 in total over the preceding 90 days from the date of the most recent transaction. These transactions should be scrutinised, using risk indicators and profiles that are appropriate to the business. Unusual or suspicious transactions or patterns of activity should be reported to the Nominated Officer and, where considered appropriate, a SAR should be submitted to SOCA.

Money transmission businesses should also be alert to multiple transactions remitted by a number of customers to the same recipient.

20.13 HM Treasury consolidated sanctions list

Money transmitters must have regard for the guidance in section 7.14.

To reduce the risk of breaching obligations under financial restrictions regimes, Money Transmission Businesses are likely to focus their resources on areas of their business that carry a greater likelihood of involvement with targets, or their agents. The risk factors that will necessitate a check against the Consolidated List should be documented and relevant staff trained in the appropriate procedures to follow.

Relevant sources of information should be consulted to build up appropriate risk-profiles based on customer types and behaviour and knowledge of locations with high levels of drug or other organised crime or terrorist activity. Information on high risk jurisdictions and locations is available from the Financial Action Task Force website **www.fatf-gafi.org** and other internet sources.

If a check produces a positive match, the transaction must not proceed and a report should be submitted to HM Treasury. The firm may also need to consider whether the firm has an obligation also to report to SOCA under PoCA or the Terrorism Act.

20.14 Typologies

The money transmission business should be aware of the money laundering and terrorist financing typologies that are relevant to their business. Typologies of general interest to the financial services industry are publicly available (see, for example **www.egmontgroup.org**), and the money transfer industry may in future develop its own sector-specific typologies. Measures should be taken to ensure relevant staff are made aware of relevant money laundering/terrorist financing cases or typology information.

In addition, money transmission businesses with an agent network should ensure that a means for agents to provide feedback on emerging money laundering typologies to the money transmission business is put in place.

20.15 Training

As a minimum, training should be delivered to all senior management, customer-facing staff, and those involved in transaction processing or monitoring.

It is suggested that training for existing staff is carried out at least once every year. New staff should be trained either before or as soon as reasonably possible after they have begun their employment.

A record including the names of staff, the content of the training, and the date, should be kept on file.

The frequency, content and method of training should account of the following:

- The level of knowledge, resources, and needs of those to be trained
- The turnover of staff
- The availability of updates to typologies and data on money laundering, fraud and terrorist financing
- Updates to the law and industry guidance
- The effectiveness of the training and the channels used to deliver it.

APPENDIX 9: Supplementary guidance for cheque encashment businesses (CEBs)

Please note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance in sections 1 to 12.

20.16 Overview of the sector

This section of the guidance provides an overall understanding of the aspects of the money-laundering and terrorist financing problems that could involve the cheque cashing trade and guidance on identifying and mitigating the risks involved.

20.17 What are the money laundering risks faced by Cheque Encashment Businesses?

20.17.1 General

Third party cheque cashers are not normally exposed to large scale money laundering from the most serious crimes such as drug trafficking and robbery, because the flow of cash in a cheque cashing transaction goes in the opposite direction to that required by most money launderers, who need to convert their cash proceeds of crimes. However, cheque cashers must identify and mitigate the risks of their service being used by money launderers seeking to convert or transfer criminal property. The Proceeds of Crime Act has increased the exposure of cheque cashers considerably, since it is impossible to have complete certainty about the legitimacy of any payment.

20.17.2 Sources of cash

A potential risk to a cheque encashment service offered by a Principle through Agents or franchisees lies with the Agents/Franchisees themselves. These members could be operating as a 'shell company' using the cheque cashing business as a means to cleanse monies that are the proceeds of crime. Monies paid out in cheque encashment are reimbursed to the Agent by the Principal, unwittingly assisting the integration of laundered monies.

A money launderer may use a front company to supply cash to other businesses or coerces others into allowing their accounts to be used for this purpose.

20.17.3 Tax evasion

It is a criminal offence to evade tax due from an individual to
HM Revenue & Customs. Tax includes not only Income Tax and Corporation Tax but also VAT and Excise Duty. Tax evasion may be the subject of a money laundering offence. A third party cheque encashment service may be guilty of such an offence if it cashes cheques for customers, knowing or having reasonable ground to suspect that the customer is cashing cheques through their service, to conceal the proceeds from HM Revenue & Customs, i.e. evading tax. However, a third party cheque encashment service may reasonably assume its customers pay tax, which is due, unless there is some reason to suspect otherwise.

20.17.4 Benefit fraud

Cheque cashers may come across indicators of benefit fraud while cashing wage checks. Suspicious activity should be reported to SOCA.

20.17.5 Other types of fraud or theft

The most common risk to the cheque casher is that of deception by the customer. A minority of customers will try any way they can to deceive the cheque casher. Cheques can be stolen, stopped, forged, or altered in many ways.

A signatory for a company cheque book may make cheques payable to an accomplice and then give approval to the cheque encashment company on a telephone call checking entitlement. A further example is where the customer is a director of the company on which the cheque is drawn. The company could be in financial difficulty and the customer is trying to draw funds on the account knowing there is no money available.

Advance Fee Fraud occurs where a customer receives a letter saying they have won the lottery in another country. A cheque is sent which is meant to cover the taxes for the payment, sometimes along with the supposed winnings. The letter suggests that the winner cashes the cheque and then sends the money for the taxes, via another means. The customer is unaware this is a scam and the cheque is usually stolen.

20.18 Managing the risks

20.18.1 Agents/Franchisees

Agent/Franchisees operating on behalf of a Principal should be scrutinised for their suitability to offer a cheque cashing service. In particular, the Principal will want to confirm the financial stability of the persons operating the agency. Agents should be audited to a level commensurate with the nominated MLRO's view of the money laundering risk. During a compliance audit, the Principal will want to make sure the Regulations are being adhered to. Principals must have systems in place which allows them to monitor activity, whereby if an Agent's business suddenly increases or drops the Principal can establish whether there is any cause for concern. If there is, this should be reported to the nominated MLRO.

Principals must be aware of the risks involving the Principle/Agent relationship and make sure that before the Agent/Franchisee is recruited, a thorough vetting process is undertaken. This should involve thorough checking of their credentials, (including the beneficial ownership) of firms intending to conduct business on behalf of the principal.

The legitimacy of the company's funds should also be checked before entering into a contract. This will require sight of a bank statement, set of accounts, and trade references. Credit checks should also be done to ascertain that the business is financially stable. ID must be sought for the person in charge of the Agency/Franchise and this must be held on file with all other documents. Only when these checks have been completed satisfactorily, should an Agent/Franchisee be allowed to operate. Franchisees must be registered as an MSB before trade can begin to operate on behalf of the principal (franchisor).

Risk assessments and due diligence measures must, where appropriate, include the following:

- Where does the Agent/Franchisee purchase their cash?
- Does the Agent/Franchisee purchase any cash from any other business?
- What price is the Agent/Franchisee charged for their cash?
- Is the discount in line with commercial rates?
- Does the cash sold reflect the business's declared turnover?

A normal cheque casher will obtain cash from a bank. Where they obtain cash from other sources, it is important that they can provide an audit trail of the sources. If the cheque casher buys cash in from a retailer or other business they must thoroughly check the credentials of that business.

20.18.2 Cheque Cashing Customers

The cheque cashing industry relies on the thorough checking and researching of all their customers and cheques. Any situation that does not fit with the customer's explanation or transaction history should always be brought to the nominated MLRO's attention by submitting a suspicious activity report. The MLRO will then monitor the account and decide whether a report is to be made to SOCA. Suspicious activity includes any customer or transaction that does not fit into the normal course or pattern of business. Suspicious activity is sometimes difficult to recognise and so it is imperative for businesses and their staff to be aware of the risks and to use judgement, based on everything surrounding the transaction or attempted transaction to determine whether it is suspicious and needs to be reported to the Nominated Officer (or MLRO).

20.19 Identification issues

20.19.1 General

The customer must provide proof of entitlement to the cheque being cashed. This can be provided on paper or details can be given verbally which enable the cheque casher to seek confirmation from the drawer. Fraud regarding ID is prevalent, therefore when checking ID the cheque casher must be vigilant and aware that any piece of ID could be forged.

The majority of cheques a cheque casher will handle are for wages - such customers must have wage slips that follow a pattern and should be of similar amounts. Anything that deviates from a customer's normal pattern of business should be queried and reported if suspicion is aroused.

For small businesses where the cheque is made payable to their business, the cheque casher should require the normal proof of ID of the individual cashing the cheque plus evidence of their 'trading as…' name. This should be a letter from their bank, HM Revenue & Customs, Solicitor, Accountant or VAT Return.

Sole Trader customers who have cheques made payable to their business need to provide proof of ID as above plus complete a declaration to state they are the sole trader and sole signatory to the account and therefore wholly entitled to the cheque.

For partnerships, proof of ID must be produced and documented for all partners.

Limited Companies – Cheques made payable to Limited companies should not be cashed since there is no reason why a limited company's bank account should not receive the funds directly.

20.19.2 Industry recommended thresholds

For commercial reasons, customers wishing to use third party cheque cashing services must prove their identity before a transaction can be processed. Cheque cashers make the assumption that every new customer will become a regular customer and therefore wishes to establish a business relationship. N.B. The industry recommended requirements are above and beyond the minimum insisted upon by HMRC.

20.19.3 Electronic verification

There can be genuine reasons why a customer does not show up electronically. This can often mean they have not lived in one property long enough, or have never been registered as a voter. In cheque cashing, electronic verification should be additional to the ID the customer has provided and should not be relied upon as the sole method of checking ID. A new customer's address should always be checked via use of the voters' roll.

Drawers of cheques whose name is unfamiliar to a cheque casher should be investigated thoroughly. Business name, address and telephone number can be verified by electronic means. Further searches into the list of directors may establish that the customer is not connected to the company on which the cheque is drawn, and may alert the cheque casher as to a drawer's negative credit status.

20.19.4 Overseas customers

Whilst not applying to the normal daily business of the cheque casher, there may be extreme circumstances where an existing customer is out of the country. The cheque casher needs to be certain that the correct person will be in receipt of the cash, and so will require proof of ID and a sound understanding of the reason that a customer cannot be present.

20.19.5 Financial exclusion

Each cheque encashment business must establish, through risk assessment, an approach to dealing with customers who may face difficulties in providing the standard evidence of identity due to financial exclusion issues, for example some asylum seekers or refugees. Appendix 5 includes guidance on verifying the identity of customers who cannot provide the standard evidence of identity.

20.20 Linked transactions

Cheque cashers must have systems in place that enable them to review a customer's cumulative value of cheques cashed. These checks should be made on milestone amounts, e.g. £10,000, and increments of £10,000 thereafter. This review will include consideration of how often cheques are cashed, whether drawers are common or change frequently and whether the frequency and value of cheques matches the customer's explanation for their encashment. Any cause for concern should be reported to the nominated MLRO.

20.21 Training

Cheque cashing companies should re-train their staff throughout the year and will test that their staff are up-to-date and constantly reminded of the importance of the prevention of money laundering. The results of anti money laundering tests, and details of training given, should be put in personnel files.

20.22 Suspicion indicators

- An Agent seems able to financially support a continued increase in business with little or no detriment to his cash flow, though his business on reflection should not be able to support such an increase.
- Fictitious companies may be set up for the purpose of cheque fraud – look out for low and consecutive cheque numbers.
- A number of different people cashing cheques all of which are drawn on the same company, with an unfamiliar company name.
- There will be an indication of benefit fraud where people try to cash their benefit cheques (Job Seekers Allowance) and produce a wages slip as ID or vice-versa where they are cashing their wages cheque and produce paperwork regarding Job Seekers Allowance as ID.
- People wanting to cash their final pay cheque may be trying to cash the cheque in the knowledge this is not the amount they are entitled to - as final pay cheques are more likely to be stopped, or re-issued with a lower amount than the original cheque due to deductions for monies for holiday/sickness, the non-return of uniform, damaged equipment, non-completion of work, etc.

- In some circumstances there may be an indication of fraudulently obtained cheques where a person has a number of cheques drawn on different individuals, rather than company cheques, claiming to have done work for these people. One scam encountered within the cheque encashment industry involved the fraudster requesting monies from elderly individuals to administrate the release of their winnings for a lottery/competition. The elderly individuals were asked to give the fraudster a cheque, which the fraudster then tried to cash.
- A sudden increase in cheque values.
- A customer wants to cash a cheque which was made payable to them weeks earlier - usually cheque cashing customers using a third party cheque cashing service need the cash quickly and therefore an old cheque date could mean the cheque has been stolen or tampered with. The customer could have informed the drawer that the cheque is lost, a replacement may have been provided and cashed elsewhere, and the customer then tries to cash the original cancelled cheque.
- A recently issued chequebook - post containing the chequebook may have been intercepted by a fraudster who then creates ID to replicate the original payee's ID.
- It appears that there has been something added to the cheque after the time of issue, e.g. different handwriting is evident, value digits appear squeezed in.

21. APPENDIX 10: Supplementary guidance for trust or company service providers

Please note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance in sections 1 to 12.

21.1 Overview of the sector

A diverse range of individuals and firms may come under the definition of Trust or Company Service Provider (TCSP) set out in MLR 2007 Regulation 3(10), including:

- Company formation agents
- Providers of registered offices, business addresses, accommodation or correspondence addresses for businesses other than sole proprietors
- Firms providing company director, company secretary or partner services. Individuals or firms providing their services as nominee director, nominee company secretary or nominee shareholder
- Individuals or firms providing their services as director or company secretary in relation to certain firms acting in high risk areas
- Individuals or firms acting as professional trustees unless they relate to certain low risk trusts.

Guidance on the activities that will bring these types of business within the scope of the TCSP definition and the relevant supervisory authorities appointed by the Regulations can be found in Notice MLR9.

The main concern for these sectors is that trusts, companies and some other legal entities can be used to launder the proceeds of crime. The reason for Trust or Company Service Provider businesses being included in the MLR 2007 is that they are involved with these entities and may be in a position of access to information that could indicate or raise suspicion of money laundering or terrorist financing activity.

The MLR 2007 place obligations on businesses in the TCSP sector to obtain information on their clients' identities and business activities, and to have systems in place so that any suspicious activity that could indicate money laundering or terrorist financing is recognised and disclosed to the Serious Organised Crime Agency.

Effective anti-money laundering and terrorist financing systems and records will assist law enforcement agencies during their investigations and also protect businesses from inadvertently becoming involved in money laundering or terrorist financing activity.

21.2 What are the money laundering risks faced by businesses in the TCSP sectors?

The risks fall into two categories:

- The risk that the business might become directly involved in money laundering or terrorist financing, for example through setting up company and trust structures, or handling client money or managing bank accounts; and
- The risk that clients might be involved in money laundering, for example in relation to their possession or use of money or other assets which are the proceeds of criminal activity.

The levels of risk that TCSP businesses are exposed to will vary greatly, depending on the services they provide to their clients. For example, the risks faced by an individual or firm acting as a company director involved in the management of a client's financial affairs will be much higher than for a recruitment agency who has only limited involvement with their client companies that is restricted to administering the appointment of directors.

The appropriate responses to mitigate the risks will therefore also differ greatly. In the first example above, the director would need to identify and assess any risks arising out the client's activities and establish appropriate procedures to monitor the company's transactions so that unusual or suspicious activity is identified. In the case of the recruitment agency, basic knowledge of their client's identity and business activities will be more appropriate. Businesses must decide how much information to obtain from clients in order to identify and assess any risk factors associated with them and mitigate risks arising from their ongoing business relationship with the clients.

21.3 Factors that may increase the risk of money laundering

Client-related

- The client cannot provide sufficient evidence of identity
- Difficulty obtaining details of the beneficial owners for the client
- The client has criminal convictions

- The client is a Politically Exposed Person (see section 7.12.3 for definition and further guidance) who may be at risk of exposure to corruption
- Non face-to-face clients who are not physically present for identification purposes
- The client uses intermediaries who are not subject to adequate AML laws
- The client is in a business with high levels of cash income that could lend itself to money laundering by mixing criminal cash with legitimate takings, such as pubs, restaurants, casinos, taxi firms, beauty salons and amusement arcades
- The client has complex trust or company ownership structures that could be used to hide the identity of the underlying beneficial owners
- The client sets up shell companies with nominee shareholders and/or directors
- The client has companies with capital in the form of bearer shares
- The client does not have up-to-date company accounts.

Service/transaction-related

- Handling the receipt and transmission of money or managing clients' bank accounts
- The client makes large cash deposits or withdrawals
- The client takes cash payments that could be undeclared for tax purposes
- Complex financial transfers or property transactions
- The movement of money across international borders
- Divergence from the type, volume or frequency of transactions expected in the course of the business relationship
- Transactions which are unusual for the type of business.

Geographic areas of operation of the business or clients

- Countries with lax anti-money laundering controls (go to **www.fatf-gafi.org** for information)
- Countries with high levels of organised crime, corruption or from which terrorist organisations are known to operate.

21.4 The Risk-Based Approach

Assessment of the risks inherent in the type of TCSP business services undertaken will enable businesses to determine and implement an appropriate and proportionate risk-based approach to AML/CTF controls.

Relevant people in the business must have a good understanding of the risks of money laundering activity or terrorist financing and be trained in the appropriate action to take to mitigate the risks through customer due diligence measures and ongoing monitoring of transactions.

Businesses must monitor their compliance with the procedures they have put in place.

In order to effectively monitor and manage risk, the risk categorisation of individual clients should be reviewed periodically.

21.5 Customer Due Diligence

21.5.1 Relevant guidance

The customer due diligence measures that are specified in the MLR 2007 are explained more fully in sections 7 and 8 and Appendix 5 of this guidance. This section provides supplementary information on specific issues that may have particularly relevance for TCSPs.

In addition, businesses involved in acting, or arranging for others to act, as trustees should refer to the customer due diligence guidance provided by the Law Society at **www.lawsociety.org.uk** which explains in more detail the identification requirements when the client or its beneficial owners are trusts.

21.5.2 Who must be identified and when?

You must identify:

- The customer, and
- Any beneficial owners

when you establish a business relationship with a client or carry out an ‘occasional transaction’ – i.e. a transaction amounting to 15,000 euro (or the equivalent in sterling) or more, where there is no business relationship established with the client.

The definition of ‘business relationship’ is set out in section 7.9.1.

You must also carry out these identity checks in any circumstances where you suspect money laundering or have doubts about the veracity or adequacy of information previously provided.

21.5.3 When it is not necessary to verify the identity of the client or beneficial owners

One-off transactions below the threshold for customer due diligence

If the product or service is a one-off transaction amounting to less than 15,000 euro, e.g. company formation but no further services are required which would involve establishing an ongoing business relationship with the client, then verification of identity is not necessary unless you suspect money laundering activity.

However, if a customer who has carried out a one-off transaction returns to carry out further transactions, you should consider that you may be entering into a business relationship requiring customer due diligence measures. Section 7.9 provides further information on the definition of a business relationship and what customer due diligence measures are required when establishing a business relationship.

Acting as, or arranging for another person to act as a trustee of an administrative trust during probate.

This activity is outside the scope of MLR 2007 Regulation 3(10)(d).

Simplified due diligence
MLR 2007 Regulation 13 allows simplified due diligence to be applied for certain customers i.e. companies whose securities are listed on a regulated EEA market or equivalent overseas subject to specified disclosure obligations, and financial institutions and public authorities which are subject to the requirements of the EU Money Laundering Directive or are situated in a non-EEA state with equivalent requirements (see section 7.11 for further information).

Under simplified due diligence there is no requirement to apply the customer due diligence measures unless you suspect money laundering activity, in which case customer due diligence checks must be carried out. However, risk-assessment and ongoing monitoring of the business relationship are still required.

Reliance
MLR 2007 Regulation 17 allows you to rely on certain regulated persons, including financial institutions, accountants and lawyers to undertake these checks on your behalf, if they are supervised by specified bodies for compliance with the MLR 2007 in the UK, or subject to equivalent legislation in an EEA or non-EEA state including mandatory professional registration recognised by law and supervision for compliance with requirements equivalent to the EU Money Laundering Directive (see section 7.13 for further information).

Under MLR 2007 Regulation 17, the person you rely on must consent to carrying out the Customer Due Diligence checks on your behalf and agree to provide the relevant records on request. You remain liable for any failures to apply the appropriate checks. You should read section 7.13 and section 12 for further information on reliance and the relevant record-keeping requirements.

21.5.4 Timing of verification of identity

The regulations generally require the verification of the identity of the customer, and, where applicable, the beneficial owner, to take place before the establishment of a business relationship or the carrying out of an occasional transaction. However, the regulations also allow that, if it is necessary not to interrupt the normal conduct of business and there is little risk of money laundering or terrorist financing occurring, then verification may take place during the establishment of the business relationship, provided that it is done as soon as is practicable after contact is first established.

This could apply where it is necessary to carry out transactions or services before evidence of identity is received, for example, where a company formation agent is establishing a business relationship with a new client to form a company and provide ongoing registered office services. As it is not practical to interrupt the initial online company formation process to wait for receipt of copies of identity documentation through the post, the transaction can be carried out, if there is an agreement for the documents to be provided in a reasonable amount of time, and provided there are no factors present that could indicate a significant risk of money laundering activity.

21.5.5 Non-production of documents or information

If evidence of identity is not received within the time limit you have specified, you must not carry out any further transactions with or for the client. You must terminate the business relationship if you are not able to obtain the necessary evidence of identity or other information required for CDD. In these circumstances you

must consider making a disclosure of suspicious activity to SOCA (see section 10). If any client funds are held you should either return them to the client if there are no grounds for a SAR, or seek consent from SOCA to refund the funds if a SAR is to be made.

21.5.6 Meaning of beneficial owner

The definition of beneficial owner is explained in section 7.8.2. In general it means:

- The individual or individuals behind the customer who ultimately own or control the customer or
- Any individual on whose behalf a transaction or activity is being conducted.

N.B. The beneficial owner provisions do not apply to companies that are listed on the stock-exchange or equivalent regulated markets outside the UK.

The meaning of beneficial owner for trusts is more complicated. The legal definitions are set out in section 7.8.5 of this guidance. In addition, section 4.7.6 of the Law Society's AML guidance, available at **www.lawsociety.org.uk** explains the legislation in more detail and provides practical advice on identifying trust beneficial owners.

21.5.7 Determining who to identify

It is important to understand who the clients and beneficial owners are for the purposes of applying customer due diligence measures.

The following scenarios may be of help in determining whose identity must be verified.

Scenario 1*: A client approaches a company formation agent direct to establish a business relationship or carry out an occasional transaction (over 15,000 euro):*

- Obtain and verify the identity of the client (see section 8 and Appendix 5)
- Identify and verify the identity of any beneficial owners in relation to the client, e.g. company shareholders owning or controlling more than 5% (see section 7.8.2 and Appendix 5)
- Identify and verify the identity of any third parties on whose behalf the client is acting.

Scenario 2*: A client is introduced to a company formation agent by a lawyer or accountant. The end client is invoiced for the service:*

- As for scenario 1, however, it may be possible to rely on customer due diligence checks done by the lawyer or accountant, subject to the conditions relating to reliance which are referred to in section 4.2.3 above.

Scenario 3*: A company formation agent establishes a business relationship with a new client who is an accountant or lawyer and arranges company formations, for a third party or parties. The accountant or lawyer is invoiced as the client:*

- Verify the identity of the client (see section 8 and Appendix 5)
- Identify and verify the identity of any beneficial owners of the client; i.e. partners or company shareholders owning or controlling more than 25% of capital, profits or voting rights (see section 7.8.2 and Appendix 5).

It is not necessary to routinely verify the identity of the third party or parties. However, some details about underlying clients and transactions will be required to fulfil the customer due diligence requirements to obtain information on the purpose and intended nature of the business relationship, and to carry out effective risk assessment and ongoing monitoring (see sections 4.2.8 and 4.4 below, and sections 7 and 8 for more information). The information obtained when the business relationship is established should include details of the expected nature and level of business and, where considered appropriate, the sources of funds involved.

Scenario 4*: An individual is appointed as a company director in a company meeting one or more of the criteria set out in MLR9:*

- Obtain and verify the identity of the client company (see section 8 and Appendix 5)
- Identify and verify the identity of any beneficial owners in relation to the client; e.g. company shareholders more than 25% (see section 7.8.2 and Appendix 5).

Scenario 5*: A recruitment agent or employment business arranges the appointment of a director with a client company:*

- Identify and verify the identity of the client in accordance with scenario 4.

It is envisaged that the client whose identity must be verified will, in most scenarios, be the company with whom the director is placed. However, where a candidate is charged a fee for an arrangement service, they will also be a client in respect of whom customer due diligence measures must be taken.

Scenario 6*: A mailbox service provider sets up a new customer account:*

- Obtain and verify the identity of the client in accordance with scenario 1.

Scenario7*: An individual or firm is appointed as a professional trustee:*

- Obtain and verify the identity of the client (see section 8 and Appendix 5)
- Identify and verify the identity of the beneficial owners in relation to the client, i.e.

  - Any individual who is entitled to a specified vested interest in at least 25% of the capital of the trust property

  - The class of persons in whose main interest the trust is set up or operates

  - Any individual who has control over the trust.

See section 7.8.2 and Appendix 5 for further information.

21.5.8 Information on the purpose and intended nature of the business relationship

It is important that you obtain sufficient information at the time you establish a business relationship with a new client to enable you to build an effective risk profile of the client.

The extent of information you should obtain will depend upon the risks associated with the type of customer, the products or services supplied, and the transactions to be carried out.

The nature and level of risk you identify will inform your decisions on the extent of future transaction monitoring that will be required.

See section 7.9 for further information on the definition of business relationships and the customer due diligence measures that are required.

21.6 Ongoing monitoring of business relationships

This is explained in more detail in section 9.

The basic regulatory requirement is that TCSPs must monitor their clients' transactions so as to be in a position to identify and scrutinise unusual and potentially suspicious activity requiring a report to SOCA (see section 10).

Monitoring is applicable to information on the client's transactions to which the TCSP business has access in the normal course of the business relationship. At a basic level, the requirement will be satisfied by relevant persons in the business having sufficient awareness of the money laundering risk factors that are present for particular clients or types of client. However, where the products or services involved, or the client's profile present a higher risk of money laundering, then more formal and regular monitoring arrangements should be put in place and conducted at an appropriately senior level.

Where a customer's transactions or activities are not consistent with their risk-profile, consideration must be given as to whether additional enquiries should be made to address any potential risk. These should include source of funds checks, where considered appropriate, to ensure the customer's activity is consistent with the knowledge and expectations established by the customer due diligence information and risk-assessment.

Records must be kept of the documents and information that are the subject of ongoing monitoring.

21.7 Enhanced due diligence and ongoing monitoring

Enhanced due diligence measures and enhanced ongoing monitoring must be applied in situations of higher risk. Examples of risk indicators in the TCSP sectors are given in section 3 above.

The specific Regulatory requirements in relation to enhanced due diligence and ongoing monitoring are set out in section 7.12.

21.8 Suspicion indicators

Section 10 of this guidance covers the Proceeds of Crime Act requirement to report suspicious activity to SOCA, including the requirements for consent for the return of funds.

The following indicators may be relevant to TCSPs. Depending on the particular circumstances, these factors could result in grounds for suspicion or the need for further scrutiny:

- Attempts to obscure or avoid identifying the beneficial owners

- Unwillingness to disclose the source of funds
- Clients whose owners or directors have a lavish lifestyle that appears to exceed known sources of income
- Frequent changes to shareholders or directors
- Excessive or unnecessary use of nominees
- Unnecessary granting of power of attorney
- The purchase of companies that have no obvious commercial purpose
- Subsidiaries having no apparent purpose
- Companies which continuously make substantial losses
- Uneconomic group structures for tax purposes
- Use of a client account instead of paying for things directly
- Out of the ordinary instructions
- Inexplicable changes to instructions
- Use of bank accounts in several currencies without reason
- Transfers of funds without underlying transactions
- Sales invoice totals exceeding the value of goods
- Clients who appear uninterested in legitimate tax avoidance schemes
- Unusual large cash payments in circumstances where payment would normally be made by cheque, banker's draft etc.
- Clients transferring large sums of money to or from overseas locations with instructions for payment in cash
- Clients paying cash into numerous bank accounts
- Large third party cheques endorsed in favour of the client
- Unexplained transfers of significant sums through several bank accounts.

22. Glossary of terms

Beneficial owner	The individual who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted (see section 7.8).
Businesses	For the purposes of this guidance, businesses means Money Service Businesses, High Value Dealers, and those Trust and Company Service Providers for whom HMRC is the Supervisory Authority in Regulation 23 of MLR 2007. It includes companies, partnerships and sole proprietors.
Business relationship	A business, professional or commercial relationship between a relevant person (i.e. someone to whom the MLR 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.
Cash	Notes, coins or traveller's cheques in any currency.
Consent	Permission given by SOCA, for the carrying out of any action that would constitute a money laundering offence in the absence of that permission (see section 10).
Criminal conduct	Conduct which constitutes an offence in any part of the United Kingdom, or would constitute an offence in any part of the United Kingdom if it occurred there.
Criminal Property	Any money or other assets which constitutes a person's benefit from crime.
Customer due diligence	Identifying and verifying the identity of the customer and any beneficial owner of the customer, and obtaining information on the purpose and intended nature of the business relationship.
EEA	European Economic Area.
Enhanced due diligence	Additional customer due diligence measure that must be applied: • Where the customer has not been physically present for identification purposes • Where the customer is a Politically Exposed Person, or • In any other situation which by its nature can present a higher risk of money laundering or terrorist financing.
FATF	Financial Action Task Force.
Financial institution	Has the meaning given by MLR 2007 Regulation 3(3).
Financial Sanctions Targets List	A consolidated list of targets listed by the United Nations, European Union and United Kingdom under legislation relating to current financial sanctions regimes. It is maintained by the HM Treasury Asset Freezing Unit.
FSA	Financial Services Authority: statutory regulator of most financial services providers under the Financial Services and Markets Act 2000.
High Value Dealer	A firm or sole trader who by way of business trades in goods (including an auctioneer dealing in goods), when he receives, in respect of any transaction, a payment or payments in cash of at least 15,000 euros in total, whether the transaction is executed in a single operation or in several operations which appear to be linked.
Identification	Ascertaining the name of, and other relevant information about, a customer or beneficial owner.
Internal Report	A report made to the Nominated Officer or MLRO in a business.
JMLSG	Joint Money Laundering Steering Group: body representing UK Trade Associations in the Financial Services Industry and aiming to promote good anti-money laundering practices and give relevant practical guidance.
Money laundering	An act which: • constitutes an offence under s 327, 328 or 329 of PoCA or • constitutes an attempt, conspiracy or incitement to commit such an offence or • constitutes aiding, abetting, counselling or procuring the commission of such an offence or • would constitute an offence specified above if done in the United Kingdom. (PoCA, s 340 (11)). A person also commits an offence of money laundering if he enters into or becomes concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property: • by concealment • by removal from the jurisdiction • by transfer to nominees, or • in any other way. (Terrorism Act, s 18).

MLR 2007	The Money Laundering Regulations 2007.
MLRO	Money Laundering Reporting Officer. This term is used to describe the nominated officer appointed under Regulation 20 (2)(d), MLR 2007 and s331, PoCA.
Money service business	An undertaking which by way of business operates a currency exchange office, transmits money (or any representations of monetary value) by any means or which cashes cheques which are made payable to customers.
Supervisory Authority	Bodies identified by MLR 2007 Regulation 23 as being empowered to supervise the compliance of relevant businesses with the 2007 Regulations.
Nominated Officer	A person in a firm or organisation nominated by the firm or organisation to receive disclosures under Regulation 7 and s 330 of PoCA from others within the firm or organisation who know or suspect that a person is engaged in money laundering. Similar provisions apply under the Terrorism Act.
Occasional transaction	A transaction (carried out other than as part of a business relationship) amounting to 15,000 euros or more, whether the transaction is carried out in a single operation or several operations that appear to be linked.
Ongoing monitoring of a business relationship	• Scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the relevant person's knowledge of the customer, his business and risk profile, and • Keeping the documents, data or information obtained for the purpose of applying customer due diligence measures up to date.
PoCA	Proceeds of Crime Act 2002.
Politically Exposed Person	An individual who is or has, at any time in the preceding year, been entrusted with prominent public functions, and an immediate family member, or a known to close associate, of such persons.
Prejudicing an investigation	The making of any disclosure or falsifying, concealing, or destroying, or being complicit in these, of any documents that are relevant to a money laundering investigation.
Regulated Sector	Persons and firms which are subject to the Money Laundering Regulations.
SAR	Suspicious activity report made to SOCA.
Senior management	The directors and senior managers (or equivalent) of a firm who are responsible, either individually or collectively, for management and supervision of the firm's business.
Senior manager	An individual, other than a director (or equivalent), who is employed by the firm, and to whom the Board (or equivalent) or a member of the Board, has given responsibility, either alone or jointly with others, for management and supervision.
Simplified due diligence	An exception to the obligation to apply the customer due diligence measures for specified customers, e.g. financial institutions subject to the Money Laundering Directive or equivalent legislation and supervision. It is also available for some categories of products and transactions which may be provided by financial institutions
'Smurfing'	Banking industry jargon used to describe the act of splitting a large financial transaction into smaller transactions to avoid regulatory controls and scrutiny by law enforcement agencies. Typically, each of these smaller transactions is below the limit for identification checks. Criminal enterprises often send different couriers to a number of money transfer/bureau de change agents to carry out these transactions and the term 'smurfing' originates from an image of the indistinguishable small cartoon characters, the Smurfs.
SOCA	Serious Organised Crime Agency.
Terrorism Act (TA 2000)	Terrorism Act 2000, as amended by the Anti-terrorism, Crime and Security Act 2001.
Terrorist offences	The terrorist offences relate to fundraising, using or possessing terrorist funds, entering into funding arrangements, money laundering, disclosing information relating to the commission of an offence (similar to tipping off), or failing to make a disclosure in the regulated sector. (s 19 and 21A TA 2000 (as amended)).
Terrorist property	• Money or other property which is likely to be used for the purposes of terrorism (including any resources of a proscribed organisation) or • Proceeds of the commission of acts of terrorism, or • Proceeds of acts carried out for the purposes of terrorism. 'Proceeds of an act' includes a reference to any property which wholly or partly, and directly or indirectly, represents the proceeds of the act (including payments or other rewards in connection with its commission). 'Resources' includes any money or other property which is applied or made available, or is to be applied or made available, for use by the organisation (Terrorism Act, s 14).

Tipping off	A tipping-off offence is committed if a person knows or suspects that a disclosure falling under PoCA s 337 or 338 has been made, and he makes a disclosure which is likely to prejudice any investigation which may be conducted following the disclosure under s 337 or s 338. (PoCA, s 333)
Transaction	The provision of any advice by a business or individual to a client by way of business, or the handling of the client's finances by way of business. A transaction could be simply operating across a client's account.
Trust or Company Service Provider	A firm or sole practitioner who by way of business provides any of the following services to other persons - (a) forming companies or other legal persons (b) acting, or arranging for another person to act - (i) as a director or secretary of a company (ii) as a partner of a partnership or (iii) in a similar position in relation to other legal persons (c) providing a registered office, business address, correspondence or administrative address or other related services for a company, partnership or any other legal person or arrangement (d) acting, or arranging for another person to act, as - (i) a trustee of an express trust or similar legal arrangement or (ii) a nominee shareholder for a person other than a company whose securities are listed on a regulated market.
Verification	Verifying the identity of a customer, by reference to reliable, independent source documents, data or information, or of a beneficial owner through carrying out risk-based and adequate measures.

Do you have any comments?

We would be pleased to receive any comments or suggestions you may have about this notice. Please write to:

HM Revenue & Customs
Money Laundering Regulations Team
Ralli Quays
3 Stanley Street
Salford
M60 9LA

Please note this address is **not for general enquiries**. You should ring our advice service about those.

If you have a complaint or suggestion

If you have a complaint please try to resolve it on the spot with our officer. If you are unable to do so, or have a suggestion about how we can improve our service, you should contact one of our Regional Complaints Units. You will find the telephone number under ‘Revenue & Customs' or under 'Customs and Excise' in your local telephone book. Ask for a copy of our factsheet ‘Complaints and putting things right’. You will find further information on our website at **www.hmrc.gov.uk**

If we are unable to resolve your complaint to your satisfaction you can ask the Adjudicator to look into it. The Adjudicator, whose services are free, is a fair and unbiased referee whose recommendations are independent of HM Revenue & Customs.

You can contact the Adjudicator at:

The Adjudicator’s Office
Eighth Floor
Euston Tower
286 Euston Road
London
NW1 3US

Phone: **0300 057 1111**
Fax: **0300 057 1212**
Internet: **www.adjudicatorsoffice.gov.uk**