HM Revenue & Customs

Anti-money laundering guidance for trust or company service providers

MLR8 TCSP

Contents

We have a range of services for people with disabilities, including guidance in Braille, audio and large print. Most of our forms are available in large print. Please contact us on any of our phone helplines if you need these services.

Contacts
Please phone:
the VAT & Excise
Helpline on
0845 010 9000
or go to
www.hmrc.gov.uk

1 Introduction

This guidance is addressed to proprietors, directors, managers, employees and Nominated Officers of Trust or Company Service Providers (TCSPs) who are the subject of the Money Laundering Regulations 2007 (MLR 2007) and for whom HM Revenue & Customs (HMRC) is the supervisory authority.

For further information on the businesses that fall within this sector and the registration requirements and processes, please go to MLR9 *Registration notice*.

Trust or Company Service Providers that are supervised by HMRC should follow this guidance but may also find the Consultative Committee of Accountancy Bodies' (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 6 of this guidance when carrying out those services.

This guidance explains measures brought about by the Money Laundering Regulations 2007, which came into force on 15 December 2007.

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).

This guidance is also in line with other MLR supervisors. HMRC have adopted the principles of good regulation in the Regulators Compliance Code.

1.1 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 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
- provides specific good practice guidance on AML/CTF procedures.

Assists Trust or Company Service Providers 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.

1.2 Status of the guidance

This guidance is 'relevant guidance' which is approved by the Treasury, for the purposes of Money Laundering Regulations 2007 regulations 42(3) and 45(2). 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 Money Laundering Regulations 2007.

It is also 'relevant guidance' for the purposes of the Proceeds of Crime Act (PoCA) 2002 section 330(8), which requires 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 (TA) 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.

1.3 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 Money Laundering Regulations 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, 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

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.

2.2 What is terrorism?

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.

Money laundering and terrorist finance offences are committed however small the amount involved.

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.

2.3 What are sanctions?

Sanctions are normally used by the international community for one or more of the following reasons:

- to encourage a change in behaviour of a target country or regime
- to apply pressure on a target country to comply with set objectives
- as an enforcement tool when international peace and security has been threatened and diplomatic efforts have failed
- to prevent and suppress the financing of terrorists and terrorist acts.

Financial sanctions are normally one element of a package of measures used to achieve one or more of the above. Financial sanctions measures can vary from the comprehensive – prohibiting the transfer of funds to a sanctioned country and freezing the assets of a government, the corporate entities and residents of the target country – to targeted asset freezes on individuals/entities.

3 Money Laundering Regulations 2007: General obligations

3.1 Policies and procedures

Money Laundering Regulations 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
- 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 7.11.3 for definition and further guidance)
- nominate an individual in the organisation to receive disclosures under Part 7 of PoCA and Part 3 of TA 2000
- 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.

3.2 Sanctions for non-compliance

The civil and criminal sanctions for failure to comply with the Money Laundering Regulations 2007 are explained in appendices 1 and 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 Money Laundering Regulations 2007.

Senior management 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.

Senior management must produce adequate AML/CTF risk management policies and risk profiles, including evidence of their policies. Businesses particularly the larger businesses may find it helpful to have written policies in place. 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
- Money Laundering Regulations 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 corporate bodies

Under Money Laundering Regulations 2007 regulation 47, an officer in a corporate body (that is, 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 Money Laundering Regulations 2007 who consents to or is involved in committing offences under the Money Laundering Regulations or the Terrorism Act, or where any such offence is due to any neglect on their part, will be individually liable to prosecution for the offence as well as the corporate body. Partners of partnerships and officers of unincorporated associations covered by the Money Laundering Regulations 2007, are in a similar position. Failure of senior managers to comply with the Money Laundering Regulations 2007 may result in financial penalties or a prison term of up to 2 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 Money Laundering Regulations 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 Money Laundering Regulations 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 controls and communication

5.1 Why are internal controls and communication necessary?

Money Laundering Regulations 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, 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 appendix 6), or to the owner of the business, who is responsible for making a disclosure to Serious Organised Crime Agency (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
- nature, scale and complexity of the business
- type of products, customers, and activities involved
- diversity of operations, including geographical diversity
- volume and size of transactions, and
- distribution channels.

5.1.1 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' 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.

5.1.2 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 Money Laundering Regulations 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 Money Laundering Regulations 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 Money Laundering Regulations 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 Money Laundering Regulations 2007. This can be done by adapting the downloadable HMRC F&P application form, from the MLR website, go to **www.hmrc.gov.uk/mlr/mlr101.pdf**
- conduct commercial investigations, for example, on credit worthiness, on all agents
- conduct a programme of site visits to agents
- undertake transaction monitoring and testing to confirm the business' 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 Money Laundering Regulations 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 Money Laundering Regulations 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.

5.3 HMRC risk based approach to supervision

The appropriate approach in any given case is ultimately a question of judgement by Senior Management in the context of the risks they consider the business faces.

HMRC recognise that a regime that is risk based cannot be a zero failure regime. Therefore, enforcement action by HMRC is very unlikely where a business can demonstrate that it has taken all reasonable steps, exercised all appropriate due diligence and put in place an effective system of controls that identifies and mitigates its money laundering risks.

6 A risk-based approach

6.1 What is a risk-based approach?

Money Laundering Regulations 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, for example, cash over the counter, electronic, wire transfer or cheque
  - geographical areas of operation, for example, 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 and 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, for example, 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 9 includes further information on the risks that may be present within the different business sectors and appropriate controls and countermeasures 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) 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 Task Force website, go to **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 uncommercial 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?

Note 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
- 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.

Money Laundering Regulations 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, for example, 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, for example, 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 Money Laundering Regulation 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 11.

7 Customer due diligence (CDD)

This section sets out and explains the legal definitions and detailed requirements for customer due diligence under Money Laundering Regulations 2007 and Counter-Terrorism Act 2008. A summary of the 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.

7.1 Why is it necessary to apply CDD measures?

The customer due diligence obligations on relevant businesses under the Money Laundering Regulations 2007 and Counter-Terrorism Act 2008 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 PoCA 2002 and the TA 2000 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, their business and risk profile to allow ongoing monitoring of the business relationship to ensure that transactions undertaken are consistent with that knowledge.

7.2 What is customer due diligence?

The meaning and application of customer due diligence is set out in Money Laundering Regulations 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 7.7 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 (for example, on the source of funds and purpose of transactions – see section 7.8 for further guidance).

7.3 When must these due diligence measures be applied?

Customer due diligence measures must be applied:

- when establishing a business relationship (see section 7.8)
- when carrying out an occasional transaction (that is involving 15,000 euro (or the equivalent in any currency) or more - see section 7.9)
- 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.

7.4 Determining the extent of customer due diligence measures

Money Laundering Regulations 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.

7.5 Timing of verification of identity

Under Money Laundering Regulations 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)).

7.6 Non-compliance with customer due diligence measures

Money Laundering Regulations 2007 regulation 11 requires that where a business is unable to comply with the required customer due diligence 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 SOCA (see appendix 6).

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.

7.7 Identifying the beneficial owner

7.7.1 General legal requirements

Money Laundering Regulations 2007 regulation 5(b) requires businesses to identify any beneficial owner of the customer and take risk based and adequate measures to verify their 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.

7.7.2 Who is a beneficial owner?

Money Laundering Regulations 2007 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 (for example, 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.

7.7.3 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. Note 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 & provident societies and some charities (often companies limited by guarantee or incorporated by an Act of Parliament or Royal Charter) are corporate bodies.

7.7.4 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.

7.7.5 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, for example '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 corporate body 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 Money Laundering Regulations 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 (Money Laundering Regulations 2007 regulation 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.

7.7.6 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 corporate body 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.

7.7.7 Other cases — 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 (their principal).

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

7.8.1 What is a business relationship?

A business relationship is defined as a business, professional or commercial relationship between a relevant person (that is, a business regulated under the Money Laundering Regulations 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 Money Laundering Regulations 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, that is, 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.

7.8.2 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.

7.9 Occasional transactions

7.9.1 General legal requirements

Money Laundering Regulations 2007 regulation 7 requires that customer due diligence measures must be applied when a business carries out occasional transactions. As defined in Money Laundering Regulations 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.

7.9.2 Linked transactions

As part of the risk-assessment and management requirements set out in Money Laundering Regulations 2007 regulation 20, businesses must have adequate systems in place to identify transactions 15,000 euro or more 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?

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 (that is, 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 (SAR) to SOCA (see appendix 6).

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 the customer.

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: *A risk-based approach*).

Businesses should refer to the guidance on risk factors and risk management measures 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.

7.10 Simplified due diligence (SDD)

Simplified due diligence is an exception to the obligation to apply the customer due diligence measures set out in Money Laundering Regulations 2007 regulation 5.

Money Laundering Regulations 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 Money Laundering Regulation 2007 Schedule 2 paragraph 2).

Information on the countries that meet the 'equivalent requirements' test for the purposes of Money Laundering Regulation 2007 regulation 13 is available on the websites of HM Treasury, go to **www.hm-treasury.gov.uk** and the Joint Money Laundering Steering Group, go to **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 simplified due diligence applies.

7.11 Enhanced due diligence (EDD)

7.11.1 General legal requirements

Money Laundering Regulations 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 7.11.3).
- In any other situation which by its nature presents a higher risk of money laundering.

With the exception of PEPs, the Money Laundering Regulations 2007 do not specify what these enhanced due diligence measures must comprise. Instead, businesses should consider applying the enhanced due diligence 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.

7.11.2 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.

7.11.3 Politically exposed persons (PEPs)

Under the definition in Money Laundering Regulations 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 (for example, the European Parliament), or
  - iii an international body (for example, the United Nations), 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 Parliament
– 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
– 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 (that is, of 15,000 euro or more) is a politically exposed person. Where there is a risk that such a customer may be a politically exposed person, 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 politically exposed persons. If there is doubt about whether the customer is a politically exposed person, the customer should be treated as high risk.

In deciding whether a person is a known close associate of a politically exposed person 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 politically exposed persons?

Money Laundering Regulations 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.

7.11.4 Other higher risk situations

Money Laundering Regulations 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. See section 6.2 for examples of risk indicators. Businesses 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, HM 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, go to **www.hm-treasury.gov.uk**

7.12 Reliance on third-parties to apply customer due diligence measures

Money Laundering Regulations 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 Money Laundering Regulations 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.

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 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 11 of this guidance provides further information on these record keeping requirements.

Businesses must not rely on any third-party who is bound by confidentiality requirements not to provide details of the identity of the customer or any beneficial owner, as the business needs to know who their customer is in order to comply fully with the Money Laundering Regulations 2007.

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

8 Identity and verification

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.

8.1 Nature and extent of evidence

8.1.1 Customers

Identifying a customer is a two-part process. The business first identifies the customer by obtaining a range of information, 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, for example, 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.

8.1.2 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 5.1 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 and so on, is provided in section 5.2 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 Money Laundering Regulations 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', that is, a profile of checks that have been made, for example by utility providers, phone companies, credit agencies, banks and so on. 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 and so on.
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. Note 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 (for example, 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, for example, 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.
- 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. Money Laundering Regulations 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, their 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' 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. Factors, such as intuition, direct exposure to a customer face-to-face or on the phone, 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

Money Laundering Regulations 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 Staff awareness and training

10.1 General legal obligations

Money Laundering Regulations 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.

10.2 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 Officers/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.

10.3 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 Money Laundering Regulations 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 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, for example, SOCA, FATF.

10.4 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, go to **www.fatf-gafi.org** and the website of SOCA, go to **www.soca.gov.uk**

Training methods and assessment should be determined by the individual business according to the size and complexity of the business according to the size and complexity of the business. Further information on training can be found in appendix 3, paragraph 3.14 on page 38.

11 Record keeping

11.1 General legal requirements

The purpose of Money Laundering Regulations 2007 regulation 19 on record keeping is to require a business to be able to demonstrate its compliance with the Money Laundering Regulations 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.

11.2 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 the business relationships 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 (for example, account files, relevant business correspondence, daily log books, receipts, cheques and so on) 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.

11.3 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 7.12 of this guidance, he must keep the records specified above for 5 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
- 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.

11.4 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 reasonable 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
- 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.

11.5 How long must the customer due diligence records be kept?

Evidence of customer's identity records must be kept for 5 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 5 years beginning on the date on which the transaction is completed.

All other records must be kept for 5 years beginning on the date on which the business relationship ends.

11.6 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.

11.7 Penalties for failure to keep records

Where the record keeping obligations under the Money Laundering Regulations 2007 are not observed, a business or person is open to financial penalties or potentially prosecution including imprisonment for up to 2 years.

Appendix 1: Primary legislation together with offences and civil penalties

1.1 The Terrorism Act 2000 (TA 2000) 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.

1.1.1 The Terrorism Act 2000 Part 3 – Offences

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 Terrorism Act 2000 even if terrorist property has not come into being, for example, under section 15(1) of the Terrorism Act 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' and/or an unlimited fine.

There are also offences in relation to:

- failure to disclose 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 5 years' imprisonment and/or an unlimited fine.

- Tipping off, that is, 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 TA 2000 and PoCA 2002 (Amendment) Regulation 2007). Note this section applies to persons working in a business in the regulated sector.

Conviction for this offence can incur up to 2 years' imprisonment and or/an unlimited fine

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

PoCA:

- Applies to Money Service Businesses.
- 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 2002.
- Establishes the Assets Recovery Agency (merged with the SOCA)with power to investigate whether a person holds criminal assets, and if so, their location.
- Creates five investigative powers for law enforcement.

1.2.1 The Proceeds of Crime Act 2002 Part 7 – Offences

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 PoCA. The main three offences are:

1 Concealing, disguising, converting, transferring and/or removing from the UK criminal property: 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 Trust or Company Service Providers. This includes all individuals, at whatever level (employee, manager, director and so on) of Trust or Company Service Providers. 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 appendix 6, section 6.2 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 5 years' imprisonment and/or an unlimited fine.

The final offence in Part 7 of PoCA is:

6 Tipping off, that is, 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 TA 2000 and PoCA 2002 (Amendment) Regulation 2007). Note: 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 5 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 5 years' 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, counselling or procuring an offence under sections 327-329 of PoCA.

Appendix 2: Secondary legislation together with offences and civil penalties

2.1 The Money Laundering Regulations 2007 (MLR 2007)

These regulations:

- require firms to take measures to identify 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 our Registration Guides.

2.1.1 Criminal offences

Money Laundering Regulations 2007 regulation 45 sets out the offence of failing to comply with the Money Laundering Regulations 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 Money Laundering Regulations 2007 can incur up to 2 years' imprisonment and/or an unlimited fine.

2.2.2 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
- appeal directly to an independent tribunal.

Appendix 3: Template for policy statement and risk assessment

3.1 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.

3.2 Risk assessment

Date of risk assessment.

3.3 Customer profile

Include relevant customer profile information, for example, number/percentage age of customers:

- In a business relationship (see section 7.8.1).
- 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 7.11.3).
- General description of unusual types of customer and purpose of transactions, for example, regular small amounts of money sent to family overseas.
- Any significant customers outside the normal customer profiles?
- What is the value or percentage age of cash transactions?

3.4 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 on page 56 for definition).
- Remittance of funds to countries with high levels of organised crime or drug production/distribution.
- Making funds available to persons designated 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 increase the risk of impersonation fraud.
- Transmission of money from or to individuals, organisations or locations that may be linked to terrorist activity.

3.5 Risk factors and response

Risk factors should be assessed in relation to:

- customers – types and behaviour
- products and services
- delivery channels, for example, cash over the counter, electronic, wire transfer or cheque
- geographical areas of operation, for example, 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, that is, 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 list below includes examples of the types of risk factors that may be relevant.
Note this list is not exhaustive, businesses will need to add any other relevant risk factors.

Risk factors – 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 7.11.3)
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
Risk factors – product/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
Risk factors – delivery channels
Large cash transactions
Occasional or one-off transactions as opposed to business relationships
Risk factors – 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.

3.6 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?
- Attach or refer to relevant employee instructions.

3.7 Customer due diligence: Business relationships

3.7.1 Customer due diligence when establishing a business relationship

Explain the business' 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.

3.8 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 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 7.11.3), is senior management approval obtained before establishing a business relationship?

Attach or refer to relevant internal guidance and procedural instructions.

3.9 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 (see list below):

Date risk assessment reviewed
Change made (for example, new product, new risk factor or change in status to significant or high)
Comments (for example, sudden jump in sales, change to customer profile)

3.10 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' policies or procedures, for example, risk alerts.

Attach or refer to relevant internal guidance and procedural instructions.

3.11 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.

3.12 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.

3.13 Record keeping

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

Attach or refer to relevant internal guidance and procedural instructions.

3.14 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.

Appendix 4: Summary of customer due diligence and ongoing monitoring

A full explanation of the customer due diligence (CDD) and enhanced customer due diligence (ECDD) requirements is provided in section 7. Further guidance on identification and verification is provided in section 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, for example, cash over the counter, electronic, wire transfer or cheque
- geographical locations, for example, source or destination of funds or goods.

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

Money Laundering Regulations 2007	**Type of customer activity**	**Customer due diligence and ongoing monitoring required**
Regulation 7 (CDD)	Establishing a business relationship (section 7.8.1).	Obtain and verify ID documents, data or information (section 8 and appendix 5). Where appropriate, identify and verify details of the beneficial owner (section 7.7). Obtain information on the purpose and intended nature of the business relationship (section 7.8).
Regulation 8 (OM)	Transactions undertaken throughout the course of a business relationship.	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 (section 9).
Regulation 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) (section 7.9).	Obtain and verify ID documents, data or information (section 8 and appendix 5). Where appropriate, identify and verify details of the beneficial owner (section 7.7).
Regulation 14 (EDD)	This applies to customers with whom there is a business relationship and those doing occasional transactions that fall into the following categories: Non face-to-face customers (section 7.11.2). Politically exposed persons (section 7.11.3). 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 (section 7.11.4).	In addition to obtaining and verifying the ID of the customer (section 8 and appendix 5), and where appropriate, the beneficial owner (section 7.7), take risk-based enhanced due diligence measures (section 7.11). 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 supplementary measures to verify the documents supplied (section 7.11.1). For non face-to-face customers consider undertaking the first transaction through a bank account in the customer's name (section 7.11.2). For PEPs carry out enhanced due diligence as considered appropriate and reasonable, for example, obtain details of the source of funds and purpose of funds and purpose of transactions (section 7.11).

Appendix 5: Acceptable evidence of identity

5.1 Private individuals

5.1.1 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.

5.1.2 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 their residential address
  - or their date of birth.

Government-issued documents with a photograph include:

- Valid passport.
- Valid photo card 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 customer's 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 their residential address
  - or their 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 their home address, a record of this visit may constitute evidence corroborating that the individual lives at this address (that is, 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.

Businesses will need to be vigilant, when accepting government issued documents, for forged or counterfeit documentation. Whilst there is no specific guidance on how to recognise genuine documents, the following indicators may assist businesses in identifying a document that may be false. Note this list is not exhaustive.

- Fuzzy, unclear letters or numbers – in particular, the name, date of birth, expiry date on the presented ID.
- Bumpy, rough or uneven surface texture over the information.
- Tattered edges or any other evidence which might suggest the laminated surface has been tampered with.
- Tattered or uneven edges around the photograph.
- Lack of holographic, fine picture or watermark detail.
- Does the information on the card match the details given to the business by the customer?
- Has the documentation expired?

Any of the above could be indicators that the identity documentation presented may not be genuine. In this case, businesses should make further enquiries on the customer and ask for further evidence of their identity. Where further documentation is provided businesses should check for information consistencies.

5.1.3 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 individual's full name and current address, and
- a second match on the full name and either their current address or their 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.

5.1.4 Customers who cannot provide the standard evidence

Some customers may not be able to produce identification information to meet the standard requirement, for example, 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	Documents
Economic migrants	• National passport, or • National Identity Card (nationals of EEA and Switzerland).
Refugees (those who are not on benefit)	• (Immigration Status Document with Residence Permit, or • IND travel document (that is, Blue Convention Travel document, or • Red Stateless Persons document, or • Brown Certificate of Identity document).
Asylum seekers	IND Application Registration Card (ARC). Note: 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.

5.1.5 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 Money Laundering Regulations 2007 requires that businesses apply enhanced due diligence measures, on a risk-sensitive basis, when they don't physically meet their customers (see section 7.11).

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
- phone 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.

5.2 Customers other than private individuals (such as companies)

5.2.1 General obligations

Customers

Certain information about the entity should be obtained as a standard requirement (see section 5.2.2 aside for companies, and the relevant guidance referred to in section 5.2.3 on page 44 for other entities).

The business should then assess the risk 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 7.7.2 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, for example, 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.

5.2.2 Corporate customers

Standard evidence

To the extent consistent with the risk assessment carried out a business should 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 7.7).

Basic verification

The business should verify the identity of the corporate entity from:
- either a search of the relevant company registry, or
- in the case of a publicly owned and limited 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 5.2.1 above. Note the beneficial owner provisions do not apply to companies whose securities are listed on the 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, for example, 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 the sector specific appendix 8.

Simplified due diligence for companies listed on the 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.

5.2.3 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 for FSA regulated firms. 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 Money Laundering Regulations 2007.
- Partnerships and other unincorporated businesses.
- Clubs and societies.
- Public sector bodies, governments, state-owned companies.

Appendix 6: Suspicious activity reporting to the Serious Organised Crime Agency (SOCA)

6.1 Who is the Serious Organised Crime Agency (SOCA)?

The Serious Organised Crime Agency (SOCA) is an Executive Non-Departmental public body sponsored by, but operationally independent of the Home Office.

SOCA is an intelligence led agency with law enforcement powers and harm reduction responsibilities. Harm in this context is the damage caused to people and communities by serious organised crime.

6.2 General legal and regulatory obligations

Under Part 7 of the Proceeds of Crime Act (PoCA) and Part 3 of the Terrorism Act (TA), 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.

Money Laundering Regulations 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 (NO) who is responsible for receiving disclosures of information concerning suspicions of money laundering, made under the requirements of Part 7 of PoCA 2002 and Part 3 of the TA 2000
- 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 TA 2000.

The failure of any person to disclose such information is an offence under Part 7 of the PoCA or Part 3 of TA 2000.

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

For the purposes of the PoCA and the TA 2000 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, Money Laundering Regulations 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 terrorism 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.

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

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

The preferred means of making a report to SOCA is electronically through the SARS online system, go to **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.

6.5 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.

6.6 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.

6.7 Consent under PoCA

Where a customer's transaction 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 phone to respond to requests for consent.

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 has not 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.

6.8 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 Act 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
- details of their transactions or activities will be/have been reported to SOCA
- 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.

6.9 Suspicion indicators

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

6.9.1 New customers and occasional or 'one-off' transactions

- Checking identity is proving difficult.
- The customer is reluctant to provide details of their identity.
- 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.

6.9.2 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.

6.9.3 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.

6.9.4 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.

Appendix 7: Financial sanctions maintained by HM Treasury Asset Freezing Unit

7.1 Financial sanctions

A consolidated list of financial sanctions targets for example, individuals and entities designated as being subject to financial sanctions is available on the HM Treasury website. This list can be found at **www.hm-treasury.gov.uk/fin_sanctions_index** Please note, it does not contain firms subject to restrictions imposed by Treasury directions issued under Schedule 7 to the Counter-Terrorism Act. The requirements for compliance with firms subject to directions are distinct from those subject to sanctions.

The consolidated list includes targets listed by the United Nations, European Union and United Kingdom under legislation relating to current financial sanctions regimes. It is a criminal offence to make funds or economic resources, and in the case of Terrorism Orders financial services, available, directly or indirectly to or for the benefit of these targets. There is no tipping off offence where a firm refuses to carry out a transaction where they have reason to believe it is for a target on this list, as targets are aware of any restrictions imposed against them.

7.2 Who is responsible for sanctions policy in the UK?

The Foreign and Commonwealth Office (FCO) is responsible for overall policy on international sanctions. HM Treasury is responsible for the implementation and administration of financial sanctions in the UK, for domestic designation (under the Terrorism Order) for licensing exemptions to financial sanctions.

7.3 Asset Freezing prohibitions

7.3.1 General legal requirements

Financial sanctions in the UK can come from three sources:
- UN Resolutions.
- EU Regulations.
- HM Treasury (for domestic only freezes).

Asset freezes in the UK may be imposed by UK Statutory Instruments or directly applicable EU Regulations.

Financial sanctions in the UK are governed by various pieces of legislation. In all circumstances where an asset freeze is imposed, it is a criminal offence for a person to deal with the funds of a designated person, make funds available, directly or indirectly, to a designated person, or to make funds available to another person for the designated person's benefit without doing so under the authority of a licence issued by HM Treasury.

A list of financial sanctions currently in force in the UK is maintained by the HM 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, go to **www.hm-treasury.gov.uk/fin sanctions_index** Further information on financial sanctions can also be found via this website.

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

Under the relevant legislation it is a criminal offence for any natural or legal person to:
- deal with the funds of designated persons
- make funds, economic resources or financial services available to designated persons, or
- participate knowingly and intentionally in activities the object or effect of which is (directly or indirectly) to circumvent a prohibition or enable or facilitate the contravention of any such prohibition.

'Natural person' means an individual or sole proprietor.
'Legal person' means a trustee, limited company or partnership.

'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 these financial sanctions is 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 sanctions. Licence requests to revoke the financial sanctions in relation to a designated person are considered by HM 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 shown at paragraph 7.3.2 below.

7.3.2 Action by relevant businesses

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

For manual checking, businesses can register with the Asset Freezing Unit email notification subscription service.
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: **AFU@hmtreasury.gsi.gov.uk**

In the event that a customer is identified as a designated individual following receipt of money, for example, 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 sanctions. 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 PoCA 2002 or TA 2000.

Further guidance on reporting to SOCA can be found in appendix 6 of this guidance.

Written reports can also be made to:

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

7.3.3 HM Treasury action against breaches of financial sanctions

There are criminal penalties which apply in relation to breaches of the financial sanctions. However, in line with the principles set out in the Code for Crown Prosecutors, prosecution of a firm suspected to be in breach of the financial sanctions regimes 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.

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

Appendix 8: Supplementary Guidance Trust or Company Service Providers

Please note this specific guidance must be read in conjunction with the main guidance in sections 1-11 and appendix 7.

8.1 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 Money Laundering Regulations 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 Trust or Company Service Providers' definition and the relevant supervisory authorities appointed by the regulations can be found in the MLR9 *Registration notice*.

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 Money Laundering Regulations 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 Money Laundering Regulations 2007 place obligations on businesses in the Trust or Company Service Provider 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 (SOCA).

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.

8.2 What are the money laundering risks faced by businesses in the TCSP sector?

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 Trust or Company Service Providers 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 identity and assess any risks arising out of 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.

8.3 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 7.11.3 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 anti-money laundering (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 intended 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, for more information, go to **www.fatf-gafi.org**
- Countries with high levels of organised crime, corruption or from which terrorist organisations are known to operate.

8.4 The risk-based approach

Assessment of the risks inherent in the type of Trust or Company Service Providers business services undertaken will enable businesses to determine and implement an appropriate and proportionate risk-based approach to Anti Money Laundering/Combating Terrorism Financing 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 the risk, the risk categorisation of individual clients should be reviewed periodically.

8.5 Customer due diligence

8.5.1 Relevant guidance

The customer due diligence measures that are specified in the Money Laundering Regulations 2007, including the requirements for verification of identity, 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 particular relevance for Trust or Company Service Providers.

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**, go to **www.lawsociety.org.uk** which explains in more detail the identification requirements when the client or its beneficial owners are trusts.

8.5.2 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' – in other words, a transaction amounting to 15,000 euro (or the equivalent in any currency) or more, where there is no established business relationship with the client.

The definition of 'business relationship' is set out in section 7.8.1.

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.

8.5.3 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, for example, company formation but no further services are required which would involve 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 7.10 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 Money Laundering Regulations 2007 regulation 3(10)(d).

Simplified due diligence

Money Laundering Regulations 2007 regulation 13 allows simplified due diligence to be applied for certain customers that is, 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

Money Laundering Regulations 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 Money Laundering Regulations 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 7.12 for further information).

Under Money Laundering Regulations 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 your request. You remain liable for any failures to apply appropriate checks. You should read section 7.12 and section 11 for further information on reliance and relevant record keeping requirements.

8.5.4 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 it 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.

8.5.5 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 appendix 6). 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.

8.5.6 Meaning of beneficial owner

The definition of beneficial owner is explained in section 7.7.2. 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.

Note 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 7.7.5 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.

8.5.7 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; for example, company shareholders more than 25% (see section 7.7.2 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 restrictions set out in section 8.5.3 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 third-party or parties. The accountant or lawyer is invoiced as the client.	• Verify the identify of the client (see section 8 and appendix 5). • Identify and verify the identity of any beneficial owners in relation to the client; for example, company shareholders more than 25% (see section 7.7.2 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 7 and 9 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 *Registration notice*	• 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; for example, company shareholders more than 25% (see section 7.7.2 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.
Scenario 7	
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, in other words – any individual who is entitled to a specified vested interest in at least 25% of the capital of the trust company – the class of person whose main interest the trust is set up or operates – any individual who has control over the trust.

See section 7.7.2 and appendix 5 for further information.

8.5.8 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 monitoring that will be required.

See section 7.8 for further information on the definition of business relationships and the customer due diligence measures that are required.

8.6 Ongoing monitoring of business relationships

This is explained in more detail in section 9.

The basic regulatory requirement is that Trust or Company Service Providers 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 appendix 6).

Monitoring is applicable to information on the client's transactions to which the Trust or Company Service Provider 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 any 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.

8.7 Enhanced due diligence

Enhanced due diligence measures and enhanced ongoing monitoring must be applied in situations of higher risk. Examples of risk indicators in the Trust or Company Service Providers sector are provided in paragraph 8.8 aside.

The specific regulatory requirements in relation to enhanced due diligence and ongoing monitoring are set out in section 7.11.

8.8 Suspicion indicators

Appendix 6 in the main guidance covers the PoCA requirement to report suspicious activity to SOCA including the requirements for consent for the return of funds.

The following indicators shown in the table below may be relevant to Trust or Company Service Providers. Depending on the particular circumstances these factors could result in grounds for suspicion or the need for further scrutiny.

Suspicion indicators
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 continously make substantial losses
Uneconomic group structures for tax purposes
Use of 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 and so on
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

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 7.7).

Businesses

For the purposes of this guidance, businesses means, those Trust and Company Service Providers for whom HMRC is the Supervisory Authority in regulation 23 of Money Laundering Regulations 2007. It includes companies, partnerships and sole proprietors.

Business relationship

A business, professional or commercial relationship between a relevant person (that is, someone to whom the Money Laundering Regulations 2007 apply) and a customer, which is expected by the relevant person, at the time when the contact is established, to have an element of duration.

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
- the customer is a politically exposed person.

FATF

Financial Action Task Force.

Financial Institution

Has the meaning given by Money Laundering Regulations 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 HM Treasury Asset Freezing Unit.

FSA

Financial Services Authority: statutory regulator of most financial services providers under the Financial Services and Markets Act 2000.

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 section 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, section 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, section 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), Money Laundering Regulations 2007 and section 331, PoCA.

Nominated Officer

A person in a firm or organisation nominated by the firm or organisation to receive disclosures under regulation 7 and section 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 euro 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.
- 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 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 2007.

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, for example, 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.

Supervisory Authority

Bodies identified by Money Laundering Regulations 2007 regulation 23 as being empowered to supervise the compliance of relevant businesses with the 2007 regulations.

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 (sections 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, section 14].

Tipping off

A tipping off offence is committed if a person knows or suspects that a disclosure falling under PoCA section 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 section 337 or 338.

[PoCA, section 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

Checking the identity of a customer or beneficial owner by reference to independent source documents, data or information.

Further information

Contacts
Please phone:
the VAT & Excise
Helpline on
0845 010 9000
or go to
www.hmrc.gov.uk

Your Charter

Your Charter explains what you can expect from us and what we expect from you. For further information please go to **www.hmrc.gov.uk**

How we use your information

HM Revenue & Customs is a Data Controller under the Data Protection Act 1998. We hold information for the purposes specified in our notification to the Information Commissioner, including the assessment and collection of tax and duties, the payment of benefits and the prevention and detection of crime, and may use this information for any of them.

We may get information about you from others, or we may give information to them. If we do, it will only be as the law permits to:

- check the accuracy of information
- prevent or detect crime
- protect public funds.

We may check information we receive about you with what is already in our records. This can include information provided by you, as well as by others, such as other government departments or agencies and overseas tax and customs authorities. We will not give information to anyone outside HM Revenue & Customs unless the law permits us to do so. For more information go to **www.hmrc.gov.uk** and look for Data Protection Act within the Search facility.

Do you have any comments?

We would be pleased to receive any comments or suggestions you may have about this guidance. 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.

If you have a complaint

If you are unhappy with our service, please contact the person or office you have been dealing with. They will try to put things right. If you are still unhappy, they will tell you have to complain. Our factsheet C/FS *Complaints*, also tells you how to make a complaint. You can get a copy of this from our website. Go to **www.hmrc.gov.uk** and look for *C/FS* within the search facility or under the *quick links* menu select *Complaints & Appeals*.

These notes are for guidance only and reflect the position at the time of writing. They do not affect the right of appeal. Any subsequent amendments to these notes can be found at **www.hmrc.gov.uk**

Customer Information Team
July 2010
HMRC 07/10

HM Revenue & Customs