HM Revenue & Customs

Anti-money laundering guidance for money service businesses

MLR8 MSB

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 for proprietors, directors, managers, employees and Nominated Officers of Money Service Businesses who are the subject of the Money Laundering Regulations 2007 and for whom HM Revenue & Customs (HMRC) is the supervisory authority.

For further information on the registration requirements of businesses that fall within this sector, refer to MLR9 *Registration notice*.

Businesses should be aware that their registration details as a Money Service Business may be accessed by people wanting to check that the business is registered by HMRC, using the Money Service Business register which can be accessed from the HMRC website.

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

It 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 and HMRC's supervisory regime are in line with the principles of good regulation in the Regulators' Compliance Code and has been drawn up in consultation with other MLR supervisors.

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 provides guidance on complying with directions issued by HM Treasury under Schedule 7 to the Counter-Terrorism Act 2008 and financial sanctions legislation.

In addition this guidance includes industry sector specific guidance for:
- bureau de change
- money transmission businesses, and
- cheque encashment businesses.

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 Money Service Businesses in designing and putting in place the systems and controls necessary to lower the risk of their business being used by criminals to launder money or finance terrorism
- outlines the legislation in Schedule 7 to the Counter-Terrorism Act
- explains the requirements of Schedule 7 to the Counter-Terrorism Act in relation to Money Service Businesses and how these should be applied in practice
- explains the link between these requirements and those under the Money Laundering Regulations 2007 and,
- explains the link between Money Laundering Regulations 2007, and EU Regulation number 1781/2006 concerning information on the payer accompanying transfers of funds and the Transfer of Funds Regulations 2007.

1.2 Status of the guidance

This guidance is 'relevant guidance' which is approved by HM Treasury, for the purposes of Money Laundering Regulations 2007 regulations 42(3) and 45(2), the Transfer of Funds (Information on the Payer) Regulations 2007, and Schedule 7 to the Counter-Terrorism Act. 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 or the EC Wire Transfer/Payments Regulation or a Direction issued by HM Treasury under Schedule 7 to the Counter-Terrorism Act.

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 TA 2000 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 the Money Laundering Regulations 2007 the EC Wire Transfer/Payments Regulation and Counter-Terrorism Act
- 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 and the Counter-Terrorism Act
- the sanctions for failure to comply with the Money Laundering Regulations 2007 and/or the Counter-Terrorism Act
- business sector specific material, which has been prepared principally by practitioners in the relevant sectors
- information about directions issued by HM Treasury under Schedule 7 to the Counter-Terrorism Act and what Money Service Businesses will have to do once a direction has been issued.

2 Background

2.1 What is money laundering?

Money laundering is the process by which criminally obtained money and 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.

For the purposes of this guidance, references to terrorist financing includes proliferation financing which is assisting in the financing and/or development of nuclear, biological, radiological, chemical weapons and/or their means of delivery.

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 is a direction issued under Schedule 7 to the Counter-Terrorism Act 2008 (a 'direction')?

A direction contains legal requirements imposed by HM Treasury on UK financial and credit institutions in relation to their transactions or business relationships with:

- a person carrying on business in a country
- the government of a country
- a person resident or incorporated in a country.

Money Service Businesses are financial institutions for the purposes of the act.

The requirements may be imposed on particular businesses in the financial sector, a category of business, or all businesses in the financial sector.
HM Treasury may give a direction if one or more of the following apply:

- The Financial Action Task Force (FATF) has advised that measures should be taken in relation to the country because of the risk of terrorist financing or money laundering activities.
- HM Treasury reasonably believe that there is a risk of terrorist financing or money laundering activities and that this poses a significant risk to the national interests of the UK.
- HM Treasury reasonably believe that a country is involved in developing nuclear, radiological, biological or chemical weapons and that this poses a significant risk to the national interests of the UK.

2.3.1 What is the Financial Action Task Force (FATF)?

FATF is an inter-governmental body which develops international standards to combat money laundering and terrorist financing. It also produces lists of countries that do not have sufficient legal and regulatory standards to combat money laundering and terrorist financing.

2.4 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 Regulations 2007: General obligations

3.1 Policies and procedures

Regulation 20 of The Money Laundering Regulations 2007 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 2002 and Part 3 of the 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.

Financial institutions (which include bureau de change, money transmitters and cheque cashers) must, additionally:

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

3.2 Sanctions for non-compliance

The civil and criminal sanctions for failure to comply with the Money Laundering Regulations 2007 the EC Wire Transfer/Payments Regulation and Counter-Terrorism Act 2008 are explained in Appendices 1 and 2 of this guidance.

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 and the Counter-Terrorism Act 2008.

Senior management means a 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 MLR 2007 regulations 20 and 21
- recognition of the importance of staff promptly reporting their suspicions internally.

Risk mitigation approach:

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

4.3 Liability for offences by corporate bodies

Under the 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 and the Counter-Terrorism Act 2008 are in a similar position. Failure of senior managers to comply with the Money Laundering Regulations 2007 and Directions issued by HM Treasury under Schedule 7 to the Counter-Terrorism Act 2008 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, so as to enable them to take appropriate action to prevent or report it.

Systems of internal control and communication must be capable of identifying unusual or suspicious transactions or customer activity, of identifying transactions and business relationships specified in a direction issued by HM Treasury under Schedule 7 to the Counter-Terrorism Act, and enabling prompt reporting of the details to the Nominated Officer/Money Laundering Reporting Officer (MLRO) (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.

5.1.2 What controls are necessary?

Systems of internal control should include:

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

5.1.3 Use of agents

Where relevant businesses offer their products and services through agents that they have listed within their entry on the MLR register, the principal business is responsible for their agents' compliance with the 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 (F&P) 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 F&P 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/mlr**
- 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's AML/CTF policies and procedures are being complied with by agents
- keep records of these declarations and checks to support risk management and internal control policies and procedures.

5.2 Compliance management

Businesses must carry out regular assessments of the adequacy of their systems and controls to ensure that they manage the money laundering and terrorist financing risks effectively and are compliant with the 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 are perhaps not being carried out in accordance with the Money Laundering Regulations 2007/Counter-Terrorism Act 2008 requirements and the business's policies and procedures?
- are correct records kept in respect of evidence of ID taken and other customer due diligence checks?
- 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 7(3), 8(3) and 20(1), 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 counter measures that can be applied to deter, detect and disrupt money laundering and terrorist financing in those circumstances. Appendix 3 provides a template for a policy statement and risk-assessment that some businesses may find useful.

The business should consider the following questions.

What risk is posed by the customer?

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
- transactions that do not make commercial sense
- customers that are carrying out transactions, or business relationships with countries where Financial Action Task Force has highlighted deficiencies in systems to prevent money laundering and terrorist financing.

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 the Money Laundering Regulations 2007 and the 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 and paragraph 10 of Schedule 7 to the Counter-Terrorism Act 2008.

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 more (or the equivalent in any currency) – 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.

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

7.4 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 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 individuals who meet 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?

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 Act of Parliament or Royal Charter) are bodies corporate.

7.7.4 Partnerships (other than LLPs)

The beneficial owners of partnerships are the individuals who:

- are entitled to or control more than a 25% share of the capital or profits of the partnership or more than 25% of the voting rights, or
- otherwise exercise control over the management of the partnership.

7.7.5 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 more, (or the equivalent in any currency) 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 of 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?
- In the case of money transmission, are a number of customers sending payments to the same individual?

Businesses must be able to demonstrate to HMRC that they have adequate checks and controls in place to pick up on such indicators where there is a risk of occasional transactions (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 United Kingdom (UK)
  - ii a Community institution (for example, the European Parliament), or
  - iii an international body (for example, the United Nations (UN)), 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.
- 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 the Money Laundering Regulations, 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. Section 6.2 gives 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, enhanced 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**

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

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 customer's 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.

Businesses are not required to take a copy of the evidence seen to identify the customer. However, where a business records and holds details of identification seen such as the passport issuing authority and reference number, businesses may find it helpful where facilities exist, to take a copy of supplementary evidence of ID such as a utility bill or bank statement to support the documentary evidence obtained.

8.2 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.

8.3 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.

8.4 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 on line 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.

8.5 Criteria for use of an electronic provider

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

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

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

9 Ongoing monitoring of customers in a business relationship

9.1 The requirement to monitor customers' activities

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

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

9.4 Staff awareness

It is essential to recognise the importance of staff awareness. 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.

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, Financial Action Task Force.

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.

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 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.

11.4 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.

11.5 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 to 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' imprisonment and/or an unlimited fine.

There are also offences in relation to:

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

Conviction for this offence can incur up to 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 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 Money Service Businesses. This includes all individuals, at whatever level (employee, manager, director, and so on) of Money Service Businesses. 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 Serious Organised Crime Agency (see appendix 6 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, in other words, 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 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 Proceeds of Crime Agency 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 proceedings have already arisen, section 340(11) of Proceeds of Crime Agency includes within the definition of money laundering any attempt, conspiracy or incitement to commit an offence under sections 327 to 329.

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

The regulation:

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

1.4 Counter-Terrorism Act 2008

Schedule 7 to the act:

- addresses the risks from money laundering, terrorist financing and the proliferation of nuclear, radiological, biological or chemical weapons
- gives powers to HM Treasury to issue directions to firms in the financial sector, including Money Service Businesses
- requires Money Service Businesses to comply with directions issued by HM Treasury
- appoints HMRC as an enforcement authority and gives powers to HMRC to supervise Money Service Businesses to ensure their compliance with the requirements imposed by any direction.

1.4.1 Schedule 7 to the Counter-Terrorism Act 2008 (Part 7 of the Schedule) Offences & Civil Penalties

This sets out the primary offences relating to breaching a Counter-Terrorism Act direction, which are:

- failure to comply with requirements imposed by a direction: paragraph 30
- offences in connection with licences: paragraph 31.

Conviction for the above offences can result in unlimited fines and/or imprisonment for up to 2 years.

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 MLR9 *Registration notice*.

2.1.1 Civil penalties under the Money Laundering Regulations 2007

Regulation 42 of Money Laundering Regulations 2007 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.

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.

For money transmission businesses Transfer of Funds (Information on the Payer) regulation 14 sets out similar criteria for breaches of those regulations.

Conviction under the Money Laundering Regulations 2007 or Transfer of Funds 2007 can incur up to 2 years' imprisonment and/or an unlimited fine.

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

Include the date of any risk assessment.

3.3 Customer profile

Include relevant customer profile information, for example:

Number percentage 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 of this guidance)
- 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 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 69 for definition)
- remittance of funds to countries with high levels of organised crime or drug production/distribution
- 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 should be assessed in relation to:

- customers – types and behaviours
- 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, in other words, 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
Customers that are carrying out transactions or business with countries where the FATF has highlighted deficiencies in systems to prevent money laundering and terrorist financing
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 internal guidance and procedural instructions.

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.
- In what circumstances are checks made to the consolidated list of persons designated as being subject to financial restrictions on HM Treasury's website?

Attach or refer to relevant employee instructions

3.7 Customer due diligence: Business relationships

3.7.1 Customer due diligence when establishing a business relationship

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

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

What information on the customer's identity is obtained?

What verification is carried out?

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

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 sale, 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's policies or procedures, for example, risk alerts
- 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.

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 (SAR)

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 (EDD) requirements is provided in section 7. Further guidance on identification and verification is provided in section 8. Money transmission businesses must also follow the requirements of the EC Wire Transfer/Payments Regulation which requires verification of customers' identity for all transactions over 1000 euro (or the equivalent in any currency). These requirements are explained in appendix 7. 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, 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 list 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 7.7.2). Obtain information on the purpose and intended nature of the business relationship (section 7.8.1).
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 7.8).
Regulation 14	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 7.8), take risk-based enhanced due diligence measures (section 7.12). Where the customer is not physically present for identification purposes, or there is a risk of impersonation fraud, obtain additional evidence of 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 7.11.3).

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.

Regulation EC 1781/2006 on information on the payer accompanying transfers of funds (commonly known as the Payments Regulation or the Wire Transfer Regulation) gives money transmission businesses the option of obtaining other customer details in place of the customers address as part of the complete information on the payer. The address can be replaced by:

- the customer's date and place of birth, or
- a customer identification number, or
- the customer's national identity number, for example, passport number.

Verification of the above information is not required where the transfer of funds is not made from a customer's account and is not more than 1000 euros.

However, where businesses suspect that there may be a risk of impersonation fraud they should consider obtaining and verifying evidence of the customers address and possibly additional information. (Where additional information is held for verification purposes, the information sent with the transfer may still be restricted to the name and customer unique identification number.)

Guidance on this regulation can be found at appendix 10: *Money Transmission Businesses*.

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

Or a government-issued document (without a photograph) which incorporates the 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 customer's 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 order.
- 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 business's 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:
- Does the address 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 government-issued ID 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 8.5 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 Resident Permit, or • IND travel document (that is, Blue Convention Travel 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 do not physically meet their customers (see Section 7.11.2).

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 Money Service Businesses specific guidance paragraph 1.2.2 for companies, and the relevant guidance referred to in section 1.2.3 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 as standard in relation to corporate customers:
- 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 7.7.2).

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 each of the sector specific appendices 9 to 11.

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 Financial Services Authority 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 Financial Services Authority 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 and Part 3 of the Terrorism Act, businesses in the regulated sectors and their employees are required to disclose information to SOCA in circumstances where they:

- know or suspect, or
- have reasonable grounds for knowing or suspecting,

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

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 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. This is because they are directly responsible for making disclosures under PoCA and the TA 2000.

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

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

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

Suspicion is an opinion held that is based on information or circumstances but without certainty or proof. Unusual transactions are not necessarily suspicious. However, the 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 terrorist funding must be identified and scrutinised. This 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.

Where a business wants to report proliferation financing they should use the existing system for reporting SARs. However, businesses must identify this on the report by including the Unique Identifier xxOCPxx at the start of the Reason for Suspicion field.

Depending upon the terms of the Counter-Terrorism Act direction a business may be required to conduct enhanced due diligence or make periodic reports of its business activities in relation to a customer but not to cease operations with that customer. See appendix 7 of this guidance for further details about Counter-Terrorism Act directions. In addition to complying with the direction the business may also consider it necessary to report the transaction as suspicious. Unlike SARs there is no requirement for businesses to wait for consent for these types of reports and there are no tipping off offences. Businesses are however, advised not to let the subject of their suspicions know that they are submitting a report.

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 their 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 Acts contain similar offences.

This means that businesses must not tell a customer that:

- a transaction was/is being delayed because consent from SOCA has been requested
- 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.

Where businesses are required to carry out detailed checks on customers, or transactions following a direction, and identify affected transactions when carrying out any of the four detailed checks shown in paragraph 2.3 then the tipping off offences under the Proceeds of Crime Act and Terrorism Act do not apply.

There is no tipping off offence under the Counter-Terrorism Act. For further details regarding the Counter-Terrorism Act see appendix 7.

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.
- There is no genuine reason for the customer using the services of a Money Service Business.
- 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: Directions issued by HM Treasury under Schedule 7 to the Counter-Terrorism Act 2008

7.1 What is a direction issued under Schedule 7 to the Counter-Terrorism Act 2008 (a direction)?

See section 2, paragraph 2.3 on page 3.

7.1.1 Who supervises businesses to ensure their compliance with requirements imposed by a direction?

Schedule 7 to the Counter-Terrorism Act appoints HMRC as the enforcement authority and gives new powers to HMRC to supervise Money Service Providers to ensure their compliance with the requirements imposed by any direction.

7.1.2 Who will be required to comply with the terms of a direction?

Directions can specify the firms that must comply with the terms of the direction. When a direction is issued, the Treasury will specify the range of businesses which are obliged to comply.

7.1.3 How often will directions be issued?

Directions are issued in response to significant risks to the national interests of the UK. As such, the frequency of directions will depend on the perceived risk to the UK.

7.1.4 How long will a direction last?

One year. After a year, HM Treasury will consider whether it is necessary to renew the direction. Directions may be withdrawn at any time.

7.1.5 How will businesses know when a direction has been issued?

All businesses should sign up to HM Treasury's alert system, which will issue notification of directions, which can be done at **www.hm-treasury.gov.uk/fin_crime_mailinglist**

HM Treasury will also put an announcement on their website, go to **www.hm-treasury.gov.uk/home** when they issue a direction. In addition, HMRC may put an announcement on their Money Laundering Regulations website.

7.1.6 What will directions require?

Directions can impose a range of requirements on a business in relation to their transactions or business relationships with the targeted country or institution:

- enhanced due diligence
- enhanced ongoing monitoring
- systematic reporting
- limiting or ceasing business.

The requirements to carry out enhanced customer due diligence and ongoing monitoring are in line with similar requirements under the Money Laundering Regulations 2007. The requirements for systematic reporting and limiting or ceasing business are new.

7.1.7 What is systematic reporting?

Systematic reporting requires businesses to periodically report all transactions with people and organisations that are affected.

HM Treasury will explain in each systematic reporting direction what information should be provided about transactions and business, including where and when information should be sent.

7.1.8 Should businesses continue to submit Suspicious Activity Reports (SAR) in relation to these transactions and business?

Yes, businesses should continue to submit SARs where necessary alongside systematic reporting.

7.1.9 What if Money Service Businesses have to cease business with certain people or organisations?

Businesses must not do business with people or organisations specified as 'designated persons' in a direction which requires the cessation of business or transactions. In some circumstances HM Treasury may grant general licences to exempt certain transactions or types of transaction from the requirements of the direction, or specific licences to exempt individual transactions. Either the business or the business's customers can apply for a licence. HM Treasury will provide further information on how to apply for licences when they issue a direction.

7.1.10 What will happen to the money if a business has to stop a transaction?

Preferably, the money should be refused before a transaction can be started. HM Treasury will issue guidance with each direction regarding the transactions which will be subject to the requirements.

7.1.11 HMRC action against breaches of Counter-Terrorism Act Directions

Failure to comply following a direction issued under Schedule 7 to the Counter-Terrorism Act is a criminal offence. Failure to comply following a direction is therefore a serious matter. However, where there is evidence that a business failed to comply with a direction we are likely only to report the mater to the appropriate prosecuting authority for a decision to be made as to prosecution in accordance with the Code for Crown Prosecutors if we consider the failure to comply is severe. HMRC also has civil powers in respect of breaches of a direction.

Appendices 9,10 and 11 of this guidance includes information on industry good practice on compliance with the Counter-Terrorism Act 2008 for bureau de change, money transmission businesses and cheque encashment businesses.

7.1.12 Will branches of financial and credit institutions outside the UK be subject to the requirements of the direction?

Yes, the direction applies to all branches of a financial or credit institution within the EEA but not to any non-financial subsidiaries of financial or credit institutions, wherever they are based, (a list of countries included in the EEA are shown at appendix 12).

7.1.13 Will the directions list the individuals within a business that businesses should not deal with?

No, where businesses are required to limit or cease business with another organisation the directions will identify the organisation or business only. However, firms should not continue business with individuals within an organisation or business when those individuals are acting in the course of the organisation or business's activities.

7.2 What is customer due diligence

The meaning and application of customer due diligence is set out in paragraph 10 of Schedule 7 to the Counter-Terrorism Act 2008.

These regulations require businesses to:

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

7.3 Enhanced due diligence

7.3.1 General legal requirements

If an enhanced due diligence direction is issued by HM Treasury under Schedule 7 to the Counter-Terrorism Act this may require affected businesses to apply enhanced due diligence measures:

- before entering into a transaction or a business relationship with a 'designated' person, as described at paragraph 2.3
- during a business relationship with a person shown at paragraph 2.3.

The precise due diligence measures required will be set out in the direction.

7.4 What policies and procedures do Money Service Businesses need in place?

Money Service Businesses must have policies and procedures in place that identify and scrutinise transactions or business relationships which are subject to any direction issued by HM Treasury under Schedule 7 to the Counter-Terrorism Act 2008.

7.5 Do Money Service Businesses need to undertake ongoing monitoring of customers in a business relationship?

Money Service Businesses must conduct ongoing monitoring of their business relationships with their customers. The Counter-Terrorism Act 2008 paragraph 11(3) 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.

7.6 Do Money Service Businesses need to provide training?

Money Service Businesses must ensure that relevant employees are aware of their responsibilities under the Counter-Terrorism Act 2008 following the issue of a direction by HM Treasury.

Appendix 8: Financial sanctions maintained by HM Treasury Asset Freezing Unit

8.1 Financial sanctions

A consolidated list of financial sanctions targets, that is, those individuals and entities designated as being subject to financial sanctions, is available. Go to **www.hm-treasury.gov.uk/fin_sanctions_index** Please note, this list does not contain firms subject to restrictions imposed by HM 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 (UN), European Union (EU) and United Kingdom (UK) under legislation relating to current financial sanctions regimes. It is a criminal offence to make funds or economic resources, and in the case of the Terrorism (United Nations Measures) Order 2009. 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.

8.2 Who is responsible for sanctions policy in the UK?

The Foreign and Commonwealth Office (FCO) is responsible for the 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.

8.3 Financial sanctions versus HM Treasury directions

Financial sanctions requirements originate from UN resolutions and/or EU regulations and businesses must not make funds, economic resources, or in certain circumstances financial services available to targets. In contrast, directions under the Counter-Terrorism Act 2008 are solely domestic decisions of HM Treasury and businesses must comply with the terms of a direction.

8.4 Asset Freezing prohibitions

8.4.1 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 sanctions can be found on the HM Treasury website, go to **www.hm-treasury.gov.uk/fin_sanctions_index** It does not however, include firms subject to restrictions imposed by HM Treasury directions issued under Schedule 7 to the Counter-Terrorism Act. The requirements for compliance with firms subject to Treasury directions are distinct from those subject to sanctions. See paragraph 8.3 which sets out the differences.

Further information on financial sanctions can also be found at **www.hm-treasury.gov.uk/fin_sanctions_index**

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 person (individual or sole proprietor) or legal person (trustee, limited company or partnership) to:

- deal with the funds of designated persons
- make funds, economic resources or (in the case of persons designated under the Terrorism Order 2009) 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.

'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 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 below.

8.4.2 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 the PoCA 2002 or the 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

8.4.3 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.

Appendices 9, 10 and 11 include guidance on industry good practice on compliance with the financial sanctions requirements for bureau de change, money transmission businesses and cheque encashment businesses.

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

Appendix 9: Supplementary guidance – Bureau de Change

Please note this specific guidance must be read in conjunction with the main guidance in sections 1-11 and appendices 7 and 8.

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

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

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

In this section, bureau de change activities do not include money transmission products, which are dealt with in a separate section. However, such products are normally supplied on an agency basis and it is important to ensure that bureau de change establish Anti-Money Laundering (AML) related accountabilities with the product provider and ensure that these are clearly defined and documented.

9.1 Do bureau de change fall into the scope of the Counter-Terrorism Act?

Bureau de change are Money Service Businesses and therefore fall within the scope of the Counter-Terrorism Act. All businesses within the scope of the legislation should include how to comply with directions in their policies and processes and sign up to the HM Treasury email alert system, go to **www.hm-treasury.gov.uk/fin_crime_mailinglist**

9.2 What should businesses do when HM Treasury issues a direction that affects their business?

Directions issued under the Counter-Terrorism Act powers will specify which businesses must comply with the requirements contained within it. Firms that must comply with the requirements should consult HM Treasury issued guidance, which will be issued alongside each direction, and will explain in detail the obligations on firms.

Businesses are legally required to comply with the terms of a direction. They must therefore ensure that they meet the terms of the direction, and must examine all relevant business areas to ensure that they are doing so. Directions may take different forms and may require different responses in order to ensure businesses are doing all that is required of them. It is not possible to provide guidance to cover every eventuality. But in practical terms where for example named businesses are the subject of a direction it is good practice for bureau de change to search their list/database of known corporate customers to check whether there is any existing relationship with the target of the direction and take the action required by the direction. Businesses should take steps to ensure their ongoing compliance with the requirements of a direction and should note their response to directions in their records.

Businesses will have to identify the customers or transactions that are affected, and put in place procedures to ensure that they are able to comply with the terms of the direction.

Businesses may have to do one or more of the following:

- Carry out enhanced customer due diligence (see appendix 7). A business would normally have to do this under the Money Laundering Regulations in high-risk situations such as when the customer is a politically exposed person.
- Carry out ongoing monitoring of customers in a business relationship (see appendix 7, paragraph 7.4). This is the kind of monitoring businesses would be expected to do in high-risk situations.
- Report all transactions with designated persons (that is, people or businesses targeted in a direction).
- Cease or limit business with designated persons.

9.3 What are the money laundering risks faced by bureau de change?

There is a high risk that the proceeds of crime will pass through bureau de change at all stages of the money laundering process. However, many

millions of foreign exchange transactions are conducted each month and the likelihood of a particular transaction actually involving the proceeds of crime is very low.

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

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

9.3.1 Factors that may increase the Money Laundering Risk

Size of transactions and product types:
Cash transactions: Cash is the mainstay of much organised criminal activity. For the criminal, it has the obvious advantage of leaving no discernible audit trail and is their most reliable and flexible method of payment. Cash is also a weakness for criminals. They are more at risk of being traced to the original offence which generated the cash in the first place. Cash seizure powers also mean they are more at risk of having the money taken away by law enforcement. The objective of the first stage of money laundering, that is, placement, is to move the criminal cash into the financial system. They will therefore often seek to exchange cash in one currency for foreign currency (or visa versa). This may involve exchanging small denominations of one currency for large denominations of another currency. This is considered to be the most difficult and risky part of the money laundering cycle for criminals.
Speed and size of the transaction: Money launderers normally want to move funds quickly in order to avoid detection or seizure. This is more easily done in large one-off transactions.
Split transactions: The more sophisticated money launderer will look to split a large transaction into several smaller ones with the intention of avoiding AML-related controls. Such splitting can occur within one location, across branches or across organisations. This is known as 'smurfing' — when a number of people each exchange small amounts of cash. The funds eventually end up back with the criminal.
The product is easily transported across jurisdictions and can easily be transferred to another person without leaving an audit trail. This may be particularly pertinent when a product can be transported to high-risk jurisdictions. Currency smugglers will look to move products into countries with no exchange control and lax AML/CTF legislation.
Buy-backs and refunds: Amounts of foreign currency may be presented by launderers for exchange into sterling in cash, draft, travel cheques or other instrument. This could be either an attempt at placement or part of the layering process.
Swaps through a third currency: Amounts of currency could be presented for exchange into a third currency, an example would be dollars are exchanged into euro through sterling, possibly from small denominations into easily transported large notes. This would be part of the layering process.
Customer related:
The customer operates within a high-risk sector. Some money launderers will be proprietors of cash-based businesses such as restaurants, pubs, casinos, taxi firms, beauty salons and amusement arcades. The aim here is to mix 'dirty' money with 'clean' and so muddy the trail.
The customer is a Money Service Business.
The customer undertakes transactions that make no commercial sense or do not match the profile of the customer. This also includes significant and unusual changes to a customer's established pattern of behaviour.
The customer is not the beneficial owner of the funds and carries out transactions on behalf of a third-party or parties
Geographical factors:
Transactions linked to customer connected with countries that are known to have lax AML controls.
Transactions may also straddle jurisdictions, with funds moving from well-regulated countries to those with poor regulatory regimes.
The bureau operates within a geographical area where it has previously identified a higher than average number of potential money laundering cases.

9.3.2 Factors that may reduce the money laundering risk

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

9.4 Managing the risk

To assist in managing the risk of their business being used as a vehicle for money laundering, each bureau de change operator must develop policy and procedure documents that outline the steps the firm will take to meet the requirements of the regulations in relation to training, identification and verification procedures, risk assessment and management, the monitoring of business relationships, suspicious activity reporting, internal systems and controls and compliance monitoring and management.

9.5 Identification issues

9.5.1 Industry recommended thresholds

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

9.5.2 Evidence of identification

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

- method of payment, for example, cash
- transaction type, for example, type of currency
- source of funds.

9.5.3 Financial exclusion

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

9.6 Linked transactions

Businesses must put in place a process to monitor repeat transactions with customers whose identity has been obtained, in order to identify customers who may be attempting to split large transactions into several smaller, less conspicuous amounts, which could indicate 'smurfing' activity (see Glossary on page 69 for definition). It is deemed good practice to monitor for repeat business over the preceding 90 days from the date of the most recent transaction, using risk indicators and profiles that are appropriate to the business. Unusual or suspicious transactions or patterns of activity should be reported to the Nominated Officer.

9.7 HM Treasury consolidated list of Financial Sanctions Targets

Bureau de change must have regard for the guidance in appendix 8.

Sanctions legislation does not prescribe how firms should comply. However it is an offence to:

- deal with the funds (and economic resources) of a designated person,
- make funds (and economic resources) available to a designated person, and

in the case of the Terrorism Order

- provide financial services, to or for the benefit of a designated person without a licence from HM Treasury.

To reduce the risk of breaching obligations under financial restrictions regimes, bureau are likely to focus their resources on areas of their business that carry a greater likelihood of involvement with targets or their agents. Within this approach, bureau are likely to focus their prevention and detection procedures on higher value transactions rather than the vast majority of transactions that are of very low value with no identification documents being presented or recorded. The risk factors that necessitate a check against the consolidated list should be documented and relevant staff trained in the appropriate procedures to follow. The consolidated list can be found at **www.hm-treasury.gov.uk/fin_sanctions_index** Businesses should note that the consolidated list 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. See appendix 8 which sets out an important difference.

A business that is unable to demonstrate why no controls are in place or why no check was undertaken in a particular case is more at risk of prosecution.

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

If a check produces a positive match, the transaction must not proceed and a report should be submitted to HM Treasury. The business may also need to consider whether they have an obligation to report to SOCA under PoCA or the TA (see appendix 6 for further information).

In addition, the Asset Freezing Unit at HM Treasury also publishes an Investment Ban list which includes details of those subject to specific 'investment' prohibitions currently related to Burma/Myanmar. The risk factors that necessitate a check against the Investment Ban list should be documented and relevant staff trained in the appropriate procedures to follow.

9.8 Training

In accordance with the guidance in section 10 of this guidance, foreign exchange businesses should undertake to train all relevant staff:

- when appointed to a money service businesses role
- at least once every 2 years thereafter.

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

9.9 Suspicion indicators

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

Appendix 10: Supplementary guidance – Money Transmission Businesses

Please note this specific guidance must be read in conjunction with the main guidance in sections 1-11 and appendices 7 and 8.

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

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

Money transmission businesses carry out most transactions either directly, face-to-face with the customer at the money transmission businesses high street premises, or through agents, although a growing number of transactions are now carried out via the Internet.

10.1 What should businesses do when HM Treasury issues a direction under the powers in the Counter-Terrorism Act 2008?

Directions issued under the Counter-Terrorism Act powers will specify which businesses must comply with the requirements contained within it. Firms that must comply with the requirements should consult the Treasury issued guidance, which will be issued alongside each direction, and will explain in detail the obligations on firms.

Businesses will have to identify the customers or transactions that are affected, and put in place procedures to ensure that they are able to comply with the terms of the direction.

Businesses may need to do one or more of the following:

- Carry out enhanced customer due diligence (see appendix 7). Businesses would normally do this in high-risk situations such as when the customer is a politically exposed person.
- Carry on ongoing monitoring of customers in a business relationship (see appendix 7, paragraph 7.4). This is the kind of monitoring that businesses will carry out in high-risk situations.
- Report all transactions with designated persons (that is, people or businesses targeted in a direction).
- Cease or limit business with designated persons.

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

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

The scrope for money transmission businesses to adopt a risk based approach is limited by the requirements of EC regulation 1781/2006 which requires businesses to obtain complete information on the payer, and that this information must accompany transfers of funds at all stages. It also requires that this information is verified for transactions over 1000 euro.

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

10.3 How should the risk-based approach be implemented?

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

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

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

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

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

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

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

10.4 What are the money laundering risks in the industry?

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

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

10.4.1 Factors that increase risk

- Factors that relate to the product itself, including:
  - High value remittances.
  - Cash funding and cash payouts.
- The countries in which the product operates may give rise to a higher risk of money laundering because of a generally higher crime rate or likelihood of money laundering or terrorist financing.
- Factors that relate to the nature of the business arrangement, including:
  - The existence of an agency relationship, where the money transmission business is dependent on an agent for customer contact. The determining factor here is how much communication exists between the money transmission business and the agent.
  - The level of control or comfort regarding the entity delivering the funds in the receiving country.
- Non face-to-face transactions.
- New customers with no previous relationship with the money transmission business, looking to undertake larger transactions.
- Lack of knowledge regarding the origin or destination of funds.
- Lack of a meaningful purpose for the transaction.
- Customers carrying out transactions or business with countries where FATF has highlighted deficiencies in systems to prevent money laundering and terrorist financing.

10.4.2 Factors that decrease risk

- Factors that relate to the product itself, including:
  - the product is designed and mainly used for low value remittances
  - funding from and payment into bank accounts
  - the using of accounts to keep track of customer transactions
  - the ability to track linked transactions and identify transaction patterns
  - visibility of transactions conducted at other locations by agents of the same or a related money transmission business
  - the ability to freeze transactions after they have been initiated.
- The countries in which the product operates are regarded as having a lower risk of crime, money laundering or terrorist financing.
- Knowledge of the recipient as well as of the sender of funds.
- Factors relating to the nature of the business arrangement, including:
  - the money transmission business is a single operation without agent relationships and hence with direct customer contact
  - control or comfort regarding the entity delivering the funds in the receiving country.
- Face-to-face contact with the customer.
- An ongoing relationship with the customer.
- Knowledge of the origin of funds.
- A stated purpose for the transaction, confirmed by the features of the transaction.

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

10.5.1 General legal requirements

In addition to the customer due diligence measures that must be applied under the Money Laundering Regulations, money transmission businesses must also comply with the EC Payments/Wire Transfer Regulation and Transfer of Funds (Information on the Payer) Regulations 2007 (which set out the UK's supervision and enforcement provisions), and the requirements of any direction issued by HM Treasury under its powers in Schedule 7 to the Counter-Terrorism Act.

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

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

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

10.5.2 Definitions

Payment Service Provider (PSP)

For the purposes of this notice, a payment service provider means a money transmission business

Payer

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

Payee

The Payee is the beneficiary of a transfer of funds.

Intermediary Payment Service Provider (IPSP)

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

10.5.3 Obligations on payment service providers (PSPs)

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

The PSP for the payer must:

- Obtain complete information on the payer (see paragraph 10.5.4 below) from all customers wanting to conduct a money transfer.
- Verify the complete payer information (CIP) on the basis of documents, data or information from a reliable and independent source where the transaction is over 1000 euro whether carried out as one operation or in several operations that appear to be linked and together exceed 1000 euro.
- If the payer does not have an account number, allocate the transaction a unique identifier number which allows the transaction to be traced back to the payer.
- Keep records of the details of the transaction, including the complete information on the payer, for 5 years.
- If the payment service provider for the payee is situated in the European Community, ensure that the transfer of funds is accompanied by the account number of the payer, or a unique identifier allowing the transaction to be traced back to the payer
- For intra-EC transfers, if requested by the PSP of the payee, make available the complete information on the payer, within three working days
- If the payment service provider for the payee is outside the European Community, ensure that complete information on the payer is sent to the payment service provider of the payee.

The PSP for the payee must:

- Detect if the CIP is missing.
- In the case of missing or incomplete information on the payer, reject the transfer or ask for the missing information.
- Where there is a regular failure to supply the required information on the payer, take steps such as warning letters and deadlines, before either rejecting future transfers from the payment service provider or deciding whether or not to restrict or terminate its business relationship with that payment service provider.
- Where information is missing or incomplete, consider whether the transfer of funds, or any related transaction is suspicious, and if so, submit a suspicious activity report (SAR) to the Serious Organised Crime Agency (SOCA)
- Keep records of all such instances detailing the reasons for complete information on the payer (CIP) not being provided, your decision as to whether or not to carry out future transactions with the PSP and, if appropriate, details of any reports made to SOCA.
- Keep records of any information received on the payer for 5 years.

The IPSP must:

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

10.5.4 Complete information on the payer (CIP)

CIP consists of the:

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

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

- The payer's date and place of birth.
- The payer's customer identification number.
- The payer's national identity number (for example, passport number).

Customer's identification number

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

10.5.5 Questions concerning the sending of complete information on the payer

Who do I send information on the payer to if the transaction goes through an IPSP?
If the IPSP is responsible for arranging the transfer of funds then you should send the complete information on the payer to that IPSP. (If you do not do this then the payment from the IPSP may be blocked when the payment goes through the banking system.)

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

If I am an IPSP do I need to send the information on each payer to the PSP of the payee or can I just send details of the PSP that is my customer?
Unless you have a written agreement with the PSP who is your customer (see details below) you should send the information on the payer for each individual transaction to the person paying the money to the payee.

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

If I am an IPSP and the PSP of the payer wishes to send information on the payer direct to the overseas PSP what am I required to do?
You must decide if you are content with the arrangement. If not you should insist on receiving the information on the payer. If you are content you should obtain written confirmation from the PSP that they are sending the information on the payer direct to the overseas PSP. Record the PSP as the payer with your transmission.

If as a PSP or IPSP I have sent the information on the payer to the PSP of the payee do I also need to send it to my bank/IPSP when I arrange for a payment covering several separate money transmission arrangements?
No the bank/IPSP will regard you as the payer and will therefore only need your details.

If I am a PSP of a payer but I do not deal with the PSP of the payee (for example I have a bank account in the overseas country and instruct my bank to transfer funds to the payee's account or I use a non-business representative to withdraw money from my overseas account and distribute it to payees) to whom do I send the information on the payer?*
If there is no overseas PSP you must send the complete information on the Payer to the overseas bank where you are transmitting the payment.

Does the information need to be sent in any particular format?
Yes it needs to be sent in such a way that there is a retrievable record of the information that was sent, when it was sent and to whom. The CIP also needs to be traceable back to the individual transactions to which they relate, examples may include:
- copies of emails
- copies of faxes
- computer records.

10.5.6 Sanctions for non-compliance

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

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

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

For further information regarding criminal offences and penalties for money laundering and terrorist financing see Appendices 1 and 2.

10.6 Verification of identity

10.6.1 General legal requirements

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

Money Laundering Regulations 2007 regulation 7(3) requires that a relevant person must:

- determine the extent of customer due diligence measures on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction
- be able to demonstrate to the supervisory authority that the extent of the measures is appropriate in view of the risks of money laundering and terrorist financing.

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

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

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

10.6.2 Alternative means of verification

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

10.6.3 Beneficial owners

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

10.6.4 Pooled funds

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

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

10.7 Nature and purpose of the business relationship

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

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

For business customers, further information includes:
- Turnover of the business, its size, and its number of employees.
- Length of establishment.

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

10.8 Ongoing monitoring of business relationships

Section 9 provides guidance on the requirement for ongoing monitoring of business relationships under Money Laundering Regulations 2007 regulation 8 and any requirement for enhanced ongoing monitoring under a direction issued by the Treasury under Schedule 7 to the Counter-Terrorism Act 2008.

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

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

10.9 Customers who are money transmission businesses

Regulation 13 of Money Laundering Regulations 2007 allows simplified due diligence for Money Service Business (MSB) customers, which means that money transmission businesses are not required to apply the customer due diligence measures concerning verifying the identity of the customer and beneficial owner, or obtaining information on the purpose and intended nature of the business relationship. It is, however, good practice for money transmission businesses to check the online MSB register to check that a Money Service Business is registered with HMRC before entering into a business relationship with another Money Service Business.

Businesses must conduct ongoing monitoring of the business relationship. Section 9 provides further guidance on methods of ongoing monitoring.

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

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

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

10.10 Use of agents

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

to manage the risks where business is conducted through agents.

10.11 Enhanced due diligence

10.11.1 Non face-to-face customers

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

10.11.2 Politically exposed persons (PEPs)

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

10.11.3 Other higher risk situations

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

Section 6.2 gives examples of risk indicators.

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

10.13 Suspicious activity reporting

See appendix 6 for guidance on reporting suspicious activity under Part 3 of the PoCA and Part 7 of the TA 2000, including examples of circumstances that should arouse suspicion.

10.13.1 Linked transactions

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

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

10.14 HM Treasury consolidated sanctions list

Money transmitters must have regard for the guidance in appendix 8.

Sanctions legislation does not prescribe how firms should comply. However it is an offence to:

- deal with the funds (and economic resources) of a designated person
- make funds (and economic resources) available to a designated person, and

in the case of the Terrorism Order

- provide financial services, to or for the benefit of a designated person without a licence from HM Treasury.

Therefore, to reduce the risk of breaching obligations under financial restrictions regimes, money transmission businesses are likely to focus their resources on areas of their business that carry a greater likelihood of involvement with targets, or their agents. The risk factors that will necessitate a check against the consolidated list should be documented and relevant staff trained in the appropriate procedures to follow. The Consolidated List can be found at **www.hm-treasury.gov.uk/fin_sanctions_index**

Businesses should note that the consolidated list 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. See appendix 8, paragraph 8.3 which sets out an important difference.

A business that is unable to demonstrate why no controls are in place or why no check was undertaken in a particular case is more at risk of prosecution.

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

If a check produces a positive match, the transaction must not proceed and a report should be submitted to HM Treasury. The business may also need to consider whether they have an obligation to report to SOCA under PoCA or the TA (see appendix 6 for further information).

In addition, the Asset Freezing Unit at HM Treasury also publishes an Investment Ban list which includes details of those subject to specific 'investment' prohibitions currently related to Burma/Myanmar. The risk factors that will necessitate a check against the Investment Ban list should be documented and relevant staff trained in the appropriate procedures to follow.

10.15 Case Studies

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

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

10.16 Training

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

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

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

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

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

Appendix 11: Money Laundering Regulations – Specific guidance for Cheque Encashment Businesses (CEBs)

Please note this specific guidance must be read in conjunction with the main guidance in sections 1-11 and appendices 7 and 8.

11.1 Overview of the sector

This section of the guidance provides an overall understanding of the aspects of the money laundering and terrorist financing problems that could involve the cheque-cashing trade and guidance on identifying and mitigating the risks involved. It also provides information on the obligations of businesses when a direction is issued by HM Treasury.

11.2 Do Cheque Encashment Businesses fall into the Scope of the Counter-Terrorism Act?

Cheque Encashment Businesses are Money Service Businesses and therefore fall within the scope of the Counter-Terrorism Act.

All businesses within the scope of the legislation should include how to comply with directions in their policies and processes and sign up to the HM Treasury email alert system, go to **www.hm-treasury.gov.uk/fin_crime_mailinglist**

11.3 What should businesses do when HM Treasury issues a direction that affects their business?

Directions issued under the Counter-Terrorism Act powers will specify which businesses must comply with the requirements contained within it. Firms that must comply with the requirements should consult the Treasury issued guidance, which will be issued alongside each direction, and will explain in detail the obligations on firms.

Sanctions legislation does not prescribe how firms should comply. However it is an offence to:

- deal with the funds (and economic resources) of a designated person
- make funds (and economic resources) available to a designated person, and

in the case of the Terrorism Order

- provide financial services, to or for the benefit of a designated person without a licence from HM Treasury.

Businesses will have to identify the customers or transactions that are affected, and put in place procedures to ensure that they are able to comply with the terms of the direction.

Businesses may need to do one or more of the following:

- carry out enhanced customer due diligence (see appendix 7). Businesses would normally do this in high-risk situations such as when the customer is a politically exposed person
- carry out ongoing monitoring of customers in a business relationship (see appendix 7, paragraph 7.4). This is the kind of monitoring businesses would do in high-risk situations
- report all transactions with designated persons (that is, people or businesses targeted in a direction)
- cease or limit business with designated persons.

HM Treasury consolidated list of financial sanctions targets

Cheque encashment businesses must have regard for the guidance in appendix 8.

To reduce the risk of breaching obligations under financial restrictions regimes, businesses are likely to focus their resources on areas of their business that carry a greater likelihood of involvement with targets or their agents. Within this approach, businesses are likely to focus their prevention and detection procedures on direct customer relationships, and then have appropriate regard to other parties involved. The risk factors that necessitate a check against the consolidated list should be documented and relevant staff trained in the appropriate procedures to follow. Businesses should note that the consolidated list 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. See appendix 8, paragraph 8.3 which sets out an important difference.

Relevant sources of information should be consulted to build up appropriate risk profiles based on the customer types and behaviour and knowledge of locations with high levels of drug or other organised crime or terrorist activity.

Information on high risk jurisdictions and locations is available from the Financial Action Task Force website **www.fatf-gafi.org** and other Internet sources.

If a check produces a positive match, the transaction must not proceed and a report should be submitted to HM Treasury. The business may also need to consider whether they have an obligation to report to SOCA under PoCA or the TA (see Appendix 6 for further information).

In addition, the Asset Freezing Unit at HM Treasury also publishes an Investment Ban list which includes details of those subject to specific 'investment' prohibitions currently related to Burma/Myanmar. The risk factors that will necessitate a check against the Investment Ban list should be documented and relevant staff trained in the appropriate procedures to follow.

11.4 What are the risks faced by cheque encashment businesses?

11.4.1 General

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

11.4.2 Sources of cash

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

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

11.4.3 Tax evasion

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

11.4.4 Benefit fraud

Cheque cashers may come across indicators of benefit fraud while cashing wage checks.

Any instances of the above should be reported to SOCA (Which does not investigate money laundering exclusively).

11.4.5 Other types of fraud or theft

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

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

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

11.5 Managing the risks

11.5.1 Agents/Franchisees

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

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

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

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

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

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

11.5.2 Cheque-cashing customers

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

11.6 Identification Issues

11.6.1 General

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

The majority of cheques a cheque casher will handle are for wages – such customers must have wage slips.

Cheques should follow a pattern and should be of similar amounts. Anything that deviates from a customer's normal pattern of business should be queried and reported if suspicion is aroused.

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

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

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

Limited Companies – cheques made payable to a limited company should be presented through the bank account of that company. However, where cheque cashers accepts cheques on a regular basis that are made payable to a limited company they should ensure that they assess the risks involved and establish whether there are valid reasons for cashing a cheque made payable to a limited company. See paragraph 1.9 for suspicious indicators.

11.6.2 Industry recommended thresholds

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

11.6.3 Electronic verification

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

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

11.6.4 Overseas customers

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

11.6.5 Financial exclusion

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

11.7 Linked transactions

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

11.8 Training

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

11.9 Suspicion indicators

- An agent seems able to financially support a continued increase in business with little or no detriment to their cash flow, though the business on reflection should not be able to support such an increase.
- Fictitious companies may be set up for the purpose of cheque fraud – look out for low and consecutive cheque numbers.
- A number of different people cashing cheques all of which are drawn on the same company, with an unfamiliar company name.
- There will be an indication of benefit fraud where people try to cash their benefit cheques (Job Seeker's Allowance) and produce a wages slip as ID or vice-versa where they are cashing their wages cheque and produce paperwork regarding Job Seeker's Allowance as ID.
- People wanting to cash their final pay cheque may be trying to cash the cheque in the knowledge this is not the amount they are entitled to – as final pay cheques are more likely to be stopped, or reissued with a lower amount than the original cheque, due to deductions for monies for holiday/sickness, the non-return of uniform, damaged equipment, non-completion of work, and so on.
- In some circumstances there may be an indication of fraudulently obtained cheques where a person has a number of cheques drawn on different individuals, rather than company cheques, claiming to have done work for these people. One scam encountered within the cheque encashment industry involved the fraudster requesting monies from elderly individuals to administrate the release of their winnings for a lottery/competition. The elderly individuals were asked to give the fraudster a cheque, which the fraudster then tried to cash.
- A sudden increase in cheque values.
- A customer wants to cash a cheque which was made payable to them weeks earlier – usually cheque-cashing customers using a third-party cheque-cashing service need the cash quickly and therefore an old cheque date could mean the cheque has been stolen or tampered with. The customer could have informed the drawer that the cheque is lost, a replacement may have been provided and cashed elsewhere, and the customer then tries to cash the original cancelled cheque.
- Post containing a recently issued chequebook may have been intercepted by a fraudster who then creates ID to replicate the original payee's ID.
- It appears that there has been something added to the cheque after the time of issue, for example different handwriting is evident, value digits appear squeezed in.
- A customer wants to cash a cheque that is made payable to a limited company. The customer could be involved in tax evasion.

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 Money Service Businesses (MSBs) which includes all businesses that undertake:

- exchanging money, or
- transmitting money (or any representation of money), or
- cashing third-party cheques.

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
- a direction has been issued by HM Treasury
- in any other situation which by its nature can present a higher risk of money laundering or terrorist financing.

FATF

Financial Action Task Force.

Financial Institution

Has the meaning given by 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.

Money service business

An undertaking which by way of business operates a currency exchange office, transmits money (or any representations of monetary value) by any means or which cashes cheques which are made payable to customers.

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, their 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, by a state other than the UK, by a Community Institution or by an International body 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.

Proliferation financing

Assisting in the financing and/or development of nuclear, biological, radiological, chemical weapons and/or their means of delivery.

Regulated Sector

Persons and firms which are subject to the Money Laundering Regulations 2007.

SAR

Suspicious activity report made to SOCA.

Senior management

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.

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.

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

Any act by the business of transmitting or exchanging money or cashing cheques.

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 how 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