OFFICE OF FAIR TRADING

Money Laundering Regulations 2007

Core guidance

May 2009

OFT954

CONTENTS

1 INTRODUCTION

1.1 The purpose of this guidance is to provide businesses with advice on how to comply with their obligations under the Money Laundering Regulations 2007 (the regulations) which come into force on 15 December 2007.

1.2 It is intended for businesses that are the subject of the regulations and for whom the Office of Fair Trading (OFT) is the Supervisory Authority:

- estate agents (see chapter 10 for more information)
- consumer credit financial institutions (these are consumer credit lenders not otherwise authorised by the Financial Services Authority, see chapter 11 for further information)

1.3 The OFT with Local Authority Trading Standards Services (TSS) are responsible for effectively monitoring estate agents' and consumer credit financial institutions' compliance with the regulations.

1.4 The guidance is in two parts – part one outlines core obligations and part two provides sector specific guidance. They should be read together.

1.5 Further information about how estate agents and consumer credit financial institutions are defined can be found in the sector specific chapters.

1.6 This guidance is not intended for businesses that are supervised by the Financial Services Authority (FSA) and HM Revenue and Customs (HMRC). If you are unsure who your Supervisory Authority is please see 'who is my supervisor?' flowchart for further information. The flowchart can be found at: www.oft.gov.uk/oft_at_work/markets/services/money-laundering/ Businesses engaged in multiple activities that fall under the regulations may also find it helpful to refer to this information.

1.7 This guidance provides advice about how businesses supervised by OFT can fulfil their duties. It is not intended to be a checklist and as the

regulations introduce a risk based approach, businesses should implement measures on the basis of the risks they face.

1.8 Further information on businesses' obligations under the regulations can be found in guidance produced by industry bodies. The Joint Money Laundering Steering Group (JMLSG) provides additional detailed guidance and can be found at www.jmlsg.org.uk. The JMLSG guidance is primarily aimed at the financial services sector.

1.9 If you are unsure about your obligations under the regulations you should seek legal advice.

What is money laundering?

1.10 Money laundering is the process by which criminally obtained money or other assets (criminal property) are exchanged for clean money or assets with no obvious link to their criminal origins. It also covers money, however come by, which is used to fund terrorism.

1.11 Money laundering can take many forms such as:

- handling the proceeds of crime
- being directly involved with any criminal or terrorist property
- entering into arrangements to facilitate the laundering of criminal or terrorist property
- investing the proceeds of crime into other financial products or into the acquisition of property/ assets.

Legislation

1.12 The main UK legislation covering anti-money laundering and terrorist financing is:

- Proceeds of Crime Act 2002
- Terrorism Act 2000

- Money Laundering Regulations 2007

Proceeds of Crime Act 2002 (POCA)

1.13 POCA sets out the primary offences related to money laundering:

- concealing, disguising, converting, transferring or removing criminal property from the UK
- 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
- the acquisition, use and/ or possession of criminal property
- failing to disclose knowledge or suspicion of money laundering to either the nominated officer (where relevant) or the Serious Organised Crime Agency (SOCA) as appropriate (see chapter 4 for information on the role of nominated officers)
- tipping off any person that such a disclosure has been made.

Terrorism Act 2000

1.14 The Terrorism Act sets out the primary offences related to terrorist funding and requires regulated businesses to report knowledge or suspicion of offences related to terrorist financing:

- fund raising for the purposes of terrorism
- using or possessing money for the purposes of terrorism
- involvement in funding arrangements
- money laundering - facilitating the retention or control of money which is destined for, or is the proceeds of, terrorism.

Counter Terrorism Act 2008

1.15 Part 5 of The Counter Terrorism Act 2008, (section 62 together with schedule 7) sets out the circumstances under which Treasury can impose requirements or restrictions on consumer credit financial institutions in relation to transactions or business relationships with the government of, a person carrying on business in, or a person resident or incorporated in a country of concern. Part 6 of the Act deals with how applications may be made to lift such restrictions.

1.16 Treasury can give a direction in any of the following circumstances:

- The Financial Action Task Force (FATF) has advised that measures should be taken in relation to a country because of the risk of terrorist financing or money laundering being carried on in the country or by the government of or persons resident or incorporated in the country.

- Treasury reasonably believes that there is the risk of terrorist financing or money laundering activities being carried out in a country, by a government or person resident or incorporated in the country and that it poses a significant risk to the national interests of the United Kingdom.

- Treasury reasonably believes that the development, production or anything that facilitates the development or production of nuclear, radiological, biological or chemical weapons in a country poses a significant risk to the national interests of the United Kingdom.

1.17 A Treasury direction can be given to an individual CCFI, a group of businesses being CCFIs or all CCFIs requiring the person to undertake:

- enhanced due diligence

- enhanced ongoing monitoring of business relationships with the person or persons in relation to whom the direction is given

- provide specified information and or documents covering transactions with the person or persons in relation to whom the direction is given

- limit or cease business with. with the person or persons in relation to whom the direction is given.

1.18 The OFT is responsible for taking appropriate measures to monitor CCFIs to ensure their compliance with any directions given under the Counter Terrorism Act and has the ability to impose fines and prosecute criminal offences for breach of such directions.

1.19 This guidance focuses on the Money Laundering Regulations 2007. Further information about businesses' obligations under the other relevant legislation can be found in the guidance produced by the Joint Money Laundering Steering Group (JMLSG) at www.jmlsg.org.uk.

Money Laundering Regulations 2007: What do businesses have to do?

General overview:

1.20 The Money Laundering Regulations 2007 (the regulations) require relevant businesses to:

- put in place checks, controls and procedures in order to anticipate and prevent money laundering or terrorist financing. Further information on establishing internal checks and controls can be found in chapter 3

- train staff in those procedures and in the law relating to money laundering and terrorist financing. Further information on staff training and awareness can be found in chapter 8

- appoint a nominated officer or money laundering reporting officer to receive and consider internal disclosures and to make suspicious

activity reports to SOCA. Where the business is a sole trader with no employees, the proprietor will be the person responsible for making the reports. Further information on the role of nominated officers can be found in chapter 4 and identifying suspicious activity in chapter 7

- put in place procedures to identify customers and verify the customer's identity before entering into a business relationship or transaction and to obtain information on the purpose or nature of the business relationship. These procedures are known in the regulations as 'customer due diligence' and also require businesses to conduct ongoing monitoring of the business relationship as appropriate. The regulations specify circumstances in which businesses are not required to undertake customer due diligence measures or must undertake enhanced measures. Further information about how and when to apply customer due diligence measures can be found in chapter 6

- keep records obtained in establishing customers' identity and of business relationships for five years. Further information on record keeping can be found in chapter 9.

1.21 The regulations introduce a risk based approach which means that businesses should implement these requirements based on the level of risk/ the likelihood they have identified that the business may be used to launder money or fund terrorism. Businesses should also identify the particular factors relating to transactions and relationships that may indicate an enhanced level of risk. Further information about how to establish a risk based approach to the prevention of money laundering and terrorist financing can be found in chapter 5.

Penalties for failure to comply with the regulations

1.22 Failing to comply with the regulations could lead to a prosecution which could result in unlimited fines and/ or a prison term of up to two years.

1.23 Failing to comply with the regulations could also result in civil financial penalties (a different sanction to prosecution leading to a fine).

Registration

1.24 The regulations also require a relevant business to register with its Supervisory Authority where registers are established. Separate guidance for estate agency businesses and consumer credit businesses will be available on how and when to register if OFT decides to establish registers. See www.oft.gov.uk/oft_at_work/markets/services/money-laundering/ for more details.

2 SENIOR MANAGEMENT RESPONSIBILITY

2.1 The regulations say that risk sensitive policies and procedures must be established in order to anticipate and prevent money laundering and terrorist financing.

2.2 A risk sensitive or risk based approach is where businesses assess the risk of customers laundering money through their business. Businesses may take the starting point that most customers will not launder money but will identify criteria which could indicate higher risk of money laundering and terrorist financing.

2.3 Senior managers (those responsible for running the business including company directors, company secretaries, Chief Executives, members of management committees, or anyone else acting in this capacity) are responsible for identifying and managing the risks of their business being used for money laundering and terrorist financing.

2.4 Senior managers are required to put in place mitigating policies and procedures in order to effectively manage the risks they have identified.

2.5 Documentation on the application of those policies should be kept and reviewed/ updated on a regular basis and all employees should be trained in those procedures.

2.6 Where the business is a sole trader or partnership, the proprietor, partners or those responsible for running the business will be the senior managers.

Senior management responsibility

2.7 Senior managers are responsible for:

- establishing and maintaining appropriate risk-sensitive policies and procedures

- ensuring employees are trained in and implement those procedures and are aware of the law relating to money laundering and terrorist financing

- appointing a nominated or money laundering reporting officer to receive and make suspicious activity reports to SOCA.

Policy Statement

2.8 The business should draft a statement of its anti-money laundering and counter terrorist financing policy and the procedures by which it intends to implement it. This will clarify how it intends to undertake its responsibility for the prevention of money laundering and terrorist financing.

2.9 This will provide direction to the business and its staff and will identify those responsible for implementing particular aspects of the policy.

2.10 The policy statement should also set out how senior managers undertake their assessment of the money laundering risks their business faces and how these should be managed.

2.11 Policy statements should not be generic but tailored to the circumstances of the business. Some of the types of information that businesses may consider appropriate to include in a policy statement are (this list is not exhaustive):

- summary of the culture and values to be adopted and promoted in the prevention of money laundering and terrorist financing

- commitment to staff training in the awareness of the law and their obligations

- allocation of responsibilities and functions to specific persons

- summary of the business's assessment of the risks it faces of being used to launder money or fund terrorism and the approach for mitigating the risks identified

- summary of procedures to be adopted and the monitoring arrangements to ensure the procedures are being carried out.

What are the risks businesses should be identifying?

2.12 These are likely to differ depending on the type of business and how the business operates. Chapter 5 provides more information about how to establish a risk based approach.

Offences and personal liability

2.13 Under the regulations an officer of a body corporate, a partner in a partnership or an officer of an unincorporated association will be individually liable for an offence under the regulations if:

- the officer consents to or is involved in committing the offence or
- where such an offence is due to neglect on his part.

2.14 An officer of a body corporate is a company director, company secretary, and other senior managers responsible for running the business such as Chief Executives, members of management committees or someone else acting in this capacity.

2.15 An officer of an unincorporated association is any officer of the association or any member of its governing body or someone else acting in this capacity.

2.16 If senior management fail to comply with the regulations they could be prosecuted which could result in an unlimited fine and or prison term of up to two years.

3 INTERNAL CONTROLS

3.1 Businesses are required to establish and maintain risk sensitive policies and procedures relating to:

- customer due diligence measures and ongoing monitoring
- reporting
- record keeping
- internal control
- risk assessment and management
- the monitoring and management of compliance with and internal communication of such policies and procedures.

3.2 Businesses are required to establish policies and procedures relating to internal systems, controls and communication in order to anticipate and prevent money laundering and terrorist financing.

3.3 The internal controls should be appropriate to the business taking account of the risks of money laundering and terrorist financing that the business faces.

3.4 In simple terms this means that business must ensure that checks are made to alert them to the possibility that criminals may be using the business to launder money or fund terrorism.

3.5 The checks and controls that are put in place will help businesses to identify suspicious activity - potential risky transactions or customer activity - and to judge whether a disclosure should be made to SOCA. Chapter 7 provides guidance on when, how and to whom to disclose suspicion.

3.6 The nature and extent of the internal controls will depend on a variety of factors:

- the type of business
- how the business operates
- and the likelihood (level of risk identified) that the business may be used to launder money.

3.7 Important elements of the internal controls will be appropriate risk sensitive monitoring processes and customer due diligence measures.

3.8 Businesses are required to carry out regular assessments of their systems and controls in order to ensure that they are working in practice.

3.9 Businesses must therefore put in place processes to monitor the effectiveness and implementation of their internal controls and where businesses identify any areas of weakness to document these and the action that is being taken to rectify the problem.

4 ROLE OF THE NOMINATED OFFICER

4.1 The regulations require relevant businesses to appoint a Nominated Officer, also sometimes known as a Money Laundering Reporting Officer (MLRO), who is responsible for:

- receiving internal suspicious transaction reports (also known as disclosures) from within the business
- deciding whether these should be reported to SOCA, and
- if appropriate making such reports to SOCA.

4.2 Sole traders with no employees are not required to appoint a nominated officer but are still required to make suspicious activity reports to SOCA. Sole traders with no employees, will be, by default, the nominated officer.

Internal Reports/ Disclosures

4.3 Internal reports or disclosures are reports of knowledge or suspicion of money laundering made by employees of the business to the nominated officer. Businesses should ensure that their staff know the name of the nominated officer to whom they should make those reports and receive training on when to make such reports.

4.4 Businesses should take steps to ensure that the internal reports are made and considered by the nominated officer as soon as reasonably practicable.

4.5 The nominated officer must consider each report and if the nominated officer concludes that the internal report does give rise to a knowledge or suspicion of money laundering or terrorist financing then he/ she must promptly make an external report to SOCA.

4.6 Nominated officers should retain copies of the internal reports and copies of the decisions taken on each of the reports. Chapter 7 provides detailed guidance on suspicious activity reporting.

5 RISK BASED APPROACH

5.1 A risk based or risk sensitive approach is where the business assesses the risks that it may be used for money laundering or terrorist financing and puts in place measures to manage and mitigate those risks.

5.2 Risk assessment is owned by the senior managers of the business. Chapter 2 explains more about senior management responsibilities.

How do businesses establish a risk based approach?

5.3 A risk based approach requires a number of discrete steps to be taken to determine the most cost effective and proportionate way to manage those risks:

- identify the risk of money laundering and terrorist financing that the business faces
- assess the risks posed by:
  - customers
  - products and services
  - delivery channels (such as in person/ online/ through third parties)
  - geographical areas of operation
- design and implement controls to mitigate these assessed risks
- monitor the effectiveness and implementation of the controls and make improvements where required
- record what has been done and why.

Assessing risk

5.4 The assessment of the risks that businesses face will depend on the type of business and how the business operates.

5.5 Businesses should decide for themselves how to carry out the risk assessment appropriate to their circumstances. They should assess risk in the context of how their business may be used by those involved in money laundering and terrorist financing.

5.6 In identifying and assessing the risks of money laundering and terrorist financing that the business faces, businesses may consider it appropriate to consider (this list is not exhaustive and will depend on how the business operates):

- what risk is posed by particular customers?

  - brand new customers carrying out large one off cash transactions
  - customers that are not local to the business
  - overseas customers
  - an individual in a public position and/ or a location that carries a higher exposure to the possibility of corruption (including politically exposed persons - see chapter 6)
  - complex business ownership structures with the potential for concealing beneficiaries

- is a risk posed by a customer's behaviour?

  - reluctance of the customer to provide identification or the evidence produced is unsatisfactory
  - where the customer appears to be acting on behalf of another person and is unwilling to give details of those they represent
  - transactions that do not appear to make commercial sense

- how does the way the customer comes to the business affect the risk?

- non face to face customers
- occasional transactions as opposed to ongoing business relationships

- does the pattern of behaviour or changes to it pose a risk?
- what risk is posed by the products/ services the customer is using?

- is the main risk that of inappropriate assets being placed with, or moving from, or through, the business?
- does the product allow payment to third parties?

Managing and mitigating risks

5.7 Once businesses have identified and assessed the risks of being used for money laundering and terrorist financing, they must ensure that they put in place procedures to reduce these risks.

5.8 The regulations require that customer due diligence measures are implemented on a risk sensitive basis depending on the type of customer, business relationship, product or transaction. Examples of risk sensitive controls include:

- introducing a customer identification/ verification programme that varies depending on the assessed level of risk
- requiring additional customer identity evidence in higher risk situations
- varying the level of monitoring of customer transactions and activities depending on the assessed level of risk or activities that might be unusual or suspicious.

5.9 This list is not exhaustive. Chapter 6 provides further guidance on customer due diligence measures.

5.10 Identifying a customer or transaction as high risk does not automatically mean that they are involved in money laundering or terrorist financing. Similarly identifying a customer or transaction as low risk does not mean that they are not involved in money laundering or terrorist financing.

5.11 Businesses should ensure that staff are alert to the risks of money laundering but also use experience and common sense in applying the business's risk based controls. Chapter 8 provides more information on staff training and awareness.

5.12 The risk assessment procedures and controls should be documented and kept under regular review.

Monitoring effectiveness of the controls

5.13 Businesses must put in place some means of assessing their controls to mitigate the risk of the business being used for money laundering and whether these are working effectively. They should periodically reassess such risks particularly in light of new product types or methods of business.

5.14 Where the business identifies areas for improvement these should be documented and the action to be taken should be recorded.

6 CUSTOMER DUE DILIGENCE

6.1 Businesses must put in place procedures to identify customers before entering into a business relationship (see below) or transaction. The customer due diligence measures require businesses to:

- identify customers and verify their identity
- identify where applicable the beneficial owner and take adequate measures on a risk sensitive basis to verify their identity
- obtain information on the purpose and intended nature of the business relationship
- conduct ongoing monitoring of the business relationship to ensure transactions are consistent with knowledge of the customer and risk profile
- maintain records of the checks.

6.2 Customer due diligence measures are also sometimes known as 'know your customer' measures.

Business relationship

6.3 The regulations define a business relationship as 'a business, professional or commercial relationship between a relevant person and a customer, which is expected by the relevant person, at the time when contact is established, to have an element of duration.'

Beneficial owner

6.4 Beneficial owners are the individuals who ultimately own or control the customer or on whose behalf a transaction or activity is being conducted.

6.5 In the case of bodies corporate and partnerships, a beneficial owner is any individual who:

- owns or controls over 25 per cent of the shares or voting rights or in the case of a partnership, more than 25 per cent of the capital or profits of the partnership, or

- exercises control over the management.

6.6 In the case of a trust, the beneficial owner includes:

- individuals with vested (certain) interests in 25 per cent or more of the capital of the trust property

- the class of individuals the trust was set up or operates for (for example 'homeless persons in London', 'deaf and blind persons', 'children living in the village of Ambridge' or 'A's children and grandchildren')

- individuals who exercise control over the trust.

6.7 In the case of other legal entities or arrangements which administer or distribute funds, the beneficial owner means:

- individuals who benefit from 25 per cent or more of the entity's property

- the class of individuals the entity was set up or operates for (see above for trusts)

- individuals who exercise control over 25 per cent or more of the entity's property.

6.8 In the case of an estate of a deceased person in the course of administration, the beneficial owner means:

- the executor (original or by representation) or administrator for the time being of a deceased person in England, Wales or Northern Ireland

- the executor for the purposes of the Executors (Scotland Act) 1900 in Scotland.

When must customer due diligence be applied?

6.9 Businesses are required to carry out these measures:

- when establishing a business relationship
- when carrying out an occasional transaction
- where there is a suspicion of money laundering or terrorist financing
- where there are doubts about previously obtained customer information
- at appropriate times to existing customers on a risk sensitive basis.

Timing

6.10 The verification of the customer's identity and, where applicable, the beneficial owner, should take place before entering into a business relationship or occasional transaction.

6.11 However, businesses can complete the verification during the establishment of the business relationship if:

- this is necessary not to interrupt the normal conduct of business, and
- there is little risk of money laundering or terrorist financing occurring.

Extent of customer due diligence measures

6.12 Customer due diligence measures must be decided upon on a risk sensitive basis depending on the type of customer, business relationship, product or transaction.

6.13 This means that businesses will need to consider the level of identification, verification and ongoing monitoring that is required depending on the assessed risks and should be able to demonstrate these procedures to the OFT and the TSS if required to do so.

Non compliance with customer due diligence

6.14 Where businesses are unable to comply with the customer due diligence measures, then the business must:

- not carry out a transaction with or for the customer through a bank account
- not establish a business relationship or carry out an occasional transaction with the customer
- terminate any existing business relationship with the customer
- consider whether to make a suspicious activity report.

Simplified due diligence

6.15 In certain circumstances businesses are not required to apply customer due diligence measures.

6.16 Businesses do not have to verify the identity of customers or beneficial owners or seek additional information about the nature or purpose of business relationships where:

- the customer is a credit or financial institution that is subject to the regulations
- the customer is situated outside the UK and is subject to equivalent money laundering regulation
- the customer is a listed company subject to disclosure provisions
- subject to conditions, the customer is an independent legal professional and the product is a pooled account held in a non EEA state with equivalent money laundering regulation to which the customer is subject
- the customer is a public authority in the UK

- the customer is a European Community institution
- the product or transaction fulfils certain conditions (see chapter 11 for further information)

6.17 Businesses are still required to conduct ongoing monitoring of the business relationship in line with the risks they have identified.

Enhanced due diligence

6.18 Businesses are required to undertake additional or enhanced customer due diligence measures on a risk sensitive basis. This means that in some circumstances businesses may decide that the standard evidence of identification that they require customers to provide is not sufficient and that extra information about a particular customer is required in certain circumstances.

6.19 The regulations prescribe certain circumstances where the business must undertake enhanced due diligence and ongoing monitoring on a risk sensitive basis:

- where the customer has not been physically present for identification, that is non face to face customers
- where the customer is a politically exposed person or an immediate family member or close associate of a politically exposed person (see 6.21 below)
- in respect of a correspondent banking relationship
- in situations which by their nature can present a higher risk of money laundering or terrorist financing.

Non face to face customers

6.20 Where the customer has not been physically present, businesses should take account of the increased risk by doing one or more of the following:

- obtaining additional information or evidence to establish the customer's identity

- undertaking additional measures to verify the documents supplied or requiring certification by a financial or credit institution

- ensuring that the first payment of the operations is carried out through an account with a credit institution in the customer's name.

Politically exposed persons

6.21 A politically exposed person (PEP) is an individual who has, or has had in the previous year, a high political profile, or holds, or has held in the previous year, public office overseas. Examples of PEPs include heads of state, heads of government, ministers, members of parliaments, members of supreme or constitutional courts or other high level judicial bodies, ambassadors and high ranking officers in the armed forces. The definition of PEPs extends to cover immediate family members and known close associates.

6.22 Businesses should ensure that they have procedures in place to identify whether the customer is a PEP and take steps to establish the source of their funds which will be used during the business relationship or transaction.

6.23 Businesses must put in place procedures for senior managers to approve the establishment of a business relationship with a PEP. Where a business relationship is entered into businesses should undertake enhanced ongoing monitoring of the relationship.

Persons that businesses must not accept as customers

6.24 The Government may direct businesses not to enter into business relationships or transactions with certain individuals who are subject to financial sanctions.

6.25 A list of all sanctions currently in force in the UK is maintained by HM Treasury. This list can be found at:

http://www.hm-treasury.gov.uk/financialsanctions

How do businesses identify their customers?

6.26 Identifying a customer is a two part process:

- first stage is identifying the customer by obtaining a range of information such as names, addresses, date of birth
- second stage is verifying this information through the use of reliable independent source documents, data or information.

6.27 Evidence of identity can be documentary or electronic and appropriate records should be kept. There is no requirement for businesses to keep a copy of the evidence seen. It is sufficient to record details of the evidence seen but those records should be robust enough to trace the original document at a later date. One example is recording a passport number and issuing authority.

6.28 Businesses may consider it appropriate to use electronic methods for checking customers' identity. Where they choose to do so, businesses should be satisfied that the information supplied is accurate and reliable.

6.29 The regulations provide that a business may rely on specified third parties to identify its customers if the third party consents. In addition a business may employ a third party to identify its customers. However in both cases the business will still be ultimately responsible for its customer identification obligations and the business should satisfy itself that appropriate identification has been made.

6.30 How much evidence of a customer's identity a business should ask for will depend on the level of risk identified for that customer, business relationship, product or transaction.

Private individuals

6.31 For customers that are private individuals the business should obtain:

- full names
- residential addresses
- date of birth

6.32 Verification of this information must be based on reliable independent sources. This may be by documents provided by the customer or information obtained electronically by the business or both.

6.33 If the verification of the customer's identity is done by documents this should be based on:

- A government issued document with the customer's full name and photo with either the customer's date of birth or residential address such as:

  - valid passport
  - valid photocard driving licence
  - national identity card
  - firearms certificate
  - identity card issued by the Electoral Office for Northern Ireland

- or, a government issued document (without a photo) which includes the customer's full name and **supported by** secondary evidence of the customer's address such as:

  - old style driving licence
  - recent evidence of entitlement to state or local authority-funded benefit such as housing benefit, council tax benefit, pension, tax credit

supported by secondary evidence such as:

- a utility bill
- bank, building society or credit union statement
- most recent mortgage statement from a recognised lender

6.34 Sufficient checks should be made of the documentary evidence to satisfy the business of the customer's identity. This may include checking spelling of names, validity, photo likeness, whether addresses match etc.

6.35 Where a member of the business's staff has visited the customer at his home address a record of this visit may constitute evidence of corroborating the individual's residential address (for the purposes of a second document).

6.36 If the verification of the customer's identity is done by electronic means the business should undertake these checks from two separate sources. A copy of the electronic check should be retained or information recorded as to where a copy of the evidence can be found.

Customers other than private individuals

6.37 For customers that are not private individuals, such as corporate customers, partnerships, and private companies, the business must obtain information that is relevant to that entity such as company registration number and registered address and evidence that individuals have the authority to act for that entity. It may be necessary to establish the beneficial owners of such entities.

6.38 Verification of identification must be from reliable independent sources (relevant to that entity type) such as a search of a relevant company registry, confirmation of the company's listing on a regulated market, or a copy of the company's certificate of incorporation.

How do businesses identify beneficial owners?

6.39 Businesses are required to put in place measures to identify the existence of a beneficial owner (see 6.4 – 6.8 above). Where businesses have reason to believe or suspect or have identified that a customer is controlled or owned by a beneficial owner they should verify the beneficial owner's identity on a risk-sensitive basis.

6.40 In verifying the beneficial owner's identity the business should be satisfied that they know who the beneficial owner is and understand how they operate. This may include finding out who has ownership or control over the funds, or who is the controlling mind.

6.41 On a risk sensitive basis the business should decide how they verify the identity of beneficial owners. This may include requiring the customer to provide information directly, making use of publicly available documents or verifying the identity of the beneficial owner by some other means.

7 SUSPICIOUS ACTIVITY REPORTING

7.1 The regulations require businesses to appoint an individual in their organisation as a nominated officer who is required to make reports to SOCA where he knows or suspects or has reasonable grounds for knowing or suspecting that a person is engaged in money laundering or terrorist financing.

7.2 Any staff in the business who know, suspect or have reasonable grounds for knowing or suspecting that a person is engaged in money laundering or terrorist financing must report such matters to the nominated officer as soon as possible. On receipt of a report it is for the nominated officer to decide whether a suspicious activity report needs to be made to SOCA.

7.3 Sole traders with no employees will be, by default, the nominated officer and will be responsible for making reports to SOCA where they know or suspect or have reasonable grounds for knowing or suspecting that a person is engaged in money laundering or terrorist financing.

What is suspicion?

7.4 Suspicion has its ordinary meaning. A report should be made if a member of staff/ the nominated officer thinks that there is a possibility, which is more than fanciful, that a person is or has been engaged in money laundering or terrorist financing.

How do businesses identify suspicious activity?

7.5 The systems that businesses put in place will help to identify suspicious activity. The kinds of activity that might be considered suspicious will depend on the type of business and how the business operates.

7.6 The following list gives some indicators of transactions or activity that might be considered suspicious but is not exhaustive:

New customers:

- checking the customer's identity is difficult
- the customer is reluctant to provide details of their identity
- the customer is trying to use intermediaries to protect their identity or hide their involvement
- there appears to be no genuine reason for the customer using the business's services.

Regular and existing customers:

- the transaction is different from the normal business of the customer
- the size and 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
- there has been a significant or unexpected improvement in the customer's financial position particularly where they are unable to give proper explanation of where the money came from.

Transactions:

- money is paid by a third party who does not appear to be connected with the customer
- the customer requests payment to a third party who has no apparent connection with the customer
- a cash transaction is unusually large and the customer will not disclose the source of the funds.

Internal reporting procedures (disclosures)

7.7 All businesses must maintain internal reporting procedures requiring their staff to report suspicious activity to the business's nominated officer as soon as is practicable and ensure that staff are fully appraised of and implement such procedures.

7.8 'As soon as reasonably practicable' means as soon as is reasonably possible once a decision has been made that there are grounds to suspect money laundering or terrorist financing. Internal reporting lines to the nominated officer should be short in order to avoid delay.

7.9 Before deciding whether to make a suspicious activity report (SAR) to SOCA the nominated officer must consider each internal report/ disclosure and decide whether it does give rise to a knowledge or suspicion of money laundering or terrorist financing.

7.10 Businesses should ensure that their nominated officer has access to all relevant records.

7.11 Until the nominated officer advises the member of staff that has made the internal report that no report is to be made to SOCA, further transactions or activity by that customer, whether the same or different in nature, should be reported to the nominated officer.

7.12 If the nominated officer decides not to make a report to SOCA the reasons for not doing so should be documented and retained with the internal report.

External Reporting Procedures

7.13 SOCA's preferred method of receiving a SAR is electronically through the SARS online system at www.soca.gov.uk

7.14 Where this route is not possible SARs should be made electronically through encrypted email links approved by SOCA or by post or fax using the standard forms. Where standard forms are used these should be typed or word processed to enable them to be scanned.

7.15 The basis for the knowledge or suspicion of money laundering or terrorist financing should be contained in the SAR and should also include as much relevant information about the customer, transaction or activity as the business has on its records.

7.16 The nominated officer or sole trader must report suspicious approaches even if no transaction takes place.

7.17 Where a SAR is sent after a transaction has taken place businesses will be able to continue to do business with the customer subject to their risk assessment procedures.

Before the transaction is complete/ consent from SOCA

7.18 When a customer's transaction raises grounds of suspicion of potential money laundering, before that transaction is complete, businesses must submit a SAR to SOCA seeking consent to proceed with the transaction.

7.19 In such circumstances the SAR should be marked with 'CONSENT' and 'TRANSACTION NOT COMPLETE'. In urgent cases SOCA can be contacted by telephone to request consent.

7.20 SOCA will notify its decision as soon as possible. It is an offence for the nominated officer or sole trader to proceed with a transaction if consent has been requested but not yet granted within the seven working day period beginning the day after the SAR is submitted.

7.21 If no response from SOCA is received after the seven day period businesses may proceed with the transaction. If SOCA refuses to provide consent businesses are prevented from proceeding with a transaction for up to a further thirty one calendar days.

Tipping off

7.22 It is a criminal offence for anyone following a disclosure to the nominated officer to say or do anything that may 'tip off' another person that the disclosure has been made or prejudice an investigation.

7.23 Businesses can not tell a customer that:

- the transaction is being or was delayed because a disclosure has been made
- details of their transaction has or will be reported to SOCA
- they are being investigated by law enforcement agencies.

8 STAFF AWARENESS AND TRAINING

8.1 Businesses are required to take appropriate measures to ensure that all relevant staff members are aware of and have received training in:

- the law relating to money laundering and terrorist financing and their obligations under that legislation, and
- how to recognise and deal with suspicious transactions and activity.

8.2 One of the most important controls over the prevention and detection of money laundering is to have staff who are alert to the risks of money laundering and trained in identifying potential suspicious transactions.

8.3 Failures in staff training could give employees a defence of not knowing what is required and could leave businesses open to penalties or prosecutions.

8.4 Staff training should cover:

- the relevant money laundering legislation including the regulations, Part 7 of The Proceeds of Crime Act 2002 and sections 18 and 21A of The Terrorism Act 2000
- the business's policies and procedures in relation to the prevention of money laundering and terrorist financing
- the assessment of risks that money laundering poses to the business
- employees' responsibilities for the prevention of money laundering and terrorist financing
- identification and verification of customers' identity (customer due diligence) procedures
- how to recognise and handle suspicious transactions and activities and how this may depend on the product or service in question

- name and responsibility of the nominated officer and procedures for making an internal report or disclosure of suspicious activity to the nominated officer including obtaining consent from SOCA and the need to keep that information confidential

- record keeping.

8.5 Businesses should ensure that the content and frequency of the training reflect the business's assessment of its risk.

8.6 Training should also be tailored to staff responsibility and all new staff should be given training before they start work. Ongoing training should be given to all staff on a regular basis.

8.7 It is recommended that a business keeps records of the training that its staff have received and that it confirms with staff members that they have understood the training. Businesses should also take steps to assess the effectiveness of the training provided.

8.8 Staff should also be informed of the procedures to be adopted for monitoring compliance with the business's policies and procedures for ensuring compliance.

9 RECORD KEEPING

9.1 Businesses are required to keep certain records:

- copies of, or references to, the evidence obtained of a customer's identity for five years after the end of the customer relationship, or
- in the case of occasional transactions, five years from the date when the transaction was completed.

9.2 In relation to customer identification businesses must keep:

- a copy of or details about the identification document presented and verification evidence obtained, or
- information about where the evidence can be obtained.

9.3 If the business employs a third party to undertake its customer due diligence measures the business must ensure that the third party complies with the record keeping obligations.

9.4 The purpose of keeping these records is to demonstrate the business's compliance with the regulations and to aid any resulting investigations.

9.5 Records can be kept in a variety of methods such as original documents, photocopies of original documents, in computerised or electronic form. Businesses may also keep references as to where original documents can be found. How the records are retained will depend on how the business operates.

9.6 Businesses should also keep records of internal and external reports and decisions as part of the suspicious activity reporting. Chapter 7 outlines the requirements on business.

10 ESTATE AGENTS

10.1 Estate agents are required to comply with the regulations and are supervised by the OFT.

10.2 Estate agent means 'a firm or sole practitioner, who or whose employees, carry out estate agency work (within the meaning given by section 1 of the Estate Agents Act 1979 (estate agency work)), when in the course of carrying out such work.'

10.3 This means that anyone who engages in estate agency work within the meaning of section 1 of the Estate Agents Act 1979 must comply with the regulations. This will include internet property retailers, home information pack providers and housing associations to the extent that they engage in estate agency work but only in relation to that work.

What is estate agency work?

10.4 Under section 1 of the Estate Agents Act 1979 estate agency work includes:

- introducing and/ or negotiating with people who want to buy or sell freehold or leasehold property (or their Scottish equivalents) including commercial or agricultural property
- where this is done in the course of a business
- pursuant to instructions from a client.

Estate agents' employees and the Money Laundering Regulations 2007

10.5 Employees of estate agents who carry out estate agency work are not themselves individually supervised by the OFT but their employers will be estate agents in connection with any such work done by the employee and responsible for their compliance with the regulations.

Lettings agents

10.6 Lettings agents will not be supervised by the OFT unless and to the extent that they engage in estate agency work. Lettings agents do have obligations under the Proceeds of Crime Act 2002.

Customer due diligence

10.7 Chapter 6 sets out businesses' obligations to identify and verify a customer's identity before entering into a business relationship or transaction. For estate agents, the obligation under the regulations is to identify clients. This will usually be sellers (vendors).

10.8 Whilst estate agents are required to only undertake customer due diligence measures for sellers when acting as their agents, best practice would be to identify the purchaser in addition to the seller once an offer has been accepted.

Suspicious behaviour

10.9 Chapter 7 outlines regulated businesses' obligations to report suspicious activity to SOCA. The following list gives some indicators of some transactions or activity specific to estate agency work that may be considered suspicious. It is not exhaustive and further indicators can be found at 7.6 above:

Unusual instructions:

- a client has no apparent reason for using the firm (for example the scale of the transaction or location of the property or type of business indicates that another firm would be better placed to act).

Transactions:

- a transaction is carried out for less than market value with an unconnected person (for example the estate agent or auctioneer may be asked to offer a property at auction at a level below the market)

- settlements in cash after a large property transaction
- a client requests the estate agent or auctioneer to hold large sums of money in its client account for no apparent reason
- a client withdraws from a transaction after paying money into the client account which was to be used in relation to the transaction.

11 CONSUMER CREDIT FINANCIAL INSTITUTIONS

11.1 Consumer Credit Financial Institutions (CCFIs) must comply with the regulations and are supervised by the OFT.

What is a CCFI?

11.2 A CCFI is a consumer credit lender who is not authorised by the FSA.

11.3 As a consumer credit lender the business should hold a category A consumer credit licence. If they do not have a licence they should apply. The regulations cover those who are licensable whether they have a current licence or not.

11.4 Information on how to apply for a licence can be found at:

www.oft.gov.uk/advice_and_resources/resource_base/credit-licence/

What about multiple category licences?

11.5 If you hold a multiple category consumer credit licence which includes category A you may be a CCFI if you engage in lending and do not fall into 11.8 – 11.10 below.

My licence includes Category A but I am not engaged in lending

11.6 If despite holding a category A licence you do not engage in lending you will not be a CCFI.

My licence does not include Category A and I do not engage in lending

11.7 If you hold a consumer credit licence, but not for category A, and do not engage in lending you will not be a CCFI and will not be supervised by the OFT. However you may still fall within the regulations but be supervised by another authority.

Group Licences

11.8 A person who is covered by a Group licence under section 22 of the Consumer Credit Act 1974 is not a CCFI.

Who is not a CCFI?

11.9 Any business which is authorised by the FSA is not a CCFI even if it meets all the criteria outlined above. Such businesses will still be bound to comply with the regulations but will be supervised by the FSA rather than the OFT.

11.10 Any business which is a credit institution as defined in the regulations is not a CCFI. Credit institutions are defined in Article 4(1)(a) of the Banking Consolidation Directive and include institutions with branches in an EEA state when they accept deposits from the public or grant credit for their own account within the meaning of the directive.

11.11 A money service business is not a CCFI. A money service business means 'an undertaking which by way of business operates a currency exchange office, transmits money...by any means or cashes cheques which are made payable to customers'.

11.12 This guidance is not intended for businesses that are supervised by the FSA, HMRC or other supervisory authorities. If you are not a CCFI but believe that you still fall within the regulations and are unsure who your Supervisory Authority is please see 'who is my supervisor?' flowchart for further information. Businesses engaged in multiple activities that fall under the regulations may also find it helpful to refer to this information.

Customer due diligence

11.13 Chapter 6 sets out businesses' obligations to identify and verify customers' identity before entering into a business relationship or transaction.

11.14 Customer due diligence measures must be decided upon on a risk sensitive basis. The regulations also provide for certain circumstances

where businesses are not required to apply customer due diligence measures, known as 'simplified due diligence'.

11.15 Where CCFIs offer products or engage in transactions that fulfil all of the following criteria they will be able to apply simplified due diligence to such transactions:

- the product has a written contractual basis
- any related transaction is carried out through the customer's account with a credit institution subject to anti-money laundering regulation
- the product is not anonymous
- the transaction does not exceed 15,000 euro maximum threshold
- benefits of the product can not be realised by a third party
- in relation to products allowing for investment of funds in financial assets or claims, the benefits of which are only realisable in the long term, and where the product cannot be used as collateral and where no accelerated payments, surrender clauses or early termination can take place.

11.16 Even so businesses must apply customer due diligence measures where they suspect money laundering or terrorist financing.

11.17 Businesses are also required to conduct ongoing monitoring of the business relationship in line with the risks they have identified.

Suspicious behaviour:

11.18 Chapter 7 outlines regulated businesses' obligations to report suspicious activity to SOCA. The following list gives some indicators of some transactions or activity specific to consumer credit lenders that may be considered suspicious. It is not exhaustive and further indicators can be found at 7.6 above:

Transactions:

- acceleration of agreed repayment schedule for example by lump sum repayments or early termination
- early repayment
- quick churn of borrowing and repayment
- cash repayments (where this is different from the normal course of the business)
- the customer has no apparent reason for using the firm (for example un-commercial lending and borrowing)

Existing customers:

- change in patterns of behaviour
- peaks of borrowing and quick repayment (for example to purchase high value items which are quickly sold on)

12 FURTHER INFORMATION

OFT's supervisory role:

12.1 Further information on OFT and the TSS supervisory role under the Money Laundering Regulations 2007 can be found on the OFT website at: www.oft.gov.uk/oft_at_work/markets/services/money-laundering/

12.2 You can also contact us at:

Office of Fair Trading

Fleetbank House

2 – 6 Salisbury Square

London EC4Y 8JX

Tel: 08457 22 44 99

Email: enquiries@oft.gsi.gov.uk

OFT Publications:

12.3 The estate agency guide – what you need to know if you are engaged in estate agency work (OFT 031)

12.4 Do you need a credit licence? An introduction to consumer credit licensing (OFT147)

12.5 OFT publications can be obtained free of charge from:

Office of Fair Trading
PO Box 366
Hayes UB3 1XB

Tel: 0800 389 3158

Serious Organised Crime Agency (SOCA):

12.6 Further information on making suspicious activity reports can be found on SOCA's website at: www.soca.gov.uk

12.7 SOCA can also be contacted at:

UKFIU
PO Box 8000
London SE11 5EN

Tel: 020 7238 8282