Money Laundering Regulations 2007

Supervision of Money Service Businesses

Contents

1. Introduction: money laundering and Money Service Businesses

1.1 Money laundering includes how criminals change money and other assets into clean money or assets that have no obvious link to their criminal origins.

1.2 Money laundering takes many forms. Here are some examples detected by HM Revenue and Customs in each sub-sector:

- money transmission can involve placing illegal cash with a Money Service Business, or enabling the transfer of value by netting-off transactions in different countries without moving any money - a common practice is to split transactions into small sums
- third party cheque cashing has been exploited by some traders to evade a ban on paying cash for scrap metal
- currency exchanges are exploited to change small denomination notes into large denominations in another currency to enable easier and cheaper handling of large quantities of illegal cash - once the money has been exchanged, it's difficult to trace its origin

Terrorist financing

1.3 Terrorist financing involves dealing with money or property that you've reasonable cause to suspect may be used for terrorism. The funds and property may be from legitimate sources or criminal sources. They may be in small amounts.

Legislation

1.4 The main UK legislation covering anti money laundering and counter-financing of terrorism is:

- Proceeds of Crime Act 2002
- Terrorism Act 2000
- Money Laundering Regulations 2007

1.5 The following legislation applies to money transmission businesses only:

- The Transfer of Funds (Information on the Payer) Regulations 2007 No 3298
- Regulation (EC) No 1781/2006 on information on the payer accompanying transfers of funds (the Payments Regulation)

1.6 The Proceeds of Crime Act 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

The primary money laundering offences apply to everyone.

1.7 The Proceeds of Crime Act also creates offences of failing to make a report about suspicious activity, and tipping off any person that you've made, or intend to make, such a report. This applies to businesses in the regulated sector, such as Money Service Businesses.

1.8 The Terrorism Act sets out the primary offences relating to terrorist funding. Regulated businesses like Money Service Businesses must report a belief or suspicion of offences related to terrorist financing, such as:

- 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

1.9 The Money Laundering Regulations set out what relevant businesses such as Money Service Businesses must do to prevent the use of their services for money laundering or terrorist financing purposes. This guidance focuses mainly on the Money Laundering Regulations.

1.10 The Transfer of Funds Regulations and the associated European Union Regulation on the transfer of funds set out what information money transmission businesses must send when they arrange a transfer of funds.

Meaning of words

1.11 In this guidance, the word 'must' denotes a legal obligation. Each chapter summarises the legal obligations under the heading 'minimum requirements', followed by the actions required to meet the legal obligations. The word 'should' is a recommendation of good practice, and is the standard that HMRC expects to see. HMRC will expect you to be able to explain the reasons for any departures from that standard.

1.12 'Money Service Business' is the term used to describe the following activities, carried out by way of business in the UK:

- acting as a currency exchange office (a bureau de change)
- transmitting money or any representation of money by any means (money remittance)
- cashing cheques payable to your customer (third party cheque cashing)

1.13 Money Service Businesses must comply with the Money Laundering Regulations. They must not carry on business as a Money Service Business unless they register with HMRC. If you're unsure whether you need to register with HMRC, please refer to the registration guidance. Money transmission businesses must also register with the Financial Conduct Authority under the Payment Services Regulations 2007.

1.14 This guidance is for Money Service Businesses who are supervised by HMRC for compliance with the Money Laundering Regulations. However, if a firm is authorised by the Financial Conduct Authority under the Financial Services and Market Act 2001 and provides currency exchange, money transmission or cheque cashing services in addition to other financial or credit services; then they will be supervised by the Financial Conduct Authority for all of their activities under the Money Laundering Regulations. The Joint Money Laundering Steering Group (JMSLG) has produced equivalent guidance for firms supervised by the Financial Conduct Authority; and that guidance has also been approved by HM Treasury for the purposes of Regulation 43(3) of the Money Laundering Regulations. Authorisation for the purposes of Financial Services and Market Act 2001 is different from being authorised as a payment institution by under the Payment Services Regulations 2009.

Penalties

1.15 If a person fails to comply with the Money Laundering Regulations, they may face a civil financial penalty or criminal prosecution that could result in an unlimited fine and/or a prison term of up to 2 years.

Status of this guidance

1.16 HM Treasury has approved this guidance for the purposes of Regulation 42(3) of the Money Laundering Regulations. This means that HMRC and the courts will consider whether a person has followed this guidance when deciding whether they have failed to comply with the Regulations.

1.17 The parts of the guidance that deal with the Proceeds of Crime Act (2000) have been approved by HM Treasury for the purposes of section 330(8) of that act, and the guidance which deals with the Terrorism Act (2000) has also been approved by HM Treasury for the purposes of section 21A(6) of that act.

1.18 This guidance replaces HMRC's anti money laundering guidance for Money Service Businesses MLR8 July 2010. The guidance is effective from 8 August 2014.

Further sources of guidance

You can contact HMRC by telephone and email.

1.19 The Joint Money Laundering Steering Group (a group made up of trade associations in the financial services industry) also publishes free detailed guidance. The guidance is for members of the trade associations and firms supervised by the Financial Conduct Authority, for compliance with the Money Laundering Regulations. However, some of the sections in Part 1 of the guidance may be particularly relevant to Money Service Businesses. They contain detailed coverage of how to do due diligence checks on different types of customers, report suspicious activity and do staff training and record keeping.

1.20 The Joint Money Laundering Steering Group has also produced guidance for banks on the treatment of Money Service Businesses as customers.

2. Responsibilities of senior managers

2.1 The senior managers of a Money Service Business are personally liable if they don't take the steps necessary to protect their business from money laundering and terrorist financing.

2.2 You're a senior manager if you're a director, manager, secretary, chief executive, member of the management committee, or someone who carries out those functions, or any partner in a partnership, or a sole proprietor.

Minimum requirements

Senior managers must:

- identify, and manage effectively, the risks that their business may be exploited to launder money or finance terrorists
- take a risk-based approach that focuses more effort on higher risks
- appoint a nominated officer to report suspicious activity
- devote enough resources to deal with money laundering and terrorist financing

Actions required

Senior managers must:

- carry out a risk assessment identifying where your business is vulnerable to money laundering and terrorist financing
- prepare a policy statement and procedures to show how the business will manage the risks of money laundering and terrorist financing identified in risk assessments
- make sure there are enough trained people equipped to implement the policy adequately, and systems to help them
- monitor effectiveness of the business's policy and controls and make improvements where required

Responsibilities

2.3 Senior managers are responsible for making sure that the business has risk-based policies and procedures to help reduce the risk that criminals may exploit the business for financial crime. Your policies and procedures must address the level of risk that the business may encounter in different circumstances (see Chapter 3 on policies and procedures). When higher risks are identified, you must take extra measures (see Chapter 4 on customer due diligence), and consider whether to report suspicious activity (see Chapter 5 on reporting suspicious activity).

Policy statement

2.4 Your policy statement should make clear how you'll prevent money laundering and terrorist financing, by setting down your policies and procedures in writing.

2.5 Your policy must explain how you and other senior managers will assess risks to the business, notably how you and they will:

- identify, monitor and mitigate the risks of the business being used for money laundering or terrorist financing
- assign responsibilities to specific individuals and functions
- do due diligence checks and ongoing monitoring
- appoint a nominated officer or money laundering reporting officer to receive reports of suspicious activity from staff and make suspicious activity reports to the National Crime Agency
- make sure the staff are trained to recognise risks and understand what they should do, including the importance of reporting suspicious activity to the nominated officer
- maintain accurate, up-to-date record keeping and retention of records

2.6 The policy statement of a larger business should also include:

- the senior staff member who has responsibility for monitoring the effectiveness of the policy, including regular reviews to learn from experience
- individual staff responsibilities under the Regulations
- the process for reviewing and updating the business's policies and procedures
- the process for auditing the business's compliance with its policies and procedures
- the names of the nominated officer and any deputy

Appointing a nominated officer for the business

2.7 You must appoint a nominated officer to receive reports of suspicious activity from within the business and decide whether to report them to the National Crime Agency. You should also appoint a deputy to act in the absence of the nominated officer. If you're a sole trader with no employees you'll be the nominated officer by default, and must report suspicious activity to the National Crime Agency.

2.8 You should make sure that your staff know the name of the nominated officer and receive training on when and how to report their suspicions to the nominated officer (see Chapter 5 on reporting suspicious activity).

Personal liability

2.9 You'll be committing a crime if you don't comply with the Regulations. You may incur an unlimited fine and/or a prison term of up to 2 years if:

- you agree to, or are involved in committing a crime
- a crime is committed because of your neglect

3. Policies and procedures

Minimum requirements

The senior managers must put in place appropriate policies and procedures that reflect the degree of risk associated with the business and its customers. These are:

- customer due diligence measures and ongoing monitoring
- reporting suspicious activity
- record keeping
- internal controls
- risk assessment and management
- monitoring and managing compliance
- internal communication of these policies and procedures, including to any branches and subsidiaries outside the UK
- staff training

You must take into account situations that, by their nature, can present a higher risk of money laundering or terrorist financing, and take enhanced measures to address them. The specific measures depend on the type of customer, business relationship, product or transaction, especially large or complex transactions or unusual patterns of activity that have no apparent economic or lawful purpose.

Actions required

The following actions are also required and must be kept under regular review:

- carry out a formal, regular assessment of money laundering/terrorist financing risks, including market changes, and changes in products, customers and the wider environment
- ensure internal procedures, systems and controls, including staff awareness, adequately reflect the risk assessment
- ensure customer identification and acceptance procedures reflect the risk characteristics of customers
- take further measures for higher risk situations
- ensure arrangements for monitoring systems and controls are robust, and reflect the risk characteristics of customers and the business
- carry out regular assessments of your systems and internal controls to make sure they are working

Where you spot any weakness, you should document it and record the action taken to put the problem right.

Risk-based approach

3.1 A risk-based approach is where you assess the risks that your business may be used for money laundering or terrorist financing, and put in place appropriate measures to manage and lessen those risks.

3.2 Several features of the Money Service Business sector make it attractive to criminals, such as its worldwide reach (in the case of money remitters), the ease of making cash transactions, the one-off nature of many transactions, and the speed, simplicity and certainty of transactions.

3.3 A risk-based approach should balance the costs to your business and customers with a realistic assessment of the risk that criminals may exploit the business for money laundering and terrorist financing. It allows you to focus your efforts on the most important areas and reduce unnecessary burdens.

3.4 This chapter covers the risks for Money Service Businesses in general. Chapter 9 sets out in more detail the specific risks that apply to different types of Money Service Businesses.

Your risk profile

3.5 You must be able to understand all the ways that your business could be exposed to money laundering and terrorism financing risks, and design systems to deal with them. This means that you must:

- identify the risks of money laundering and terrorist financing that are relevant to your business - in other words, your business's risk profile
- assess the risks posed by your particular:
    - customers and any underlying beneficial owners (see the section on customer due diligence on who is the beneficial owner)
    - services
    - financing methods
    - delivery channels, for example cash over the counter, wire transfer or cheque
    - geographical areas of operation, including sending money to, from or through high risk countries, for example countries identified by the Financial Action Task Force (FATF) as having deficient systems to prevent money laundering or terrorist financing
- 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

3.6 Assessing your business's risk profile will help you understand the risks to your business and how they may change over time, or in response to the steps you take. This will help you design the right systems that will spot suspicious activity, and ensure that staff are aware of what sort of money laundering activities they are likely to encounter.

3.7 The risk profile depends on the nature of the business, branch network, customers, and activities. For each of these areas you should consider how they could be exposed, for example through the following questions. This generalised list is not exhaustive and will depend on individual business circumstances. (See Chapter 9 on risk indicators for each type of Money Service Business.)

Managing a branch network

If you manage a branch network these are some of the questions to consider to help inform your risk profile:

- how will you apply risk management procedures to a network of branches
- how will you manage and maintain records, what type of records
- if you selected a number of customer files at random, would they all have a risk assessment and adequate customer due diligence for the customers and beneficial owners
- do you have a system that will pick up where individuals, departments or branches are not implementing risk management procedures
- could you demonstrate that all staff have been trained on the Regulations and the business's procedures, and given ongoing training on recognising and dealing with suspicious transactions
- if asked, will staff know who the nominated officer is, what the firm's policies are and where they can be found

Customers

These are some of the questions to consider to help inform your risk profile in relation to your customers:

- how does the way the customer comes to the business affect the risk for
    - non face-to-face customers
    - occasional transactions, as opposed to ongoing business
- does the pattern of behaviour, or changes to it, pose a risk
- are customers companies, partnerships, or trusts
- do you undertake business in areas with a highly transient population
- is the customer base stable or does it have a high turnover
- do you act for international customers or customers you don't meet
- do you accept business from abroad, particularly tax havens, or countries with high levels of corruption, or where terrorist organisations operate
- do you act for entities that have a complex ownership structure or a cross border element
- do you accept payments that are made to or received from third parties
- which customers should be looked at more carefully
    - customers carrying out large one-off cash transactions
    - customers that are not local to the business
    - overseas customers
    - individuals in public positions and/or locations that carry a higher exposure to the possibility of corruption, including politically exposed persons (see 8.13 on politically exposed persons)
    - complex business ownership structures with the potential for concealing beneficiaries
    - customers carrying out frequent low value transactions (see 4.31 to 4.35 on linked transactions)
    - customers sending money to high risk countries

3.8 When designing systems to identify and deal with suspicious activity, here are some warning signs of potentially suspicious activity that your systems should be capable of picking up and flagging for attention. Again, this is not an exhaustive list, and these signs aren't always suspicious. It depends on the circumstances of each case.

New customers

These are some of the questions to consider when you take on new customers to help inform your risk profile:

- checking the customer's identity is difficult
- the customer is reluctant to provide details of their identity or provides fake documents
- the customer is trying to use intermediaries to protect their identity or hide their involvement
- no apparent reason for using your business's services - for example, another business is better placed to handle the transaction
- part or full settlement in cash or foreign currency, with weak reasons

Regular and existing customers

These are some of the questions to consider to help inform your risk profile in relation to your regular and existing customers:

- the transaction is different from the normal business of the customer
- the size and frequency of the transaction is different from the customer's normal pattern
- the pattern has changed since the business relationship was established
- there has been a significant or unexpected improvement in the customer's financial position
- the customer can't give a proper explanation of where money came from

Transactions

These are some of the questions to consider to help inform your risk profile in relation to the transactions you carry out:

- a third party, apparently unconnected with the customer, bears the costs, or otherwise pays the transaction costs
- an unusually big cash or foreign currency transaction
- the customer won't disclose the source of the funds
- unusual involvement of third parties, or large payments from private funds, particularly where the customer appears to have a low income
- unusual source of funds

Procedures and controls

3.9 Once you've identified and assessed the risks and warning signs, you must ensure that you put in place appropriate procedures and controls to reduce them. They'll help to decide the level of due diligence to apply to each customer and beneficial owner. It's likely that there will be a standard level of due diligence that will apply to most customers, based on your business's risk profile.

3.10 Procedures should be easily accessible to staff and detailed enough to allow staff to understand and follow them easily. They should set out:

- the types of customers and transactions that you consider to be lower risk and those that qualify for simplified due diligence and those that are higher risk and merit closer scrutiny
- how to do customer due diligence, the identification requirements for customers and beneficial owners and how to do enhanced due diligence on higher risk customers
- any other patterns or activities that may signal that money laundering or terrorist financing is a real risk
- how to keep records, where and how long they should be kept
- how to conduct ongoing monitoring of transactions and customers
- clear staff responsibilities and the name and role of the nominated officer
- how policies and procedures will be reviewed
- how to report suspicious activity to the nominated officer, and how the nominated officer should make a report to the National Crime Agency

3.11 Examples of risk-based controls include:

- introducing a customer identification and 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

This list is not exhaustive. You could also have other risk-based controls. For more guidance see Chapter 4 on customer due diligence.

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

Effectiveness of the controls

3.13 Managing the money laundering and terrorist financing risks to your business is an ongoing process, not a one-off exercise.

3.14 You should document the risk assessment procedures and controls, such as internal compliance audits, as this helps to keep them under regular review. You should have a process for monitoring whether they are working effectively, and how to improve them, for example to reflect changes in the business environment, such as new product types or business models.

4 Customer due diligence

Minimum requirements

You must:

- do customer due diligence when you:
    - suspect money laundering or terrorist financing
    - set up a business relationship with a customer
    - carry out an occasional transaction
    - have doubt about any information provided by the customer for identification or verification
- have systems to identify those who can't produce standard documents
- do enhanced due diligence to take account of the greater potential for money laundering in higher risk cases, specifically when the customer is not physically present when being identified, and in respect of politically exposed persons
- not deal with certain persons or entities if you can't do due diligence, or the results are not satisfactory
- have a system for keeping customer information up-to-date
- be able to demonstrate to HMRC that the measures you take are appropriate

4.1 You must check that customers are who they say they are. This is often referred to as 'know your customer', or customer due diligence. This chapter explains the minimum requirements and actions you need to take to do customer due diligence in relation to:

- customers, who may be individuals or businesses in or outside the UK
- beneficial owners
- business relationships
- occasional transactions
- politically exposed persons

These terms are explained below:

The customer

4.2 The customer is the person or entity with whom the Money Service Business forms a contractual relationship. This is the individual or company sending money, exchanging currency, or cashing a cheque made out to them.

4.3 If you accept business from another Money Service Business, either as a currency wholesaler or as a money transmitter acting as an intermediary in a money remittance chain, the Money Service Business from whom you accept business is your customer, and the owners or controllers of the Money Service Business with which you're doing business are beneficial owners. This is explained further in the sections on beneficial owners, below, and on undertaking transactions with other Money Service Businesses that are not agents in section 8.16.

4. 4 If you're a business providing money transmission as part of an escrow service for two other parties, both those parties to a transaction are your customers. For example, if you facilitate a payment between a payer and a payee, both the payer and the payee are your customers, and you must apply customer due diligence to each of them.

Beneficial owner

4.5 Beneficial owners are the individuals who ultimately own or control the customer, or on whose behalf a transaction or activity takes place.

4.6 For a corporate body or partnership, a beneficial owner is any individual who:

- owns or controls over 25% of the shares or voting rights or in the case of a partnership, more than 25% of the capital or profits of the partnership; or
- exercises control over the management

4.7 For a trust, a beneficial owner includes:

- individuals with interests in 25% or more of the capital of the trust property
- individuals who exercise control over the trust
- the class of individuals that the trust acts for (for example 'homeless persons in London', 'deaf and blind persons', 'children living in the village of Ambridge' or 'someone's children and grandchildren')

4.8 For other legal entities, or arrangements that administer or distribute funds, a beneficial owner includes:

- individuals who benefit from 25% or more of the entity's property
- individuals who exercise control over 25% or more of the entity's property
- the class of individuals the entity acts for

Business relationship

4.9 A business relationship is a business, professional or commercial relationship between a Money Service Business and a customer, which the business expects, on establishing the contact, to have an element of duration. For example, a business relationship for a Money Service Business exists where:

- another Money Service Business is your customer
- you set up a customer account
- there's a contract to provide regular services
- you give preferential rates to repeat customers
- any other arrangement facilitates an ongoing business relationship or repeat custom, such as providing a unique customer identification number for the customer to use

Ongoing monitoring of a business relationship

4.10 You must continue to monitor a business relationship after it is established. This means you must monitor transactions, and where necessary the source of funds, to ensure they are consistent with what you know about the customer and the customer's business and risk profile. Examples of ongoing monitoring under different business models are set out in Chapter 8.

4.11 You must also keep the information you collect for this purpose up-to-date.

Occasional transaction

4.12 An occasional transaction is a transaction of €15,000 or more (or the sterling equivalent) that is not part of an ongoing business relationship, It also applies to a series of transactions totalling €15,000 or more, where there appears to be a link between transactions (linked transactions).

Politically exposed persons

4.13 A politically exposed person is typically one who has been entrusted with one of the following functions in the past year in a state other than the United Kingdom:

- heads of state, heads of government, ministers and deputy or assistant ministers
- members of parliaments
- members of supreme courts, of constitutional courts or of other high level judicial bodies
- members of courts of auditors or of the boards of central banks
- ambassadors, chargés d'affaires and high ranking officers in the armed forces
- members of the administrative, management or supervisory bodies of state-owned enterprises

or an immediate family member or business associate of any of the above.

General customer due diligence

4.14 You must do customer due diligence when:

- establishing a business relationship
- carrying out an occasional transaction
- you suspect money laundering or terrorist financing
- you suspect that information obtained for due diligence checks on a customer is not reliable or adequate

4.15 Customer due diligence means:

- identifying customers and verifying their identity (more details below)
- identifying the beneficial owner of the customer, where applicable, and taking adequate risk-based measures to verify their identity
- obtaining information on the purpose and intended nature of a business relationship
- conducting ongoing monitoring of a business relationship, to ensure transactions are consistent with what the business knows about the customer, and the customer's risk profile
- maintaining records of these checks

Extent of customer due diligence measures

4.16 The extent of customer due diligence measures depends on the degree of risk. It depends on the type of customer, business relationship, product or transaction as described in the risk profile section of Chapter 3. It goes beyond simply carrying out identity checks to understanding who you're dealing with. This is because even people you already know well may become involved in illegal activity at some time, for example if their personal circumstances change or they face some new financial pressure. Your due diligence measures should reduce the risk of this, and the opportunities for staff to be corrupted. This is covered in more detail below, and in the chapters on principal-agent relationships and risk indicators.

4.17 This means that you must consider the level of identification, verification and ongoing monitoring that's necessary, depending on the risk you assessed. You should be able to demonstrate that the extent of these procedures is appropriate when asked to do so.

Simplified due diligence

4.18 Sometimes your business may do a simplified form of due diligence. In these cases, you don't have to verify a customer's or beneficial owner's identity; and you don't have to ask for additional information about the nature or purpose of a business relationship, unless there's an increased risk of money laundering or terrorist financing.

4.19 Simplified due diligence is permitted if the customer is:

- a public authority in the UK
- a financial institution that is itself subject to the Money Laundering Regulations or equivalent regulation in another country; situated outside the UK, and is subject to equivalent money laundering regulation in another country
- a listed company that is subject to disclosure provisions
- beneficial owners of pooled accounts held by a notary or independent legal professional, provided information on the identity of the beneficial owners is available upon request
- a European Union institution (referred to as the 'European Community' before December 2009)

4.20 You must have evidence to show that a customer or service provided is eligible for simplified due diligence.

4.21 You must also conduct ongoing monitoring in line with your risk assessment.

4.22 You must always do customer due diligence and ongoing monitoring if you suspect money laundering or terrorist financing.

4.23 Simplified due diligence is never appropriate if your customer is another Money Service Business because of the money laundering risk. When your customer is another Money Service Business you must do customer due diligence and HMRC expects you to do enhanced due diligence before entering into a business relationship.

Enhanced due diligence

4.24 'Enhanced due diligence' means in situations that are high risk, taking additional measures to identify and verify the customer's identity and source of funds and doing additional ongoing monitoring. You must do this when:

- your customer is not physically present for identification face-to-face
- your customer is a politically exposed person, or an immediate family member or a close associate of a politically exposed person
- the nature of a particular situation presents a higher risk of money laundering or terrorist financing

Non face-to-face customers

4.25 If you can't identify a customer face-to-face, then you must do more due diligence to check their identity, for example:

- obtain additional information or evidence to establish the customer's identity
- take additional measures to verify the documents supplied, or require that copies of the customer's documentation are certified by a bank, financial institution, lawyer or notary
- verification of the customer's identity using reputable third party software
- ensure the first payment of the operations is made through a bank account in the customer's name

Politically exposed persons

4.26 If your customer is a politically exposed person, then you must put in place the following enhanced due diligence measures:

- obtain senior management approval before establishing a business relationship with that person
- take adequate steps to establish the source of wealth and source of funds that are involved in the proposed business relationship
- conduct enhanced ongoing monitoring where you've entered into a business relationship

Timing

4.27 You must verify the identity of a customer or beneficial owner before entering into an ongoing business relationship or carrying out of an occasional transaction. In the case of an ongoing business relationship, where it is necessary not to interrupt the normal conduct of business, you may complete the verification of identity while you are in the course of establishing a business relationship, provided that there is little risk of money laundering or terrorist financing, and that you complete the verification as soon as practicable after contact is first established.

Non-compliance with customer due diligence

4.28 If you can't comply with the customer due diligence measures, then you must not:

- carry out a transaction with or for the customer
- establish a business relationship or carry out an occasional transaction with the customer

You must:

- terminate any existing business relationship with the customer and consider making a suspicious activity report

Customer due diligence on transactions below €15,000

4.29 For transactions below €15,000 (or the sterling equivalent) where there's no ongoing business relationship you should consider the money laundering and terrorist financing risks when deciding if you should do customer due diligence on a particular customer, as explained in Chapter 3.

4.30 Money transmission businesses must obtain information on the payer and verify that information on transactions of more than €1,000 (or the sterling equivalent) to comply with Regulation (EC) No 1781/2006 on information on the payer accompanying transfer of funds (see section 9.23 for more details). However, HMRC expects that money transmission businesses should obtain and verify the identity of customers for all money transfers, regardless of value.

Linked transactions

4.31 Linked transactions may be a series of transactions by a legitimate customer, or they may be transactions that appear to be independent, but are in fact split into two or more transactions to avoid detection. This typically happens when a customer tries to avoid anti money laundering controls by splitting transactions into several smaller amounts, below the level at which you check ID or enquire about the source of funds. You must have systems to detect linked transactions, and to undertake enhanced due diligence on them, and report any suspicious activity when they're detected.

4.32 The value of the transaction here means the gross value of the transaction, not the value of your commissions, fees or charges.

4.33 You must put in place systems to monitor customers' transactions to identify linked transactions. For example, to identify linked transactions you must be able to associate a series of money transfers made by the same customer to a recipient or several recipients over a period of time. Also, you must be

able to associate a series of money transfers made by different customers to the same recipient over a period of time.

4.34 If you conduct business through branches or agents, your systems should be able to identify linked transactions that are conducted through all your locations.

4.35 There is no specific time period over which transactions may be linked, after which enhanced due diligence is not necessary. The period of time depends on the customers, product and destination countries. HMRC recommends that businesses consider checking for linked transactions over a minimum rolling 90 day period. HMRC will check that you have an adequate system in place and are operating it effectively.

Identifying private individuals

4.36 You must obtain a private individual's full name and you should also obtain the residential addresses or date of birth.

4.37 If you verify the customer's identity by documents, you must see the originals and not accept photocopies, unless validated as described below:

- photocopied identity documents can be accepted as evidence provided that each copy document has an original certification by an appropriate person to confirm that the person is who they say they are

- an appropriate person is, for example, an independent professional person, a family doctor, an, accountant, civil servant, solicitor, notary or officer of HM armed forces

4.38 You should verify these using 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 a:

- valid passport
- valid photo card driving licence

- national identity card
- firearms certificate
- identity card issued by the Electoral Office for Northern Ireland

4.39 Where the customer does not have one of the above documents, or the customer does not meet the criteria in your risk assessment, you may wish to ask for the following:

- a government-issued document (without a photo) which includes the customer's full name, and also 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

And secondary evidence of the customer's address, such as:

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

4.40 You should check the documents to satisfy yourself of the customer's identity. This may include checking:

- spelling
- validity
- photo likeness
- whether addresses match the additional information

4.41 In most cases, additional customer information may be taken at face value. However, if the additional information provided appears out of place or contradictory, this should serve to raise suspicions about the transaction. You must make further enquiries and obtain additional information and/or

documents to establish the customer’s identity and, where necessary, the source of funds.

4.42 If you verify an individual's identity electronically, you should do so from two separate online sources, or use a service provider that does so. This check 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 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.

4.43 An electronic records check establishes that an individual exists, not that your customer is that individual. You should therefore verify key facts that only the customer may know, to establish that they are who they say they are, for example their place of birth, or how long they have been resident at an address.

Individuals not resident in the UK

4.44 You should obtain the same types of identity documents for non-UK residents as for UK residents.

4.45 If you have concerns that an identity document might not be genuine, contact the relevant embassy or consulate. You can get the customer's address from:

- an official overseas source, such as an electoral register
- a recognised, well-established directory
- a person regulated for money laundering purposes in the country where the person is resident, who confirms that they know the individual and confirms that the individual lives or works at the overseas address given

4.46 Where appropriate you can also accept written assurances from reputable persons or organisations that have dealt with the customer for some time.

Identifying organisations as customers

4.47 For corporate customers, partnerships, trusts, charities and sole traders, you must obtain identity information that is relevant to that entity. This includes:

- the full name of the company
- registration number
- registered address
- country of incorporation

4.48 It will also be necessary to establish the beneficial owners of such entities. Additionally, for private or unlisted companies you must obtain the names of all directors (or equivalent), and the names of individuals who own or control over 25% of its shares or voting rights; or the names of any individuals who otherwise exercise control over the management of the company.

4.49 You must verify the identity through reliable, independent sources that are relevant to that type of entity. For example:

- searching a relevant company registry
- confirming a company's listing on a regulated market
- obtaining a copy of the company's certificate of incorporation

You must also obtain evidence that individuals have the authority to act for that entity.

Beneficial owners

4.50 You must identify the existence of a beneficial owner and understand how they operate. This means you must understand their role and how they exercise control over a business or individual transactions. If you suspect or have identified that a beneficial owner controls or owns the customer, then you should verify the beneficial owner's identity.

4.51 Where your customer is a private individual fronting for another individual who is the beneficial owner, you should obtain the same information about that beneficial owner as you would for a customer. You must verify the identity of a beneficial owner according to the degree of risk associated with the business relationship with your customer. You should use any public records of beneficial owners such as company registers, or ask the customer for relevant information. You should also ask for evidence of the beneficial owner's identity on the basis of documents, data or information obtained from a reliable and independent source or obtain the information in some other way.

Reliance on third parties

4.52 Money Service Businesses are not permitted to rely on customer due diligence done by another Money Service Business.

4.53 You may rely on customer due diligence done by certain other businesses provided that the other business agrees to being relied on. If you rely on another business to do customer due diligence on your behalf you'll remain responsible for any failure to apply such measures; and you must make sure that the business which carries out the due diligence can give it to you if you ask for it. The types of businesses you can rely on include:

- credit or financial institutions authorised by the Financial Conduct Authority
- an auditor, insolvency practitioner, external accountant, tax advisor or independent legal professional supervised by one of the professional bodies listed in the Regulations

See also the section on undertaking business with another Money Service Business that is not your agent (sections 8.16 and 8.17).

5. Reporting suspicious activity

Minimum requirements

You must carry out the following:

- staff must raise an internal report where they know or suspect, or have reason to believe, that another person is engaged in money laundering, or that terrorist property exists
- the business's nominated officer must consider all internal reports - the officer must make a report to the National Crime Agency as soon as it's feasible to do so, even if no transaction takes place, if the officer considers that there's knowledge, suspicion, or reasonable belief that another person is engaged in money laundering, or financing terrorism
- the business must seek consent from the National Crime Agency before proceeding with a suspicious transaction or entering into arrangements if it's to provide itself with a defence to a charge of money laundering
- it's a criminal offence for anyone to do or say anything that 'tips off' another person that a disclosure has been made where the tip-off is likely to prejudice any investigation that might take place

Actions required

The following actions are also required and must be kept under regular review:

- enquiries made in respect of internal reports must be recorded
- the reasons why a report was, or was not, submitted should be recorded
- keep a record of any communications to or from the National Crime Agency about a suspicious activity report

Suspicious activity report

5.1 A Suspicious Activity Report (SAR) is the name given to a report to the National Crime Agency under the Proceeds of Crime Act or the Terrorism Act. The report details individuals or a business who you or an employee suspect may be involved in laundering money or financing terrorists.

5.2 The suspicion is that the funds involved in the transaction or activity are the proceeds of any crime. You don't have to know what sort of crime they may have committed, but the presence of one or more warning signs of money laundering, which can't be explained by the customer, will be relevant.

5.3 As a Money Service Business, because you're in the regulated sector, you're also required to make a report if you have a reasonable belief for suspecting money laundering. This means that the facts you have about the customer and the transaction would cause a reasonable person in your position to have a suspicion.

5.4 The tests for making a report about terrorist financing are similar to those for money laundering. You must make a report if you know, suspect or have reasonable grounds for knowing or suspecting that another person committed or attempted to commit a terrorist financing offence.

Nominated officer

5.5 You must appoint a nominated officer to make reports. The nominated officer (or a deputy) must make a report if they know or suspect that someone is involved in money laundering or terrorist financing.

5.6 Staff must report to the nominated officer as soon as possible if they know or suspect that someone, not necessarily the customer, is involved in money laundering or terrorist financing. The nominated officer will then decide whether to make a report.

5.7 The nominated officer should make a suspicious activity report, even if no transaction takes place. The report should include details of how they know or suspect money laundering or terrorist financing. It should also include all relevant information about the customer, transaction or activity that the business has on its records.

5.8 If a report is completed after a transaction has taken place, you'll be able to do business with the customer, subject to risk assessment procedures, but you must make additional reports if you remain suspicious after the first report. This means you'll need to proceed with extreme caution, and you should seek consent for any further transaction with that customer. You cannot ask for a general consent to transact with a customer, only to carry out a specific transaction.

5.9 If a report is made before completion of a transaction, you should seek the consent of the National Crime Agency to proceed with the transaction, and you must do so if you wish to provide yourself with a defence to a charge of money laundering. You should mark the report with 'CONSENT'.

Sole trader

5.10 A sole trader with no employees does not need a nominated officer, as they're responsible for reporting suspicious activity.

Consent

5.11 It's an offence for the nominated officer or sole trader to proceed with a transaction, or undertake any activity linked to the consent request, if the nominated officer or sole trader has sought consent, but has not yet received it, within 7 working days, beginning the day after submitting the report.

5.12 If you don't get a response from the National Crime Agency after 7 working days, you may carry on with the transaction. If the agency refuses consent, you must not proceed with that transaction or activity for up to a further 31 calendar days.

5.13 The National Crime Agency has published information on obtaining consent. Some of the key points include:

- consent is only valid for the transaction reported - any future transactions by the same customer have to be considered on their own merits (and in the light of the suspicions that arose for the original one)
- you can't ask for general consent to trade with a customer, only to carry out a particular transaction
- the initial notice period is 7 working days from the date of the report; and if consent is refused, the moratorium period is a further 31 calendar days from the date of refusal - if you need consent sooner, you should clearly state the reasons for the urgency and perhaps contact the National Crime Agency to discuss the situation
- consent requests should include:
    - the information or other matter which gives the grounds for knowledge, suspicion or belief that another person is engaged in money laundering, or that terrorist property exists
    - a description of the property that is known, suspected or believed to be criminal property, terrorist property or derived from terrorist property
    - a description of the prohibited act for which consent is sought
    - the identity of the person or persons known or suspected to be involved in money laundering or who committed or attempted to commit an offence under the Terrorism Act
    - the whereabouts of the property that is known or suspected to be criminal property, terrorist property or derived from terrorist property
- the National Crime Agency will contact you by telephone you and will confirm their decision in writing

Making a report

5.15 You must make a report as soon as possible after you know of or suspect that money laundering or terrorist financing is happening.

5.16 The National Crime Agency published guidance on making a report in January 2014.

5.17 The National Crime Agency has a secure, encrypted system for submitting reports called 'SAR Online'. If you choose to report using SAR Online, the agency will provide information and registration details that lets you:

- register your business and contact persons
- receive a welcome pack with advice and contact details, free of charge
- submit a report at any time of day
- receive e-mail confirmation of each report

5.18 You can submit reports online and this is the National Crime Agency's preferred method. The benefit is that you get an instant confirmation and reference number.

5.19 The system does not retain a file copy for your use, so you should keep your own copy of your report.

Forms

5.20 You can get reporting forms for you to type up from the National Crime Agency's website. You should send them to:

UK FIU
PO Box 8000
London SE11 5EN

Fax: 020 7238 8256

You won’t receive acknowledgement of a report sent through the post.

You can talk to the National Crime Agency. Contact the helpdesk on 020 7238 8282 for help in submitting a report or with the online reporting system. However, the helpdesk can’t give you advice on whether or not to make a report, as this is a decision that only you can make.

Tipping off

5.21 It's a criminal offence for anyone to say or do anything that may tip off another person that a suspicion has been raised, or that a money laundering investigation may be carried out. It’s also an offence to falsify, conceal or destroy documents relevant to investigations.

5.22 For regulated businesses, including Money Service Businesses, the Proceeds of Crime Act (Section 333A(1)) makes it an offence to disclose to a third person that a suspicious activity report has been made, if that disclosure might prejudice any investigation that might be carried out as a result of the report.

5.23 It's also an offence (under Section 333A(3)) of the act to disclose that an investigation into a money laundering offence is being contemplated or carried out if that disclosure is likely to prejudice that investigation. The key point is that you can commit this offence, even where you're unaware that a suspicious activity report was submitted.

5.24 Outside the regulated sector, Section 342(1) of the Act makes it an offence to prejudice a confiscation, civil recovery or money laundering investigation if the person making the disclosure knows or suspects that an investigation is being, or is about to be conducted.

5.25 The offences described in sections 5.21 to 5.24 carry penalties of up to 5 years imprisonment and/or a fine.

6. Record keeping

Minimum requirements

You must retain:

- copies of, or references to, the evidence obtained of a customer's identity, for 5 years after the end of the business relationship
- details of customer transactions for 5 years from the date of the transaction
- details of actions taken in respect of internal and external suspicion reports
- details of information considered by the nominated officer in respect of an internal report, where the nominated officer does not make an external report

Actions required

The following actions are also required and must be kept under regular review:

- maintain appropriate systems for retaining records
- making records available when required, within the specified timescales

6.1 You must keep records of customer due diligence checks and business transactions:

- for identity checks - 5 years after the end of the customer relationship
- for occasional transactions - 5 years from the date the transaction was completed
- you should also keep supporting records for 5 years after the end of a business relationship

6.2 You must also keep records of suspicious activity reports, and any other internal or external reports and decisions.

6.3 You can keep records as original documents, photocopies of original documents, in either computerised or electronic form. The aim is to ensure that the business meets its obligations and, if requested, can show how it has done so. This evidence may be used in court proceedings against the criminals.

6.4 If someone else carries out customer due diligence for you, you must make sure that they also comply with these record keeping requirements.

7. Staff awareness and training

Minimum requirements

You must ensure that relevant staff:

- are aware of the risks of money laundering and terrorist financing, the relevant legislation, and their obligations under that legislation
- know who the nominated officer is and what his responsibilities are
- train in the firm's procedures and in how to recognise and deal with potential money laundering or terrorist financing transactions or activity
- train at regular intervals, and that you record the details

The relevant director or senior manager has overall responsibility for establishing and maintaining effective training arrangements.

Actions required

The following actions are also required and should be kept under regular review:

- provide appropriate training to make relevant staff aware of money laundering and terrorist financing issues, including how these crimes operate and how they might take place through the business
- ensure that relevant employees have information on, and understand, the legal position of the business; individual members of staff, and any changes to these positions
- consider providing relevant staff with case studies and examples related to the firm's business
- train relevant staff in how to operate a risk-based approach to assessing the risks of money laundering and terrorist financing

7.1 Your staff are the best defence against money launderers and terrorist financers who may try to abuse the services provided by your business.

7.2 You must:

- tell your staff about your anti money laundering and counter terrorism financing obligation
- give them suitable risk-based training on their legal obligations
- give them information on how to identify and deal with the risks

If you don't do this, and your staff don't know what is required, then you and your business may be open to penalties or criminal charges.

Training

7.3 When you consider who to train, you should include staff that deal with your customers, deal with money or help with compliance. Think about reception staff, administration staff and finance staff, because they will each have a different involvement in compliance, and so have different training needs.

7.4 Nominated officers, senior managers and anyone involved in monitoring business relationships and internal controls must also be fully familiar with the requirements of their role and understand how to meet those requirements.

7.5 Each member of staff should be ready to deal with the risks posed by their role. Their training should be good enough, and often enough, to keep their knowledge and skills up-to-date.

It should cover:

- the staff member's duties
- the risks posed to the business
- the business's policies and procedures
- how to do customer due diligence and check customers' documents
- how to spot and deal with suspicious customers and activity
- how to make internal reports and/or disclosures of suspicious activity
- record keeping
- the Money Laundering Regulations 2007; Part 7 of the Proceeds of Crime Act; and sections 18 and 21A of the Terrorism Act

7.6 Training may include:

- face-to-face training
- online training sessions
- going to conferences
- taking part in special meetings to discuss the business's procedures
- reading publications
- meetings to review at the issues and risks

7.7 A policy manual should be set up to raise staff awareness and for reference between training sessions.

7.8 Training is necessary when staff join the business, move to a new job and when they change roles. They should also have ongoing training at least every 2 years, depending on the level of risks.

7.9 You should think about keeping evidence of your assessment of training needs and the steps you've taken to meet those needs. For example, you may be asked to produce training records in court.

7.10 Training records include:

- a copy of the training materials
- details of who has provided training, if provided externally
- a list of staff who have completed training, with dates, with their signatures, or electronic training records
- a refreshed training schedule

8. Principal-agent relationships and other business models

8.1 Money Service Businesses frequently enter into contractual arrangements with other parties to enable the Money Service Business to provide services to customers, typically as follows:

Principal–agent business models

These include:

- appointing an agent or agents to act on behalf of a Money Service Business (the principal), for example by:
    - accepting money transmission instructions from customers
    - accepting cheques for encashment
    - undertaking currency exchange

- appointing agents, and perhaps sub-agents of agents, to distribute certain products, for example prepaid cards, or to supply and operate automated terminals or services such as bill payment terminals

Other business models

Other models include:

- accepting instructions from one or more other Money Service Businesses, for example by acting as a wholesaler in order to aggregate many low value transactions submitted by other Money Service Businesses

- franchising a brand name and support services, for example by:
    - supplying foreign currency, and foreign exchange quote systems to a franchisee
    - licensing a brand name to independent Money Service Businesses

8.2 A Money Service Business may therefore act as a principal for certain transactions, and may at the same time act as an agent, a franchisor, a franchisee, or distributor for other products and services.

8.3 An agency may have agency agreements in order to act on behalf of more than one principal. This may, for example, enable the agent to offer remittances to a wider range of destinations.

Meaning of 'principal'

8.4 Acting as a principal here means that a Money Service Business is the party that contracts with a customer through its agent, and owns and is responsible for the transaction.

8.5 In a principal-agent relationship, the principal is the person who gives authority to an agent to act on the principal’s behalf. However, the responsibilities of the principal do not absolve an agent from its legal obligations to comply with the Money Laundering Regulations and the Proceeds of Crime Act

8.6 Typically, a written contract, an agency agreement – between principal and agent is necessary to set out their respective roles and responsibilities. For example, an agency agreement may provide for the principal to give its agent access to technology, systems, forms, advertising and marketing material; and to written processes and procedures necessary to comply with the Money Laundering Regulations and other legal and regulatory requirements.

Guidance for a principal in appointing and managing an agent

8.7 A Money Service Business that acts as a principal is responsible and accountable for the conduct of its agents. It must tell HMRC of the appointment or removal of every agent.

8.8 A principal should have a comprehensive and up-to-date agency agreement with each agent. It should maintain an up-to-date record of all the agents appointed, including details of the shareholding structure; board of directors, management and locations of the agents.

8.9 An agency agreement should set out the obligations of the agent to comply with all the applicable anti money laundering and other legal and regulatory requirements, as well as the internal policies and procedures of the principal. The principal should ensure that the agent understands its responsibilities under the agency agreement.

8.10 The principal must establish strong oversight of its agents and be alert to any potential criminal activity by an agent, as well as the agent's customers. HMRC expects a principal to put nominated managers and management controls in place, with clear accountability and adequate resources to support the oversight of agents.

HMRC expectations

8.11 HMRC expects principals to have clear agent selection criteria to support due diligence background checks, including on-site visits, to ensure that an agent meets minimum expectations, in particular that:

- the owners and managers of the agency are fit and proper persons for their fiduciary role
- they should be of good character, they should not have criminal records, or have been the subject of any professional conduct or disciplinary action, and they must demonstrate professional standards and competence in business conduct
- the agency should be sufficiently well capitalised and have adequate staff for its role
- the agency should meet minimum record keeping, internal controls and consumer protection measures
- the agency should maintain a good compliance record

Before making an appointment

8.12 Before appointing an agent the principal should:

- lay down clear policies and procedures for monitoring agency transactions and for regularly reviewing and auditing an agent's compliance with anti money laundering obligations
- provide an adequate training programme to ensure the agent understands its Anti Money Laundering and other obligations, and keeps staff training up-to-date (see Chapter 7 on training)
- document and implement clear and consistent standard operating procedures for the conduct of the principal's business - this includes ensuring customers can check that the Money Services Business is registered with HMRC and the Financial Conduct Authority, service standards and complaints procedures, and data protection
- establish the profile of the agent's business transactions for the purpose of analysing trends and patterns of the transactions to ensure proper reporting of suspicious transactions to the principal

After making an appointment

8.13 Once appointed the principal should:

- carry out ongoing monitoring of customers and business transactions, including regular on-site visits to assess the compliance level as well as the effectiveness and adequacy of the agent's internal controls
- consider the nature and volume of an agent's business transactions as well as the agent's location to identify operations that are exposed to higher risk - these warrant more frequent on-site visits and more intensive monitoring
- ensure the agent flags suspicious transactions reports to the principal, for reporting to the National Crime Agency by the principal
- ensure the agent refers to the principal licensee for approval:
    - large value transactions based on thresholds set by the principal

    - non face-to-face transactions
    - transactions with politically exposed persons and close relations
- ensure proper management of cash by the agent, including regular monitoring of cash holdings by the agent at its premises which should be in line with the nature, values and volume of transactions of the agent
- investigate cash holdings that exceed expected levels, or are inconsistent with the profile of transactions by the agent, to ensure that the agent is not involved in irregular activities
- secure rapid corrective action to address any weaknesses that are identified, including where termination of an agency agreement appropriate

Foreign currencies

8.14 When dealing with foreign currencies, the principal should:

- have proper arrangements for sourcing foreign currencies by an agent directly with the principal
- where the agent is also permitted to source and clear foreign currencies with other parties, the principal should ensure that proper processes and procedures can identify and approve the parties and channels that an agent may deal with
- regularly monitor the pattern of business transactions to ensure that sourcing of foreign currencies by the agent are conducted through proper channels and comply with regulatory requirements
- ensure that all transactions are properly recorded, and can be accounted for and reconciled with source documents

8.15 HMRC expects the principal to:

- have contingency arrangements for safe keeping of information maintained by the agent, in the event of business disruption for any reason
- have physical controls and security measures, including counterfeit detection equipment and closed circuit cameras as a deterrent against crime

Transactions with other Money Service Businesses that are not agents

8.16 If you accept transactions from another Money Service Business that is not acting as your agent, this is a potentially high risk activity. You should do enhanced due diligence on that Money Service Business before entering into a business relationship and, as explained in section 4.10, you must continue to monitor a business relationship after it's established. For example, you should do periodic audits of the business operations of that Money Service Business. There are some additional needs:

When undertaking money transmission as an intermediary for another Money Service Business, you must do all of the following:

- monitor transactions (for example the number and average value of transactions), and where necessary the source of funds, to ensure they are consistent with the level and type of business that you expect from that business relationship and that business's risk profile
- keep the information you collect for this purpose up to date
- ensure that you receive the complete information on the payer for each individual transaction, as required by Regulation (EC) No 1781/2006 on information on the payer accompanying transfers of funds

When acting as a settlement agent in order to settle in bulk a series of transactions undertaken by 2 other Money Service Business, or a Money Service Business and another financial institution (typically this means that you may be supplying foreign currency and transferring it to the account of a Money Service Business outside the UK on behalf of a Money Service Business in the UK) you must:

- monitor transactions, and where necessary the source of funds, to ensure they are consistent with the level and type of business that you expect from that business relationship and that business's risk profile
- at the very least you should obtain the number of underlying transactions of each bulk transfer, or supply of currency made to you by the other business
- keep the information you collect for this purpose up to date

For any other type of transactions with other Money Service Businesses that are not your agents, you must:

- monitor transactions (for example the number and average value of transactions), and where necessary the source of funds, to ensure they are consistent with the level and type of business that you expect from that business relationship and that business's risk profile
- keep the information you collect for this purpose up to date

8.17 You should not accept any money remittance transactions from another business if that business is not registered or authorised by the Financial Conduct Authority under the Payment Services Regulations 2009, or under an equivalent regime under the Payment Services Directive (2007/64/EC).

Franchising

8.18 A franchise relationship may look very similar to an agency relationship. An agency relationship may include elements that are found in a franchise relationship, for example use of a brand name.

8.19 The key difference is that, where the franchise agreement provides that a franchisee is independent of the franchisor and does not act on the franchisor's behalf, then a franchisee is not an agent. A franchisee in these circumstances must register with HMRC in its own right. The franchisee is responsible for complying with anti money laundering obligations and other legal and regulatory requirements.

8.20 A principal must not use a franchise agreement to disguise what's in practice or effect an agency agreement, in order to avoid responsibility for an agent's actions. For example, where the franchisee is incapable of acting as a principal in its own right to discharge its Anti Money Laundering obligations, or where the principal retains effective control over the franchisee's business, then HMRC will expect the relationship to be formalised as an agency agreement and not a franchise agreement.

9. Risk indicators for each type of Money Service Business

9.1 The following is an example list of common risk indicators that call for enhanced due diligence. It's not an exhaustive list, and neither are these signs always suspicious. It depends on the circumstances of each case:

Use of agents

9.2 Agents

The following are examples of common risk indicators for agents:

- represent more than one principal
- are reluctant to provide information regarding their customer’s identity to the principal
- record unusual or suspicious customer information (many transactions attributed to a single customer or customer details that may be false or incorrect)
- have a high number of transactions that fall just under the threshold for due diligence or reporting to the principal
- report a high volume of business with single customer to a high risk country
- process a customer sending money to several destinations or the same recipient on the same day
- have a pattern of customers in the office that doesn't support the turnover
- have an unusually high transaction size
- have an unusually large cash transaction
- have a size and frequency of transactions that:
    - are different from the customer’s normal pattern
    - have changed since the agency relationship was established
    - are higher than comparable agencies
    - change significantly under new management of the agency

- have transactions that seem unnecessarily complicated, or seem to use front men or companies
- undertake a large proportion of business with high risk countries
- undertake business outside normal business hours
- have records in which fake identities repeat common fields, for example a different surname with all the other details like birth day and address the same

Money transmitters

The following are examples of common risk indicators for money transmitters:

9.3 Criminals use money transmitters to disguise the origins of criminal funds and move money between different jurisdictions. Criminals try to identify weaknesses in money transmitters' anti money laundering controls and exploit them.

9.4 A further risk associated with money transmission is that some jurisdictions have weak anti money laundering systems. Some jurisdictions are high risk because they are especially vulnerable to criminal activity such as drug smuggling, people trafficking and terrorism.

9.5 **New customers**

The following are examples of common risk indicators for new agents:

- checking the customer's identity is difficult
- the customer is reluctant to provide details of their identity or provides fake documents
- the customer is trying to use intermediaries to protect their identity or hide their involvement

- there's no apparent reason for using your business's services, for example, another business is better placed to handle the size of transaction or the destination of the transmission
- the customer is unable to provide satisfactory evidence of the source of the funds
- unusual source of funds
- the transmission is to a high risk country
- non face-to-face customers
- the customer owns or operates a cash-based business
- there's an unusually large cash transaction
- the size and frequency of the transaction is different from the customer’s normal pattern
- the pattern has changed since the business relationship was established
- the transaction seems to be unnecessarily complicated, or seems to use front men or companies
- the customer sends or receives money to or from himself
- the customer is acting on behalf of third parties without there being an appropriate family or business relationship between them
- other people watch over the customer or stay just outside
- the customer reads from a note or mobile phone
- an under-age person sends or receives funds from multiple sources
- there has been a significant or unexpected improvement in the customer’s financial position
- the customer (or two or more customers) is using more than one local Money Service Business, perhaps to break one transaction into smaller transactions

9.6 **Transactions**

The following are examples of common risk indicators in relation to transactions:

- are just below the threshold for due diligence checks
- appear to have no obvious economic or financial basis benefit
- route through third countries or third parties
- regularly go to or from tax haven countries
- information accompanying the payment appears false or contradictory

9.7 Where the beneficiary of a money transmission is in a high risk country you should do enhanced due diligence checks on your customer. To help you decide if you're sending money to a high-risk country, FATF publish a list of high risk and non cooperative countries. You can find this information on the FATF website.

Inward money transmission from another country into the UK

9.8 When you receive a transfer of funds from a foreign Money Service Business, you must treat the foreign Money Service Business as your customer. If it's a bulk transfer, representing a collection of underlying transmissions, the situation is high risk. You should consider doing enhanced due diligence. At the very least you should obtain the number of underlying transactions. You must also check if complete information on the payer is present, and in the case of missing or incomplete information, you must ask for the missing information or reject the transfer.

Third party payments

9.9 Third party payments are money transmissions, normally from the UK to another country, where the liability of the UK transmitter to pay the recipient is offset or partly offset by the settlement of a liability to a third party, perhaps in a different country. This type of remittance and settlement involves two separate transactions, each of which requires appropriate due diligence.

9.10 Settling a debt by means of an offset payment to a recipient, perhaps in a different country from the beneficiary, is a separate transaction. Your customer is the overseas Money Service Business that requests payment to be made to a third party. These payments are high risk and often facilitate criminal activity and money laundering. You should consider doing enhanced due diligence on the overseas Money Service Business and also verify the validity of the underlying transaction by checking invoices, bills of lading and shipping documents.

Third party cheque cashing

9.11 By cashing third party cheques, cheque cashers can facilitate income tax evasion, cheque fraud and benefit fraud. Cheques can also be used to launder money when the proceeds of a crime are provided by cheque, for example through false Income Tax Self Assessment repayments, or cheque payments for stolen scrap metal.

9.12 **New customers**

The following are examples of common risk indicators for new customers:

- cheques issued by scrap metal dealers
- checking the customer's identity is difficult
- the customer is reluctant to provide details of their identity or provides fake documents
- the customer is trying to use intermediaries to protect their identity or hide their involvement
- no apparent reason for using your business's service
- the customer is unable to provide satisfactory evidence of the source of the funds
- non face-to-face customers
- the customer wants to cash a cheque made payable to a limited company

9.13 **Regular and existing customers**

The following are examples of common risk indicators for your regular and existing customers:

- the transaction is different from the normal business of the customer
- the size and frequency of the transaction is different from the customer's normal pattern
- the pattern has changed since the business relationship was established

Cashing scrap metal dealers' cheques

9.14 The Scrap Metal Dealers Act 2013 prevents scrap metal dealers operating in England and Wales from paying their customers in cash, in order to deter metal theft. If a customer attempts to cash a cheque issued by a scrap metal dealer through a third party cheque cashing business, instead of paying the cheque into the customer's own bank account, there is a high risk that this is an attempt to bypass the provisions of the Scrap Metal Dealers Act and to launder the proceeds of metal theft. The cheque casher must undertake enhanced due diligence, and must refuse the transaction and submit a suspicious activity report if they suspect that the payment is for stolen goods.

Agents

9.15 If you arrange for another business to cash cheques on your behalf they're acting as your agent and you're the principal. There's a significant risk that criminals will seek to exploit your business for money laundering by becoming your agent. When you take on board an agent you must make sure, you understand who the beneficial owner of the business is, and that they're fit and proper persons with regard to the risk of money laundering. You should follow the guidance on appointing agents and managing an agency relationship set out above.

Currency exchanges

9.16 Criminals use currency exchange offices provide to change bulky low denomination notes into easily transported high denomination notes currency.

9.17 Criminals also often change money to facilitate further criminal activity, and to launder criminal funds by buying assets in overseas countries. They try to identify any weakness in a currency exchange office's anti money laundering controls in order to exploit them.

Risk indicators for currency exchange offices

9.18 **New customers**

The following are risk indications in relation to new customers of currency exchange offices:

- request high denomination notes such as €100, €200, and €500 notes or $100 US notes
- the customer's willing to accept poor rates of exchange
- the destination of the transmission
- the customer's unable to provide satisfactory evidence of the source of the funds
- unusual source of funds
- non face-to-face customers
- the customer is buying currency that doesn't fit with what the business knows about their travel destination
- the customer wishes to exchange large volumes of low denomination notes

9.19 **Regular and existing customers**

The following are risk indications in relation to regular and existing customers of currency exchange offices:

- the transaction is different from the normal business of the customer
- the size and frequency of the transaction is different from the customer's normal pattern
- the pattern has changed since the business relationship was established
- there has been a significant or unexpected improvement in the customer's financial position

Requests for high value denominations

9.20 The sale of high value notes entails a significant money laundering risk. All the major UK banks and financial institutions have agreed not to sell €500 notes. You should regard any request to buy or sell €500 notes as potentially suspicious. You should refuse to sell €500 notes and submit a suspicious activity report. Requests for high denomination notes by a customer should be treated as high-risk and you should do enhanced due diligence checks and submit a suspicious activity report if appropriate.

Dealing with other Money Service Businesses

9.21 If you buy currency from or sell currency to another Money Service Business that is not acting as your agent, this is a potentially high risk transaction. You should consider doing enhanced due diligence. You should monitor these transactions to ensure that number and value of transactions is consistent with the level of business anticipated when you started the business relationship.

Directions issued under the Counter Terrorism Act 2008

9.22 HM Treasury issues these directions. They apply to all UK financial and credit institutions, including money transmitters. The directions can impose a range of requirements on businesses in relation to their transactions or business relationships with a targeted country or institution and may include:

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

Additional obligations for money transmitters

9.23 Money transmission businesses must comply with Regulation (EC) No. 1781/2006 on information on the payer accompanying transfers of funds. This means that you must:

- obtain complete information on the payer for all customers wanting to transmit money
- verify the complete information on the payer on the basis of documents data or information from a reliable independent source where the transaction is over €1,000
- send the complete information on the payer to the payment service provider for the payee if the payment service provider for the payee is situated outside the EU
- send the account number or unique identifier that allows the transaction to be traced back to the payer if the payment service provider for the payee is in the EU
- if the payer doesn't have an account number, allocate the transaction a unique identifier, which allows the transaction to be traced back to the payer

Complete information on the payer

Complete information on the payer consists of:

- the payers name
- the payers full postal address including post code
- payer’s account number or where the payer doesn't have an account number a unique identifier that allows tracing of the transaction 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 a passport number)

The customer’s identification number is a number that the service provider allocates to the payer. It must be capable of providing a link to the transaction and to any verification made.