Anti-Money Laundering Supervision: Money Service Businesses

This is interim guidance and will be amended in due course. The section on politically exposed persons will be reviewed once the Financial Conduct Authority has published their own guidance.

General introduction

Thank you for taking the time to study this guidance. It is designed to help you comply with the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (referred to as “the Regulations” in this guidance)

Meeting your legal obligations is important because it contributes to tackling the serious economic and social harm from organised crime, it also reduces the threat from terrorism in the UK and around the globe.

If you would like to know more about some of the success of UK suspicious activity reporting (SAR) see the National Crime Agency SARs report.

Almost all businesses supervised by HMRC for anti-money laundering purposes are subject either to fit and proper or approval requirements under the Regulations. These requirements are to ensure that businesses beneficial owners and senior management are appropriate people to undertake those roles. Key personnel must pass the relevant test before the business can register, and can remain registered, with HMRC.

HMRC stresses that neither of those requirements test whether the business is professionally run or operated. Registration is a legal requirement to trade, it is not a recommendation or endorsement of the business.

HMRC advises registered businesses to carefully avoid using language in this context that might give the impression that registration was a form of endorsement or recommendation.

There is more detail about these requirements in the fit and proper guidance

Status of this guidance

This guidance is for money service businesses. Bill payment service providers and telecommunication, digital and IT payment service providers can use this guidance unless any section indicates it does not apply.

This guidance has been submitted for HM Treasury approval.

This guidance replaces HMRC's guidance: “Anti-money laundering guidance for money service businesses” published on 13 August 2014 and MLR9a published 20 September 2013. The guidance is effective from 26 June 2017.

Meaning of words

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.

Further sources of guidance

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 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.

The Joint Money Laundering Steering Group has also produced guidance for banks on the treatment of money service businesses as customers.

KS suggests you say “For the sake of brevity, references to money laundering should generally be read as also covering terrorist financing unless it is clear from the context that one or other is specifically involved”.

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.
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 , or to deposit cash into somebody else's bank account, or to make a transfer of funds on behalf of somebody else
- third party cheque cashing has been exploited by some persons to evade a ban on paying cash for scrap metal or to avoid taxes
- money transmitters can be used by persons not allowed to work to send the proceeds of illegal working from the UK
- currency exchange businesses 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

1.2 Terrorist financing involves dealing with money or property that you have 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

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

- Proceeds of Crime Act 2002
- Terrorism Act 2000
- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (referred to in this guidance as "the Regulations")
- Criminal Finances Act 2017

The following legislation applies to money transmission businesses only:

- Regulation (EU) 2015/847 on information accompanying transfers of funds (the Payments Regulation)
- Payment Service Regulations 2009

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.

1.4 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 nominated officers and employees of businesses in the regulated sector, such as money service businesses.

1.5 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

1.6 The Criminal Finances Act 2017 make important amendments to the Proceeds of Crime Act and the Terrorism Act. It extends the powers of law enforcement to seek further information, recover the proceeds of crime and combat the financing of terrorism.

1.7 The 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.

1.8 The European Union Regulation on the information accompanying transfer of funds set out what information money transmission businesses must send when they arrange a transfer of funds.

Financial sanctions

1.9 All individuals and legal entities who are within or undertake activities within the UK's territory must comply with the EU and UK financial sanctions that are in force. Most financial sanctions are made through EU law which has direct effect under UK law.

The Office of Financial Sanctions Implementation works closely with the EU Commission and other member states in implementing sanctions. Other financial sanctions are put in place by UK laws.

You should report any transactions carried out for persons subject to sanctions or if they try to use your services. You can report a suspected breach, sign up for free email alerts and obtain Information on the current consolidated list of asset freeze targets and persons subject to restrictive measures at:

https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation

Data Protection

1.10 The Data Protection Act 1998 (DPA) governs the processing of information relating to individuals, including obtaining, holding, use or disclosure of information.

Personal data obtained by a business under the Regulations may only be processed for the prevention of money laundering and terrorist financing. You must inform your customers of this and the information specified in paragraph 2(3) of schedule 1 to the DPA.

This use is necessary in order to exercise a public function that is in the public interest and to carry out a function permitted by legislation. No other use may be made of the information unless you have consent of the customer or it is allowed by other legislation.

Money Service Businesses

1.11 '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)

1.12 Money service businesses must comply with the 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 2009.

1.13 This guidance is for money service businesses who are supervised by HMRC for compliance with the Regulations. However, if a firm is authorised by the Financial Conduct Authority under the Financial Services and Market Act 2000 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 Regulations.

1.14 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 74 (7)(b) of the Money Laundering, Terrorist Financing and Transfer of Funds (information on the Payer) Regulations 2017. Authorisation for the purposes of Financial Services and Market Act 2000 is different from being authorised as a payment institution under the Payment Services Regulations 2009.

Penalties

1.15 If a person or business fails to comply with the 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. You can find information on the penalties HMRC can issue here.

2. Responsibilities of senior managers

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.

A senior manager is an officer or employee who has the authority to make decisions that affect your business's exposure to money laundering and terrorist financing risk. Examples include a director, manager, company secretary, chief executive, member of the management body, or someone who carries out those functions, or any partner in a partnership, or a sole proprietor.

Minimum requirements

Senior managers must:

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

Responsibilities

2.2 Senior managers are responsible for making sure that the business has carried out a risk assessment for its business and has policies, controls and procedures to help reduce the risk that criminals may exploit the business for financial crime. Your policies controls and procedures must address the level of risk that the business may encounter in different circumstances.

2.3 You must also take account of the size and nature of your business and put in place additional measures to ensure your policies, controls and procedures are being complied with throughout your organisation including subsidiaries, branches and agents.

Actions required

Senior managers must:

- carry out a risk assessment identifying where your business is vulnerable to money laundering and terrorist financing
- prepare, maintain and approve a written policy statement, controls and procedures to show how the business will manage the risks of money laundering and terrorist financing identified in risk assessments
- review and update the policies, controls and procedures to reflect changes to the risk faced by the business
- make sure there are enough trained people equipped to implement policies adequately, including systems in place to support them
- make sure that the policies, controls and procedures are communicated to and applied to subsidiaries or branches in or outside the UK
- monitor effectiveness of the business's policy, controls and procedures and make improvements where required
- have systems to identify when you are transacting with high risk third countries identified by the EU or financial sanctions targets advised by HM Treasury and take additional measures to manage and lessen the risks

3. Risk assessment, policies, controls and procedures

Risk Assessment

3.1 Your risk assessment is how you identify the risks your business is exposed to. 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.

You must:

- identify and monitor the risks of money laundering and terrorist financing that are relevant to your business - in other words, your business's risk assessment
- take note of information on risk and emerging trends from the National Risk Assessment and HMRCs risk assessment and amend your procedures as necessary
- assess, and keep under regular review, the risks posed by your:
    - customers and any underlying beneficial owners (see sector guidance 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 third countries, for example countries identified by the EU or Financial Action Task Force (FATF) as having deficient systems to prevent money laundering or terrorist financing

Your risk assessment must be in writing and kept up to date. You must give it to HMRC if we ask for it.

In some limited circumstances we may tell you that you do not need to keep a record of your risk assessment, for example a sole practitioner with no employees, a small number of well-established clients and where the risk are understood.

Policy, controls and procedures

Policy statement

3.2 Your policy statement must lay out your policy, controls and procedures and how you and other senior managers will manage the business's exposure to risk. It must make clear how you'll lessen the risks identified in your risk assessment to prevent money laundering and terrorist financing and take account of any additional risk due to the size and nature of your business.

Policies, controls and procedures must be in writing and be communicated throughout your organisation to staff, branches and subsidiaries in and outside the UK.

Controls and procedures

3.3 Senior managers must put in place appropriate controls and procedures to reflect the degree of risk associated with the business and its customers.

3.4 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, jurisdiction, product or transaction, especially large or complex transactions or unusual patterns of activity that have no apparent economic or lawful purpose.

Minimum requirements

You must also show how you will:

- do customer due diligence checks and ongoing monitoring
- identify when a customer or beneficial owner is a politically exposed person or a family member or close associate of one and do enhanced due diligence
- appoint a nominated 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 money laundering and terrorist financing risks and understand what they should do to manage these, including the importance of reporting suspicious activity to the nominated officer
- maintain accurate, up-to-date record keeping and retention of records

Actions required

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

- ensure customer identification and acceptance procedures reflect the risk characteristics of customers
- take further measures for higher risk situations such as approving transactions with politically exposed persons
- ensure low risk situations are assessed and records retained to justify your assessment
- 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
- ensure staff training is appropriate to the individual and kept up to date and content regularly reviewed
- ensure staff know the names of the nominated officer and any deputy

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

3.5 The policy of a larger, or more complex business, must include:

- the appointment of a senior management member who has responsibility for monitoring the effectiveness of and compliance with the policy, controls and procedures, including regular reviews to learn from experience

- individual staff responsibilities under the Regulations
- the process for reviewing and updating the business's policies, controls and procedures
- the process for auditing the business's compliance with its policies, controls and procedures

Making relevant appointments within your business

3.6 You must inform HMRC of the names of the compliance and nominated officers within 14 days of the appointment and if there is a change in the post holder.

Appointing a nominated officer for the business

3.7 You must appoint a nominated officer, from within your business, to receive reports of suspicious activity from staff 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.

The nominated officer should be at an appropriate level of seniority in your business to make decisions on transactions.

3.8 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). HMRC expects the nominated officer to be based in the UK.

Appointing a compliance officer for larger, more complex businesses

3.9 You should consider whether the size and nature of your business means that you must appoint a compliance officer to ensure your compliance with the Regulations. You should take into account your risk assessment and exposure to money laundering and terrorist financing risk, the number of employees, number of premises, agent network, geographical area you operate in, type of customers, and the complexity of the business.

HMRC would not expect you to appoint a compliance officer where you are a sole trader where you carry out regulated activity from one premises, have no more than two or three staff and run an uncomplicated business model or organisation.
Businesses with, for example, more premises, use branches or agents, high turnover of customers, non-local or cross border trading and complex ways to deliver services will need a compliance officer.

3.10 Where a compliance officer is needed the business must:

- appoint a person from the board of directors, its equivalent or senior management, to act as a compliance officer.
- screen relevant employees when appointed and during the course of the appointment to ensure they have the ability to carry out their functions and are of good conduct and integrity

3.11 The compliance officer will be responsible for the business's compliance with the regulations including:

- carrying out regular audit on compliance with the regulations such as:
  - actively check adherence to the policies, controls and procedures
  - review of how effective they are
  - recommend and carry out improvements
- ensure compliance throughout the business including subsidiaries and branches
- oversight of relevant staff and agent screening

Relevant staff and agents are persons involved in the identification of risk, controls and procedures to reduce risk and your compliance with the Regulations.

3.12 It is recommended that the compliance officer and nominated officer should not be the same person. This is because the responsibilities differ, the compliance officer needs to be at board level and needs to review how the business carries out its obligations, including the reporting of suspicious activity. However, in some businesses it may not be practical to have two individuals carrying out these functions and a compliance office may have to act in the role of a nominated officer.
Larger, more complex businesses may need to appoint a deputy.

HMRC expects the compliance officer and nominated officers to be based in the UK.

3.13 Where a business is part of a group of companies an individual can carry out these roles for other parts of the group. If each subsidiary has their own compliance officer then one person should have oversight of this.

Personal liability of officers

3.14 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.

Managing group subsidiaries and branches

3.15 A parent company must apply its policies, controls and procedures in all subsidiaries or branches, in or outside the UK.
This will involve:

- putting in place controls for data protection and information sharing to prevent money laundering and terrorist financing
- share information on risk within the corporate group
- ensure subsidiaries or branches in EU member states are complying with the requirements of that country
- ensure subsidiaries or branches in a third country that does not impose money laundering requirements are following similar measures to the UK

Where a third country does not allow similar measures you must put in place extra controls to deal with this risk and inform HMRC.

Risk-based approach

3.16 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.

3.17 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.

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

Risks your business may face

3.19 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.
The risk profile depends on the nature of the business, branch network, the areas it operates in, who your customers are, where they are from and the vulnerability of your services or transactions to financial exploitation.

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

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

- 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 and will ongoing monitoring support the original assessment
- if you have applied simplified due diligence will the records show evidence for treating the customer as low risk
- 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

3.21 These are some of the questions to consider to help inform your risk assessment 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
  - if you accept customer introductions from an agent or third party, have you accepted customers from this source before
- 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 especially from a high risk third country identified by the EU
  - complex business ownership structures with the potential for concealing beneficiaries
  - customers carrying out frequent low value transactions (see guidance on linked transactions)
  - customers sending money to high risk countries
  - new or existing customers (particularly overseas customers) with an foreign exchange requirement that request a transfer of funds without asking what the rate of exchange will be
  - customers requesting a transfer of funds without an foreign exchange requirement. For example sending sterling to another UK person or overseas, Or sending Euros from a Euro account in the UK to a person overseas in Euros

The section of suspicious activity reporting has examples of potentially suspicious activity.

Controls and procedures to put in place

3.22 Once you've identified and assessed the risks and warning signs, you must ensure that you put in place appropriate controls and procedures 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 assessment.

3.23 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

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
- reviewing low risk customers and applying more due diligence where changes are apparent
- 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 depending on the circumstances of your business.

3.24 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

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

3.26 You must 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

These are the minimum requirements:

- complete customer due diligence on all customers and beneficial owners before entering into a business relationship or occasional transaction
- have procedures to identify those who cannot produce standard documents, for example, a person not able to manage their own affairs
- identify and verify a person acting on behalf of a customer and verify that they have authority to act
- apply enhanced due diligence to take account of the greater potential for money laundering in higher risk cases, including in respect of politically exposed persons and when the customer is not physically present when being identified
- apply customer due diligence when you become aware that the circumstances of an existing customer relevant to their risk assessment has changed
- not deal with certain persons or entities if you cannot do customer due diligence and consider making a suspicious activity report
- have a system for keeping copies of customer due diligence and supporting records and to keep the information up to date

Who is the customer

4.1 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.

4.2 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

4.3 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.

4.4 You must do customer due diligence when:

- establishing a business relationship with a customer
- carrying out an occasional transaction that amounts to a transfer of funds exceeding €1,000
- under the Funds Transfer regulations only, you must identify and verify the customer when a money transmission transaction is of any value and is funded by cash or anonymous e-money
- carrying out an occasional transaction with a customer of €15,000 or more
- money laundering or terrorist financing is suspected
- you suspect that information obtained for due diligence checks on a customer is not reliable or adequate

Customer due diligence means:

- identifying all customers and verifying their identity (more details below)
- identifying all beneficial owners, where applicable, and taking adequate risk based measures to verify their identity
- obtaining information on the purpose and intended nature of the business relationship
- conducting ongoing monitoring of the business relationship, to ensure transactions are consistent with what the business knows about the customer, and the risk assessment
- retain records of these checks and update them when there are changes

Timing of customer due diligence

4.5 The customer's' identity and where applicable the identity of a beneficial owner, must be verified before entering into a **business relationship** or **occasional transaction**.
You can make an exception to this practice only if both the following apply:

- it is necessary not to interrupt the normal conduct of business
- there is little risk of money laundering or terrorist financing

However, this exception is very limited as the verification must still be completed by the time the business relationship is entered into. This exemption must not be used where it is hard to verify a customer's or beneficial owner's identity.

To use this exception, a business will have to explain in its risk assessment why it considers the business relationship or transaction has little risk of money laundering or terrorist financing.

Non-compliance with customer due diligence

4.6 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
- consider making a suspicious activity report
- if no suspicious activity report is made, record the reasons why it is considered that a report is not required

Business relationship

4.7 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

4.8 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 assessment. Examples of ongoing monitoring under different business models are set out in Chapter 6.

You must also keep the information you collect for this purpose up-to-date. It should be checked periodically and expired documents replaced with copies of newly issued documents.

Occasional transaction

4.9 An occasional transaction is a transaction of (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

4.10 Politically exposed persons are persons that are entrusted with prominent public functions, held in the UK or abroad. Typically this includes:

- heads of state, heads of government, ministers and deputy or assistant ministers
- members of parliament or similar bodies
- members of the governing bodies of political parties
- members of supreme and constitutional courts and other high level judicial bodies
- members of courts of auditors or boards of central banks
- ambassadors, and high ranking officers in the armed forces
- members of the administrative, management or supervisory bodies of state owned enterprises
- directors , deputy directors and members of the board, or equivalent of an international organisation

The definition includes family members such as spouse, partners, children (of the person and their spouse or partner) and parents and known close associates. Close associates are persons who have:

- joint legal ownership, with a politically exposed person, of a legal entity or arrangement
- any other close business relationship with a politically exposed person
- sole beneficial ownership of a legal entity or arrangement set up for the benefit of a politically exposed person

Beneficial owner

4.11 For a corporate body that is not a company whose securities are listed on the regulated market, a beneficial owner is any individual who:

- owns or controls over 25% of the shares or voting rights
- ultimately owns or controls whether directly or indirectly including bearer shares holdings or other means, more than 25% share or voting rights in the business
- exercises ultimate control over the management
- controls the corporate body

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

4.13 For a partnership, a beneficial owner is any individual who:

- owns more than 25% of the capital or profits of the partnership
- more than 25% of the voting rights in the partnership
- exercises ultimate control over the management

4.14 For a trust, a beneficial owner includes:

- the settlor
- the trustees
- the beneficiaries or the individuals who benefit from the trust and in whose main interest the trust is set up
- individuals who exercise control over the trust

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

- dispose of, advance, lend, invest, pay or apply trust property;
- approve proposed trust distributions;
- vary or terminate the trust;
- add or remove a person as a beneficiary or to or from a class of beneficiaries;
- approve the appointment of an agent or adviser;
- appoint or remove trustees or give another individual control over the trust;
- resolve disputes amongst the trustees;
- direct, withhold consent to or veto the exercise of a power mentioned above

4.16 For a foundation or other legal arrangement similar to a trust the beneficial owner includes the individuals with similar positions to a trust.

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

- individuals who benefit from the entity’s property
- where beneficiaries have not been established, the class of persons in whose main interest

the entity or arrangement is set up or operates
- any individual who exercises control over the property

4.18 For the estate of a deceased person in the course of administration, a 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

A beneficial owner in any other case is the individual who ultimately owns or controls the entity or on whose behalf a transaction is being conducted

Extent of customer due diligence measures

4.19 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.
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.

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

4.20 Your business may apply a simplified form of due diligence in some cases. You will have to risk assess the customer to establish that they are low risk. You don't have to verify a customer's identity, nor a beneficial owner's identity. Also you don't need to ask for additional information about the nature or purpose of a business relationship.

Simplified due diligence is where the business relationship or transaction is considered low risk in terms of money laundering or terrorist financing. It can apply to any customer you assess as low risk with some exceptions.

4.21 To apply simplified due diligence you need to ensure that:

- your decision is supported by your customer risk assessment
- enhanced due diligence does not apply
- you monitor the business relationship or transactions to ensure that there is nothing unusual or suspicious
- it is not prevented by information on risk provided by HMRC or any other authority
- the customer is not from a high risk third country identified by the EU
- the customer is not a politically exposed person, a family member or a known close associate of a politically exposed person
- the customer is seen face to face as is any co-owner
- the source of funds or wealth are transparent and understood by your business
- the transaction is not complex or unusually large, that is, over £1 million although your risk assessment may indicate that a lower sum would be considered large in your geographical location
- where the customer is not an individual, that there is no beneficial ownership beyond that legal entity.

4.22 To decide whether a customer is suitable for simplified due diligence you should consider among other factors the type of customer, the underlying product or service and the geographical factors, in your risk assessment. One factor, on its own, should not be taken to indicate low risk.

4.23 Type of customer that may indicate lower risk:

- a public authority or publicly owned body in the UK
- a financial institution that is itself subject to anti-money laundering supervision or equivalent 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
- the customer is a European Community institution

4.24 The underlying types of transaction that may indicate lower risk:

- a life insurance policy with a low premium
- a pension scheme insurance policy with no surrender or collateral value
- an employee pension scheme providing retirement benefits by way of deductions from wages and where an assignment to another person is not allowed
- junior ISA
- child trust fund
- financial products where ownership is transparent, understood and they have a limited value

4.25 Geographical factors that may indicate a lower risk are where the customer is:

- resident or established in another EU state
- situated outside the EU in a country:
  - subject to equivalent anti-money laundering measures
  - with a low level of corruption or terrorism
  - has been assessed by organisations such as Financial Action Task Force (FATF) and the World Bank as having in place effective anti- money laundering measures

You must consider all of the factors, for example a customer from another EU state is not automatically low risk simply because they are from the EU. All of the information you have on a customer must indicate a lower risk.

4.26 You'll need to record evidence, as part of your risk assessment, that a customer or service provided is eligible for simplified due diligence. You'll also need to conduct ongoing monitoring in line with your risk assessment to ensure that the circumstances on which you based your original assessment have not changed.

4.27 Where a person says that they are representing a customer who may be low risk you should check that they have the authority to act for them or are an employee.

4.28 You should not automatically assume that a customer is low risk to avoid doing an appropriate level of customer due diligence. Persons or businesses well established in the community or persons of professional standing or who you have known for some time, may merit being categorised as low risk but you still must have evidence to base this decision on.

4.29 A business or person who has strong links to the community, is well established with a clear history, is credible and open, does not have a complex company structure, where the source of funds are transparent and where there are no other indicators of higher risk may be suitable, subject to your risk assessment, for simplified due diligence.

Your decisions may be tested on the basis of the evidence that your business holds.

4.30 You must not continue with simplified due diligence if you:

- suspect money laundering or terrorist financing
- doubt whether documents obtained for identification are genuine
- circumstances change and your risk assessment no longer considers the customer, transactions or location as low risk

Enhanced due diligence

4.31 Enhanced due diligence applies in situations that are high risk. It means taking additional measures to identify and verify the customer identity and source of funds and doing additional ongoing monitoring.

4.32 You must do this when:

- you have identified in your risk assessment that there is a high risk of money laundering or terrorist financing
- HMRC or another supervisory or law enforcement authority provide information that a particular situation is high risk
- a customer or other party is from a high risk third country identified by the EU
- a person has given you false or stolen documents to identify themselves (immediately consider reporting this as suspicious activity)
- a customer is a politically exposed person, an immediate family member or a close associate of a politically exposed person
- the transaction is complex, unusually large or with an unusual pattern and have no apparent legal or economic purpose

4.33 A branch or subsidiary of an EU entity located in a high risk third country who fully complies with the parents' anti-money laundering policies and procedures and where the parent is supervised under the 4th Directive may not be subject to enhanced due diligence if your risk assessment finds it is not high risk.

You should consider a number of factors in your risk assessment when deciding if enhanced due diligence needs to be applied. The following are some examples of things to take account of.

4.34 Customer factors based on information you have or behaviours indicating higher risk, such as:

- unusual aspects of a business relationship
- a person is resident in a high risk area
- use of a legal person or arrangement used to hold personal assets
- a company with nominee shareholders or share in bearer form
- a person or business that has an abundance of cash
- an unusual or complex company structure given the nature of the type of business
- searches on a person or associates show, for example, adverse media attention, disqualification as a director or convictions for dishonesty

4.35 How the transaction is paid for or specific requests to do things in a certain way may indicate higher risk, for example:

- Use of private banking
- anonymity is preferred
- a person is not physically present
- payment from third parties with no obvious association
- involves nominee directors, nominee shareholders or shadow directors, or a company formation is in a third country

4.36 Geographical factors indicating higher risk, including:

- Countries identified by a credible source as:
  - not subject to equivalent anti-money laundering or counter terrorist measures
  - with a significant level of corruption, terrorism or supply of illicit drugs
  - subject to sanctions or embargoes issued by EU or UN
  - providing funding or support for terrorism
  - having organisations designated as “proscribed” by the UK
  - having terrorist organisations designated by the EU, other countries and international organisations
- has been assessed by organisations such as FATF, World Bank, Organisation for Economic Co-operation and Development and the International Monetary Fund as not implementing measures to counter money laundering and terrorist financing that are consistent with the FATF recommendations

Additional measures to take

4.37 If enhanced due diligence is appropriate, then you must do more to verify identity and scrutinise the background and nature of the transactions than for standard customer due diligence, for example at least:

- obtain additional information or evidence to establish the identity
- take additional measures to verify the documents supplied, or require certification by a bank, financial institution, solicitor or notary
- ensure the first payment is made through a bank account in the name of the customer
- take more steps to understand the history, ownership, and financial situation of the parties to the transaction
- establish the source of wealth and source of funds
- carry out more scrutiny of the business relationship and satisfy yourself that it is consistent with the stated purpose

4.38 A certified document should have:

- a statement that the document is " Certified to be a true copy of the original seen by me' , and where appropriate, "This is a true likeness of the person"
- an official stamp of the person certifying
- Signed and dated with a printed name
- occupation, address and telephone number

Politically exposed person's risk

4.39 You must always apply enhanced due diligence on politically exposed persons, their family members or a known close associate of one. You must have systems in place to determine whether a customer is a politically exposed person or a family member or known close associate of one.

4.40 If the customer is a politically exposed person, family member or known close associate of one, 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 or transaction
- conduct enhanced ongoing monitoring where you've entered into a business relationship

4.41 You must continue to apply enhanced due diligence when the politically exposed person has left the function or position and for a further period of 12 months.

4.42 For family members and close associates the obligation to apply enhanced due diligence stops as soon as the politically exposed person no longer holds the office.

4.43 You must assess the level of risk that the politically exposed person presents and apply an appropriate level of enhanced due diligence.

4.44 The level of risk of a politically exposed person may vary depending on where they are from and the public accountability they are subject to. The following are examples only.
A lower risk politically exposed person may be one who holds office in a country, similar to the UK, with traits such as:

- low levels of corruption
- political stability and free and fair elections
- strong state institutions where accountability is normal
- credible anti-money laundering measures

- a free press with a track record for probing official misconduct
- an independent judiciary and a criminal justice system free from political interference
- a track record for investigating political corruption and taking action against wrongdoers
- strong traditions of audit within the public sector
- legal protections for whistle blowers
- well-developed registries for ownership of land, companies and equities

A politically exposed person may be a lower risk if they are, for example:

- subject to rigorous disclosure requirements such as registers of interests or independent oversight of expenses
- a government MP with no ministerial responsibility or an opposition MP
- have not been a politically exposed person for at least 12 months.

4.45 A high risk politically exposed person may be from, or connected to, a country with traits such as:

- high levels of corruption
- political instability
- weak state institutions
- weak anti-money laundering measures
- armed conflict
- non-democratic forms of government
- widespread organised criminality or illicit drug supply
- a political economy dominated by monopolies with close links to the state
- lacking a free press and where legal or other measures constrain journalistic investigation
- a criminal justice system that suffers from political interference
- lacking expertise and skills related to book-keeping, accountancy and audit, particularly in the public sector
- law and culture hostile to the interests of whistle blowers
- weaknesses in the transparency of registries of ownership for companies, land and equities

4.46 A high risk politically exposed person may show characteristics such as:

- lifestyle or wealth does not match what you know of their income source
- credible allegations of financial misconduct have been made in relation to bribery or dishonesty
- there is evidence they have sought to hide the nature of their financial situation
- has responsibility for or can influence the awarding of large procurement contract where the process lacks transparency
- has responsibility for or can influence the allocation of government grant of licenses such as energy, mining or permission for major construction projects

4.47 A family member or close associate of a politically exposed person may pose a lower risk if they:

- are related or associated with a PEP who poses a lower risk;
- are related or associated with a PEP who is no longer in office
- are under 18 years of age.

4.48 The family and close associates of a politically exposed person may pose a higher risk if they have:

- wealth derived from the granting of government licences or contracts such as energy, mining or permission for major construction projects
- wealth derived from preferential access to the privatisation of former state assets
- wealth derived from commerce in industry sectors associated with high-barriers to entry or a lack of competition, particularly where these barriers stem from law, regulation or other government policy
- wealth or lifestyle inconsistent with known legitimate sources of income or wealth
- subject to credible allegations of financial misconduct made in relation to bribery or dishonesty
- appointment to a public office that appears inconsistent with personal merit

4.49 You must always apply enhanced due diligence to politically exposed persons, their family members and close associates. However, where your risk assessment indicates a lower risk, the politically exposed person, family member and close associates may be subject to less scrutiny than those who present a higher risk, for example:

- supervision is at a less senior management level
- source of wealth and funds establish from known information or publicly available information only
- ongoing monitoring is less intensive

Customer due diligence on transactions below €15,000

4.50 For transactions below €15,000 (or the sterling equivalent) where there's no ongoing business relationship you must 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.

Money transmission businesses must obtain information on the payer and payee and verify the payer information on electronic transactions of more than €1,000 (or the sterling equivalent) and any cash transaction or anonymous e-money to comply with the Regulation. However, HMRC expects that money transmission businesses should obtain and verify the identity of customers for all money transfers, regardless of value.

Linked transactions

4.51 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.
The value of the transaction here means the gross value of the transaction, not the value of your commissions, fees or charges.

4.52 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.
If you conduct business through branches or agents, your systems should be able to identify linked transactions that are conducted through all your locations.

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 individuals

4.53 As part of your customer due diligence measures, you must identify individuals. You should obtain a private individual's full name, date of birth and residential address as a minimum.

You should verify these using current government issued documents with the customer's full name and photo, with a customer's date of birth or residential address such as:

- a valid passport
- a valid photo card driving licence (full or provisional)
- a national identity card
- a firearms certificate
- an identity card issued by the Electoral Office for Northern Ireland

4.54 When verifying the identity of a customer using the above list of government-issued

documents you should take a copy and keep it in the customer's file.
Where the customer doesn't have one of the above documents 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, for example an old style driving licence or recent evidence of entitlement to state or local authority funded benefit such as housing benefit, council tax benefit, pension, tax credit
- secondary evidence of the customer's address, not downloaded from the internet, for example a utility bill, bank, building society or credit union statement or a most recent mortgage statement

4.55 If you verify the customer's identity by documents, you must see the originals and not accept photocopies, nor accept downloads of bills, unless certified (see "Additional measures to take") 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 it is a true copy and the person is who they say they are
- for standard customer due diligence an appropriate person is, for example, a bank, financial institution, solicitor or notary, independent professional person, a family doctor, chartered accountant, civil servant, or minister of religion

The documents must be from a reliable source not connected to the customer.

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

- spellings
- validity
- photo likeness
- whether addresses match

4.57 More information on official documents and how to spot counterfeits and forgeries is published by the Home Office in their 'Basic Guide to Forgery Awareness'. The Nominated Officer, or other responsible person, should be aware of the issues within this and cascade relevant parts to staff as part of their training programme:

http://www.devonaudit.gov.uk/wp-content/uploads/downloads/2015/03/Recognising_Fraudulent_Identity_Documents_v3.pdf

4.58 If a member of staff has visited an individual at their home address, a record of the visit may corroborate the individual's residential address (instead of the need for a second document). This should be covered in the risk assessment.

Where an agent, representative or any other person acts on behalf of the customer you must ensure that they are authorised to do so, identify them and verify the identity using documents from a reliable and independent source.

Electronic verification

4.59 If you verify an individual's identity electronically, you should:

- use multiple positive information sources, such as addresses or bill payment
- use negative sources, such as databases identifying identify fraud and deceased persons
- use data from multiple origins collected over a period of time
- incorporate checks that assess the strength of the information supplied.

4.60 if using an service provider you should ensure that it is reliable and accurate using extensive source data. You should consider the following criteria in your selection:

- it is registered with the Information Commissioner's Office to store personal data
- it is accredited to give identity verification services through a government, industry or trade association process that involves meeting minimum standards
- the standards it works to, or accreditation, require its information to be kept up to date
- it's compliance with the standards are assessed
- it uses a range positive information sources, and links a person, through other sources, to both current and previous circumstances
- it uses negative information sources, such as databases relating to identity fraud and deceased persons
- it uses a wide range of alert source, such as up to date financial sanctions information
- it has transparent processes that enable the firm to know what checks were carried out, what the results of these checks were, and what they mean in terms of how much certainty they give as to the identity of the subject.
- should be able to keep records of the information used to verify identity information

4.61 You should ensure that you understand the meaning of the electronic checks results so that you can satisfy yourself that they meet an appropriate level of confirmation for the risk assessed for the person and that you have further information to support and interpret the check. You must ensure that you understand the services they supply, the datasets they use and the scoring system for pass/fail.

4.62 An electronic records check establishes that an individual exists, not that your customer is that individual. Simply carrying out electronic verification to check the name and address of a customer you have not seen does not mean that you have verified that the person you are dealing with is who they say they are.

4.63 You should ensure that the checks you use show that you have identified the customer, verified the identity and that they are, in fact, the same person that is using your services. You should therefore verify key confidential facts, obtained from independent sources that only the customer may know to establish who they say they are. For example testing background information like their place of birth, how long they have been resident at an address with previous addresses when resident for a short period or education history.

4.64 Manual identity documents can be checked alongside electronic verification where greater risk is indicated. See the additional measures to take for enhanced due diligence.

4.65 An electronic records check is not always appropriate. For example, the Council for Mortgage Lenders notes that electronic verification products may not be suitable for fraud prevention purposes, such as verifying that a person's signature is genuine.

Individuals not resident in the UK

4.66 You should obtain the same types of identity documents for non UK residents as for UK residents.
If you have concerns that an identity document might not be genuine, contact the relevant embassy or consulate.

If documents are in a foreign language, you must satisfy yourself that they do in fact provide evidence of the customer’s identity. HMRC may require official translations when inspecting your customer due diligence records.

Identifying organisations as customers

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

- the full name of the company
- company or other registration number
- registered address and principal place of business

4.68 For private or unlisted companies you must take reasonable steps to obtain and verify:

- country of incorporation
- names of the members of management body, or if none, its equivalent and the name of the senior person responsible for the company

4.69 It will also be necessary to establish the beneficial owners of such entities, that is, for private or unlisted companies, 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.
You must verify the identity through reliable, independent sources that are relevant to that type of entity. For example:

- searching a relevant company registry
- obtaining a copy of the company's certificate of incorporation

Where an individual claims to act on behalf of a seller or buyer, you must also obtain evidence that the individual has the authority to act for them, identify the individual and verify the identity.

Obligation of customers to provide information

4.70 Corporate bodies in the UK, who are not listed on a regulated market, have obligations to keep a register of people with significant control (a PSC register) and must provide this information when requested. When a corporate person enters into a transaction with a money service business you can request that they provide you with the following information:

- name, registered number, registered office and principal place of business
- names of the board of directors or equivalent body
- names of the senior person responsible for its operations
- the law to which it is subject
- its legal and beneficial owners
- its memorandum of association or similar documents

Guidance on the requirements to maintain PSC registers is available at:

https://www.gov.uk/government/publications/guidance-to-the-people-with-significant-control-requirements-for-companies-and-limited-liability-partnerships

4.71 This information will assist in identifying beneficial owners but it will not provide you with all the information you need to verify their identity, for example, the address or date of birth of the individual.

Trustees have similar obligations to tell you that they are acting as a trustee, to identify all of the beneficial owners of the trust and any other person that may benefit.

The customer must notify you of any changes to the information supplied.

Beneficial owners

4.72 You must identify the existence of any beneficial owners (the section on customer due diligence gives information on who is a beneficial owner). You must verify the beneficial owner's identity so that you are satisfied that you know who the beneficial owner is. If it is a legal person you must take reasonable measures to understand the ownership structure.
You will not have satisfied your obligation to identify, verify and understand the structure of a beneficial ownership if you rely solely on the information contained in a register of persons with significant control.

Where a customer is incorporated and in exceptional circumstances, where you have made unsuccessful attempts, and have exhausted all ways, to identify the beneficial owner of a corporate body you may treat the most senior person managing the customer as the beneficial owner. You must keep records of all the steps you have taken to identify the beneficial owner and why they have been unsuccessful.

Reliance on third parties

4.73 You can rely on the following persons to apply customer due diligence for you before entering into a business relationship with a customer:

- another UK business subject to the Regulations
- a business in the European Economic Area (EEA) subject to the 4th Money Laundering Directive
- a branch or subsidiary established in a high risk third country who fully complies with an EEA parent’s procedures and policies
- a business in a third country who is subject to equivalent measures

You may not rely on a business established in a country that has been identified by the EU as a high risk third country.

4.74 The third party must agree that you will rely on them. The agreement must include arrangements to:

- obtain immediately on request (or within 2 working days) copies of the customer due diligence information from the third party
- ensure the third party retains copies of the due diligence information for five years from the date the reliance was agreed

4.75 If you rely on a third party you will remain responsible for any failure to apply due diligence measures appropriately. This is particularly important when relying on a person outside the UK. It may not always be appropriate to rely on another person to undertake your customer due diligence checks and you should consider reliance as a risk in itself.

When you rely on a third party to undertake due diligence checks, you will still need to do your own risk assessment of the customer and the transaction and you must still carry on monitoring the business relationship.

Reliance does not include accepting information from others to verify a person's identity for your own customer due diligence obligations, nor electronic verification, which constitutes outsourcing a service.

You must not rely on simplified due diligence carried out by a third party or any other exceptional form of verification, such as the use of source of funds as evidence of identity.

See also the section on undertaking business with another money service business that is not your agent (sections 6.16 and 6.17).

5. Money transmitters - additional obligations

5.1 Money transmission businesses must comply with Regulation (EU) 2015/847 on information on the payer and payee accompanying transfers of funds. This EU legislation has direct effect in the UK and it lays out the information that must be sent with a transfer of funds. The rules apply to all transfers of funds in any currency that you send or receive.

5.2 This does not apply to bill payment service providers and telecommunication, digital and IT payment service providers.

5.3 You must not carry out a transaction if you cannot provide the information and verify it.

The money transmitter for the "payer" must:

- send the information on the payer and payee to the payment service provider for the payee

For transfers outside the EU:

- obtain complete information on the payer and payee for all customers wanting to transmit money where the transaction is over €1,000
- obtain payer and payee names, payment account numbers or unique transaction ID if transaction is €1,000 or less and it does not appear to be linked
- 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
    - €1,000 or less and the funds were received in cash or anonymous e money or money laundering or terrorist financing is suspected

For transfers inside the EU:

- obtain payer and payee names, payment account numbers or unique transaction identifier where the transaction is over €1,000
- verify the information on the payer on the basis of documents data or information from a reliable independent source where the transaction is:
    - over €1,000
    - €1,000 or less and the funds were received in cash or anonymous e money or money laundering or terrorist financing is suspected

5.4 The money transmitter for the “payee” must:

- verify the information on the payee, before crediting the payees account, or making the funds available to the payee, on the basis of documents data or information from a reliable independent source where the transaction is over €1,000
- verify the information on the payee, before crediting the payees account, or making the funds available to the payee, where the transaction is €1,000 or less if the pay-out is in cash or anonymous electronic money or money laundering or terrorist financing is suspected
- have effective procedures to detect missing or incomplete information on the payer and payee and implement a risk based approach, taking account of the risk in each case, in deciding whether a transaction will be accepted, suspended or rejected
- ask for the information on the payer and payee, or reject the transaction, where it is missing or incomplete on a risk sensitive basis, before crediting the amount to the payee
- consider warning or ending a business relationship with a payment service provider where they repeatedly fail to provide the information required and report the failure and steps taken to HMRC
- where missing or incomplete information is suspicious consider making a suspicious activity report

5.5 An intermediary money transmitter, who acts between a payer and payee money transmitter, must:

- ensure the payer and payee information stays with the transfer
- have effective procedures to detect missing or incomplete information on the payer and payee and implement a risk based approach, taking account of the risk in each case, in deciding whether a transaction will be accepted, suspended or rejected
- ask for the information on the payer and payee, or reject the transaction, where it is missing or incomplete on a risk sensitive basis, before crediting the amount to the payee
- consider warning or ending a business relationship with a payment service provider where they repeatedly fail to provide the information required and report the failure and steps taken to HMRC
- where missing or incomplete information is suspicious consider making a suspicious activity report

Information accompanying transfer of funds

5.6 The complete information on the payer must consist of:

- the payer’s name
- the payer’s 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

5.7 The complete information on the payee must consist of:

- the payee name
- the payee's account number or where the payee doesn't have an account number a unique identifier that allows tracing of the transaction to the payer

5.8 As an alternative to the payer's 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)

5.9 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.

6.1 These are minimum requirements, a money transmitter may decide to provide complete information, where reduced information is permitted, to limit the requests for complete information from a payee money transmitter.

6.1 Information on the payer and the payee must be retained for a period of five years. This may be extended for a further five years where a criminal investigation or legal proceedings are carried out.

Exclusions

6.1 The rules do not apply to transfer of funds:

- that involve the payer withdrawing cash from the payer's own payment account
- that transfer funds to a public authority to pay taxes, fines or other levies within a Member State
- where both the payer and the payee are payment service providers acting on their own behalf
- that are carried out through cheque images exchanges, including truncated cheques.
- using payment cards, electronic money instruments, mobile phones or other digital or information technology (IT) prepaid or post-paid devices with similar characteristics, where they are used exclusively for the purchase of goods or services and the number of the card (16 digit PAN number), instrument or device accompanies all transfers

  However, the use of a payment card, an electronic money instrument, a mobile phone, or any other digital or IT prepaid or post-paid device with similar characteristics in order to effect a person-to-person transfer of funds, falls within the scope of this Regulation.

6. Reporting suspicious activity

Core obligations ● Staff must raise an internal report where they know or suspect, or where there are reasonable grounds for having knowledge or suspicion, that another person is engaged in money laundering, or that a terrorist finance offence may be committed. ● The business's nominated officer must consider all internal reports. The nominated officer must make a report to the National Crime Agency (NCA) as soon as it is practical to do so, even if no transaction takes place, if they consider that there is knowledge, suspicion or reasonable grounds for knowledge or suspicion that another person is engaged in money laundering, or financing terrorism. ● The business must consider whether it needs to seek a defence to a money laundering or terrorist financing offence (consent) from the NCA before proceeding with a suspicious transaction or entering into arrangements. ● It is 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: ● 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 NCA about a suspicious transaction report

Suspicious activity reports ("SARs")

6.1 This is the name given to a report sent to the NCA under the Proceeds of Crime Act or the Terrorism Act. The report identifies individuals who you, or an employee, suspect may be involved in laundering money or financing terrorism. The term suspicion is meant to be applied in its everyday, normal sense. But if you are still not sure of the meaning of suspicious, then the courts have said that 'it is a possibility that is more than fanciful'.

6.2 The suspicion is that the funds or property involved in the transaction is the proceeds of any crime or linked to terrorist activity. You do not have to know what sort of crime may have been committed, but one or more warning signs of money laundering, which cannot be explained by the customer, will be relevant.

6.3 As a money service business in the regulated sector, you are also required to make a Suspicious Activity Report (SAR) as soon as possible after you know or suspect that money laundering or terrorist financing is happening. This means that the facts you have about the persons involved and the transaction would cause a reasonable person in your position to have a suspicion. There is guidance about submitting a SAR within the regulated sector in the How to report SARs section of the NCA website. The NCA document "Guidance on Submitting Better Quality SARs" takes you through the information you should provide and the SAR glossary codes you should use.

6.4 You can submit a suspicious activity report to the NCA by registering with the NCA online. The NCA provide information and registration details online and the NCA prefers this method. The system doesn't retain a file copy for your use, so you may wish to keep a copy of your report but this must be securely kept. This system lets you:

- register your business and contact persons
- receive a welcome pack with advice and contact details
- submit a report at any time of day
- receive email confirmation of each report.

6.5 The NCA also issues report forms for you to fill in manually but you will not receive an acknowledgement of a report sent this way. For help in submitting a report or with online reporting to the NCA contact the UK Financial Intelligence Unit (UK FIU) helpdesk - Telephone: 020 7238 8282 or online at NCA.

Submitting a request for a defence to the NCA, whether you are granted a defence, or not, does not replace the requirement on the business to complete customer due diligence before entering into a business relationship (see Defence SAR below). It is important that you have detailed policies, controls and procedures on internal reporting and the roll of the nominated officer (see nominated officer below).

You must provide regular training for your staff in what suspicious activity may look like in your business and you should keep records of that training, who has received it and when. The nominated officer must be conversant with guidance on how to submit a report and in particular be aware of the codes detailed in the glossary that must be used in each report.

6.6 A suspicious activity report must be made to the NCA no matter what part of your business the suspicion arises in. The tests for making a report about terrorist financing are similar. You must make a report if you know, suspect or had reasonable grounds for knowing or suspecting that another person committed or attempted to commit a terrorist financing offence.

Nominated officer

6.7 You must appoint a nominated officer to make reports (see suspicious activity reports) from within your registered business. 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.

6.8 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.

6.9 A sole trader with no employees does not need a nominated officer as they are the nominated officer by default.

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

6.11 If a report is made before a transaction is completed or the start of a business relationship, you must ask for a defence to a money laundering or terrorist financing offence from the NCA to go ahead with the transaction. You should tick the “consent requested” box on the SAR form.

A defence (consent)

6.12 It is an offence for the nominated officer to proceed with a transaction prior to receiving a granted letter from the NCA within the 7 working day statutory time period”. This period starts from the day after submitting the report.

6.13 A defence relates to offences in Proceeds of Crime Act and the Terrorism Act but not to other criminal offences.

6.14 Seeking a defence, granting it or no reply from the NCA is not a permission to proceed or oblige you to proceed, nor is it an approval of an act or persons, or mean that there is no criminality involved. You should consider your position carefully. A defence does not mean you do not have to verify a customer's identity or that of any beneficial owners. The business must continue to comply with all the requirements of the Regulations.

6.15 If you do not receive a refusal notification from the NCA within the notice period it is up to you to interpret your position and you may. If you consider that you have met the requirements for making a disclosure assume a defence.

6.16 If the NCA refuses you a defence, you must not proceed with a transaction for up to a further 31 calendar days, i.e. the moratorium period. In terrorist financing cases the moratorium period does not apply, you do not have a defence until a request is granted.

6.17 The NCA has published information on obtaining a defence. Some of the key points include:

- a defence 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 a general defence 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 a defence is refused, the moratorium period is a further 31 calendar days from the date of refusal - if you need a defence sooner, you should clearly state the reasons for the urgency and perhaps contact the National Crime Agency to discuss the situation
- the National Crime Agency will contact you by telephone you and will confirm their decision in writing

Tipping off

6.18 It is 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 or terrorist financing investigation may be carried out. It is also an offence to falsify, conceal or destroy documents relevant to investigations.

Do not tell or inform the person ordering the transaction or anyone else that:

- the transaction is being or was delayed because a suspicion has been raised
- details of a transaction have or will be reported to the NCA
- law enforcement agencies are investigating the customer

Such an offence carries a penalty of up to 5 years imprisonment and/or a fine.

Suspicious activity

6.19 Here are some warning signs of potentially suspicious activity that your systems should be capable of picking up and flagging for attention. This is not an exhaustive list, and these signs aren't always suspicious. It depends on the circumstances of each case. More specific examples for each type of money service business are at section 10.

New customers

6.20 These are some of the questions to consider in deciding risk and whether or not to submit a suspicious activity report when you take on new customers:

- 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
- they, or associates, are subject to, for example, adverse media attention, have been disqualified as directors or have convictions for dishonesty

Regular and existing customers

6.21 These are some of the questions to consider when deciding risk and whether or not to submit a suspicious activity report 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

6.22 These are some of the questions to consider when deciding risk and whether or not to submit a suspicious activity report 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

7. Record keeping

<table>
<tr><td>
Core obligations
You must retain:

copies of the evidence obtained of a customer’s identity for five years after the end of the business relationship
details of customer transactions for five 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 a suspicious activity report
copies of the evidence obtained if you are relied on by another person to carry out customer due diligence, for five years from the date of the agreement, the agreement should be in writing

You must also maintain:

a written record of your risk assessment
a written record of your policies, controls and procedure

</td></tr>
<tr><td>
Actions required
The points below are to be kept under regular review:

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

</td></tr>
</table>

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

- for 5 years after the end of the business relationship
- for 5 years from the date an occasional transaction was completed
- you should also keep supporting records for 5 years after the end of a business relationship
- you should keep records from closed branches or agents

The records should be reviewed periodically to ensure, for example, that a fresh copy of expired documents is held.

After the period above the records can be deleted unless you are required to keep them in relation to legal or court proceedings. You will not be required to keep them for more than twenty five years.

7.2 Your risk assessment and policies, controls and procedures must be kept up to date and be amended to reflect any changes in your business.

7.3 You can keep records in the form of original documents or copies in either hard copy 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.

7.4 If someone else carries out customer due diligence for you, you must make sure that they also comply with these record keeping requirements. You must be able to demonstrate that records of customer due diligence checks carried out by an outsourcing service, and which are stored on their server, will be available to you should you wish to move to another service or should that service go into liquidation.

All electronic records must be subject to regular and routine backup with off-site storage.

8. Staff awareness and training

Core obligations You must: ● ensure relevant staff and agents (and the agents 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 ● staff and agents are trained at regular intervals ● maintain a written record of what you have done to raise awareness and the training given to staff ● ensure that a relevant director or senior manager has overall responsibility for establishing and maintaining effective training arrangements. Larger and more complex businesses must: ● Screen relevant staff and agents before they take up post and during the course of the appointment assess that they are effective in carrying out their function and are of good conduct and integrity
Actions required The points below are to be kept under regular review: ● appropriate training to make relevant staff and agents aware of money laundering and terrorist financing risks, including how these crimes operate and how they might take place through the business ● ensure that relevant employees and agents have information on, and understand, the legal obligations of the business - individual members of staff and any changes to these obligations ● regularly share risk assessment, policy, control and procedures information within the business and with branches and subsidiaries ● consider providing relevant staff and agents with case studies and examples related to the firm's business ● train relevant staff and agents in how to operate a risk based approach to assessing the risks of money laundering and terrorist financing ● provide IT and system security training to staff who have access to it ● larger businesses must set up a system to screen staff and agents before they take up the post and at intervals ● keep records of training given

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

You must:

- tell your staff and agents about your anti-money laundering and counter terrorism financing obligations and the risk of IT systems being abused
- give them suitable (risk based) training on their legal obligations
- tell them how to identify and deal with the risks
- make them aware of data protection obligations

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

8.2 Relevant staff or agents are persons who are engaged in your compliance with the Regulations, are able to contribute to the identification or mitigation of risk or protection or detection of the money laundering and terrorist financing threat that your business may face.

Training

8.3 When you consider who needs to be trained you should include staff and agents who deal with your customers, deal with money or help with compliance. Think about reception staff, administration staff and finance staff, because they'll each have a different involvement in compliance, and have different training needs.

8.4 The training process should therefore cover the whole end to end process from sales and receiving customers' instructions, through to valuation, dealing with offers and completion.

8.5 Nominated officers, senior managers and anyone who is 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.

8.6 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 policies and procedures
- how to conduct customer due diligence and check customers' documents
- how to spot and deal with suspicious customers and activity

- how to make internal reports, including disclosures of suspicious activity
- data protection requirements
- record keeping
- the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017; Part 7 of the Proceeds of Crime Act; and sections 18 and 21A of the Terrorism Act

Training may include:

- face-to-face training
- online training sessions
- HMRC webinars
- going to conferences
- taking part in special meetings to discuss the business procedures
- reading publications
- meetings to look at the issues and risks

8.7 A policy manual is useful to raise staff awareness and for reference between training sessions. Staff training is necessary when staff join the business, move to a new job or when they change roles. They should also have ongoing training at least every 2 years or when a significant change happens, depending on the level of risks.

You must keep evidence of your assessment of training needs and the steps you've taken to meet those needs. You may be asked to produce training records in court.

Training records include:

- a copy of the training materials
- details of who provided training, if provided externally
- a list of staff who have completed training, with dates, and their signatures (confirming their understanding of the obligations) or electronic training records
- an updated training schedule

9. Principal-agent relationships and other business models

10.1 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

10.1 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.

10.1 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'

10.1 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.

10.1 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

10.1 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

10.1 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.

10.1 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.

10.1 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.

10.1 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

10.1 HMRC expects principals to have clear agent selection criteria to support due diligence background checks, including on-site visits.

10.1 Any employer is under a legal obligation to ensure his staff have the right to work in the UK. It is also good practice for a principal to ensure that his agents meet their obligations to check their own employees.

10.1 An employer's duty in relation to right to work applies to agents and employees. Guidance can be found at:
https://www.gov.uk/government/publications/right-to-work-checks-employers-guide

A principal that does not screen their agents with due care is unlikely to be seen as fit and proper themselves.

Principals should ensure that an agent meets minimum expectations, in particular that:

- the beneficial owners, senior managers, officers and nominated officer 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
- they have the right to work in the UK and documents have been checked
- 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

10.1 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 5 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

10.1 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 is appropriate

Foreign currencies

10.1 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

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

10.1 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 4.70, 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 2015/847 on information on the payer accompanying transfers of funds

10.1 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

10.1 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 (2015/2366/EC).

Franchising

10.1 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.

10.1 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.

10.1 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.

10. Risk indicators for each type of money service business

10.1 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

Agents

10.2 The following are examples of common risk indicators that principals and agents need to be aware of:

- 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
- transactions too fast to be possible

Money transmitters

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

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.

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.

New customers

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

- 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

Transactions

10.5 The following are examples of common risk indicators where 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

10.6 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 and the EC 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

10.7 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 and payee 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

10.8 Third party payments are money transmissions, either from the UK to another country, (outbound remittance) or from another country to the UK (inwards remittance)", 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.

10.9 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

10.10 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.

New customers

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

- 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

Regular and existing customers

10.12 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

10.13 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

10.14 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

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

New customers

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

- they 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

Regular and existing customers

10.17 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

10.18 The sale of high value notes, in any currency, entails a significant money laundering risk. All the major UK banks and financial institutions have agreed not to sell €500, €200 and $100 notes. You should regard any request to buy or sell €500, €200 and $100 notes as potentially suspicious. You should refuse to sell €500, €200 and $100 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

10.19 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

10.20 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