Anti-Money Laundering Supervision: Money Service Businesses

Who this guidance is for

This guidance is addressed to firms, proprietors, directors, managers, employees, agents and Nominated Officers of money service businesses who are the subject of the Regulations. A money service business may be supervised by HMRC or the Financial Conduct Authority.

A money service business includes those who are money transmitters, cheque cashers or currency exchangers.

For further information on the businesses that fall within this sector, the registration requirements and processes for businesses supervised by HMRC, please see the Registration guidance.

General introduction

This guidance explains measures under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the Regulations), which came into force on 26 June 2017. The guidance also includes the changes brought about by the 2019 amendments, which came into force on 10 January 2020.

Meeting your legal obligations is important because it contributes to tackling the serious economic and social harm from organised crime. It also contributes to reducing 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 annual 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 both businesses' and agents' beneficial owners, officers and managers are appropriate people to undertake those roles. Relevant persons must pass the appropriate 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.

Registered businesses should avoid using language about their business 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 test and HMRC approval guidance.

Status of this guidance

This guidance has been approved by HM Treasury.

The 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 replaces HMRC's guidance: "Anti-money laundering guidance for money service businesses" published on 7 March 2018. The guidance is effective from 2 June 2020.

Meaning of key terms

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 these 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.

The words 'minimum requirements' is the legal minimum that your business is required to do. The words 'actions required' is what HMRC expects you to do to meet these legal requirements.

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 complete due diligence checks on different types of customers, report suspicious activity, and do staff training and record keeping.

The Joint Money Laundering Steering Group (JMLSG) publishes more information about businesses' obligations and the level of risk in other jurisdictions (Annex 4-1 of part 1)
http://www.jmlsg.org.uk/industry-guidance/article/jmlsg-guidance-current

The Financial Conduct Authority has published detailed guidance on the treatment of politically exposed persons for anti- money laundering purposes.

The European Supervisory Authorities Joint Committee has published guidelines on the measures payment service providers should take to detect missing or incomplete information on the payer and payee and The Risk Factors Guidelines on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions.

The National Crime Agency (NCA) has published guidance on making Suspicious Activity Reports (SARs) suspicious activity on their website: How to report SARs.

1. Introduction: money laundering and money service businesses

1.1 Money laundering is the process through with criminals disguise the criminal origin of money and assets they earned through criminal activity.

1.2 Money laundering takes many forms. Here are some examples detected by HM Revenue and Customs in the money transmission, currency exchange, and cheque cashing sectors:

- 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 in the UK to send the proceeds of illegal working to other countries
- 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

1.3 A person or an entity commits an offence of Terrorist Financing if they;

- fund-raise or are involved in fund-raising, using or possessing money or other property for the purposes of terrorism
- conceal, transfer or remove from jurisdiction, any money or other property used to finance terrorism
- facilitate the retention or control of money, which is destined for, or is the proceeds of terrorism
- do not comply with a prohibition imposed by a freezing order or enable any other person to contravene the freezing order
- deal with, or make available funds or economic resources which are owned, controlled by or benefitting a designated person (under the Office of Financial Sanctions Implementation List)

Legislation

1.4 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 these Regulations.

1.5 The main UK legislation covering anti-money laundering and counter-financing of terrorism include:

- 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
- Terrorist Asset-Freezing etc. Act 2010
- Anti-terrorism, Crime and Security Act 2001
- Counter-terrorism Act 2008, Schedule 7

1.6 Information on Sanctions can be found through:

- HMT Treasury Sanctions Notices, Guidance and News Releases

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

1.7 The following legislation applies to money transmission businesses only:

- Regulation (EU) 2015/847 on information accompanying transfers of funds (the Payments Regulation)
- Payment Services Regulations 2017

1.8 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

1.9 The primary money laundering offences apply to everyone.

1.10 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.

1.11 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, which can be found in 1.3.

1.12 The Criminal Finances Act 2017 makes important amendments to the Proceeds of Crime Act, the Terrorism Act and the Anti-terrorism, Crime and Security Act. It extends the powers of law enforcement to seek further information, recover the proceeds of crime and combat the financing of terrorism. It extends the powers of law enforcement to seek further information, recover the proceeds of crime and combat the financing of terrorism. It also introduces corporate offences of failing to prevent tax evasion which may apply to businesses who facilitate this criminal activity. HMRC has published guidance to help businesses put processes and procedures in place to prevent persons associated with the business from criminally facilitating tax evasion.

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

1.14 The Terrorist Asset-Freezing etc. Act 2010 gives HM Treasury power to freeze the assets of individuals and groups reasonably believed to be involved in terrorism, whether in UK or abroad, and to deprive them of access to financial resources.

1.15 The Anti-terrorism, Crime and Security Act 2001 is to ensure the security of dangerous substances that may be targeted or used by terrorist groups and allows for freezing orders to be made against national security threats and the civil asset seizure regime for terrorism.

1.16 Counter-terrorism Act 2008, Schedule 7 gives powers to HM Treasury to issue directions to firms in the financial sector in relation to customer due diligence, ongoing monitoring, systematic reporting and limiting or ceasing business.

1.17 HMT Treasury Sanctions Notices, Guidance and News Releases, the Office of Financial Sanctions Implementation (OFSI) publishes a list of all those subject to financial sanctions imposed by the UK. OFSI helps to ensure that these financial sanctions are properly understood through sanction notices, guidance and news releases.

1.18 As a supervisory authority HMRC is responsible for monitoring your compliance with the UK anti-money laundering regime. In its capacities as a supervisory authority and a law enforcement authority, HMRC may also use this regime to gather information for tax purposes.

Financial sanctions

1.19 EU financial sanctions (including where they implement UN sanctions) apply within the territory of the EU and to all EU persons, wherever they are in the world. UK financial sanctions apply within the territory of the UK and to all UK persons, wherever they are in the world.

1.20 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. All UK nationals and UK legal entities established under UK law, including their branches, must also comply with UK financial sanctions that are in force, irrespective of where their activities take place.

1.21 All EU nationals and legal entities established under EU law must comply with the EU financial sanctions that are in force, irrespective of where their activities take place.

1.22 OFSI works closely with the EU Commission and EU member states in implementing sanctions. The UK imposes sanctions applied by the UN and EU as well as a limited number of its own sanctions (e.g. Terrorist Asset-Freezing etc. Act 2010).

1.23 You must report to OFSI as soon as practicable if you know or have reasonable cause to suspect that a designated person has committed an offence. You should report any transactions carried out for persons subject to sanctions or if they try to use your services.

1.24 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-sanctionsimplementation

Data Protection

1.25 The data protection legislation, i.e. the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) governs the processing of information relating to individuals, including obtaining, holding, use or disclosure of information.

1.26 Personal data obtained by a business under the Regulations may only be processed for the prevention of money laundering and terrorist financing unless use of the data is allowed by other legislation or after obtaining the consent of the data subject.

1.27 You must provide new customers with a statement that personal data will only be used for the purposes of preventing money laundering and terrorist financing and provide them with the information as required under Article 13 of the GDPR. The information you must provide includes:

- the identity and the contact details of the controller and the controller's representative if they have one
- the contact details of the data protection officer, if you have one
- the reason you're processing the personal data, including the legal basis
- who will receive the personal data
- whether you intend to transfer the personal data outside of the UK, and if so, whether they have an EU data adequacy agreement, or appropriate safeguards
- how long you will store the personal data
- the existence of a right to request access to and deletion of personal data, including data portability
- the right to complain to the Information Commissioners Office
- whether providing the personal data is a statutory or contractual obligation and the possible consequence of failing to provide it
- the existence of any automated decision making, including profiling.

1.28 The processing of personal data in accordance with these Regulations is lawful and necessary for the prevention of money laundering or terrorist financing and is for the performance of a task carried out in the public interest.

Money Service Businesses

1.29 '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)

1.30 Money service businesses must comply with the Regulations. You must not carry on business as a money service business unless you are registered with HMRC. HMRC will contact you through your Government gateway account when your application for registration has been determined. If you have applied to register before 10 January 2020 but your application has not yet been determined, you can continue to trade as an MSB.

1.31 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 2017.

1.32 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 (FSMA) and provides currency exchange, money transmission or cheque cashing services then they will be supervised by the Financial Conduct Authority for all their activities under the Regulations. This does not include a consumer credit firm who carries out money service business activities (this only

apples to firms whose business model falls within the definition of an 'exempt money service business' in Regulation 7 (5) of the Regulations). The Financial Conduct Authority's notification requirements, and exceptions, for businesses authorised under FSMA can be found at: https://www.fca.org.uk/firms/money-laundering-terrorist-financing/reporting.

1.33 The Joint Money Laundering Steering Group (JMSLG) has produced equivalent guidance for firms supervised by the Financial Conduct Authority; and that guidance will be approved by HM Treasury for the purposes of the Regulations. 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 2017.

Penalties and sanctions

1.34 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.

1.35 HMRC also have the power to

- suspend or cancel a business' registration
- ban or suspend individuals from having a role in a supervised business
- issue a statement censuring the business.

1.36 HMRC will usually publish details of penalties and sanctions issued.

1.37 You can find information on the penalties HMRC can issue here.

1.38 Not complying with the Regulations may also lead to money laundering charges under the Proceeds of Crime Act 2002.

2. Responsibilities of senior managers

Senior managers

2.1 The senior managers of a money service business are responsible for the oversight of compliance with the Regulations and can be held personally liable if they don't take the steps necessary to protect their business from money laundering and terrorist financing.

2.2 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 can 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

2.3 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

2.4 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. They are also responsible for approving that risk assessment. Your policies, controls and procedures must address the level of risk that the business may encounter in different circumstances.

2.5 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 by subsidiaries, branches and agents).

Actions required

2.6 Senior managers must:

- ensure a risk assessment is carried out, identifying where your business is vulnerable to money laundering and terrorist financing
- ensure a written policy statement, controls and procedures are prepared, maintained and approved, to show how the business will manage the risks of money laundering and terrorist financing identified in risk assessments
- ensure the policies, controls and procedures are reviewed and updated to reflect changes to the risk faced by the business and written records of any changes are kept

2.7 Senior managers should also be involved in the responsibilities of the business to:

- 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

2.8 The risk assessment, policies, controls and procedures must be reviewed in response to changes to your business, the market, information from HMRC, and changes to relevant legislation. So as to ensure that your risk assessment accurately identifies and addresses the money laundering and terrorist financing risk to which your business is subject, your risk assessment should – in any event – be updated on at least an annual basis.

3. Risk assessment, policies, controls and procedures

Risk-based approach

3.1 A risk-based approach is where you assess the risks that your business may be used for money laundering or terrorist financing and put in place appropriate measures to manage and reduce those risks. An effective risk-based approach will identify the highest risks of money laundering and terrorist financing that your business faces and put in place measures to manage these risks.

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

3.3 A risk-based approach should balance the costs to your business and customers with a realistic assessment of the risk that your business may be exploited for the purpose of money laundering and terrorist financing. It allows you to use your informed judgement to focus your efforts on the highest-risk areas and reduce unnecessary burdens on customers presenting a limited risk of money laundering and/or terrorist financing.

Risks your business may face

3.4 Assessing the money laundering and financial risks your business faces is the first step to a risk-based approach. This will help you design the right systems to spot suspicious activity and ensure that staff are aware of what sort of indicators of possible money laundering they may encounter.

3.5 The risks your business faces depends on factors including the nature of your business, how it is structured (e.g. the branch network or your agent 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.

3.6 Specific risks in relation to money service businesses are covered in Risk indicators for each type of money service business. For each of these areas you must consider how your business could be exposed and put in place policies, controls and procedures to effectively address these. This generalised list is not exhaustive and will depend on individual business circumstances. An effective risk-based approach will require you to identify the risks facing your business, in view of your business' individual characteristics.

3.7 The FATF website also provides guidance on the risk based approach for money value transfer services.

Risk Assessment

3.8 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.

3.9 You must:

- Ensure your risk assessment identifies and monitors the risks of money laundering and terrorist financing that are relevant to your business, including those posed by your:
  - customers and any underlying beneficial owners (see sector guidance on customer due diligence on who is a 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

- take note of information on risk and emerging trends from sources including the National Risk Assessment and HMRCs risk assessment and amend your procedures as necessary

3.10 Your risk assessment must be in writing and kept up to date. It needs to reflect changes in your business and the environment that you do business in. At least an annual review of the risk assessment is recommended and any revisions must be noted in the document.

3.11 The risk assessment must be given to HMRC if we ask for it, as well as the information the risk assessment was based on, and any records you're required to keep of it.

3.12 In a limited range of circumstances, we may tell you that you do not need to keep a record of your risk assessment (if, for example, you are a sole practitioner with no employees, have a small number of well-established clients and where you understand your money laundering and terrorist financing risks). We do not expect that it will apply to many businesses given the complexity of money service businesses. Contact HMRC if you think this applies to you.

3.13 Specific risks in relation to money service businesses are covered in Risk indicators for each type of money service business.

Customers

3.14 Your business-wide risk assessment must take account of the full range of circumstances associated with your business model. The risk assessment must consider the risk factors relating to:

- Its customers
- the countries or geographic areas it operates in
- its products or services
- its transactions
- its delivery channels.

3.15 Your risk assessment should also include the following non-exhaustive list:

- if you accept customer introductions from an agent or third party, have you accepted customers from this source before
- are your customers companies, partnerships, trusts or some combination of these
- do you undertake business in areas with a highly transient population
- is your 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 those based in, or have beneficial owners in, tax havens, or countries with high levels of corruption or where terrorist organisations operate (Transparency International publish a corruption perception index)
- 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

3.16 Other situations that may present a higher risk and need to be considered in your risk assessment are covered in the enhanced due diligence.

3.17 See also Money Service Business risk which details some of the specific risks that your business may be subject to.

Policy, controls and procedures

Policy statement

3.18 Your policy statement must lay out your policy, controls and procedures and how you and other senior managers will manage the business' exposure to risk. It must be proportionate to the size and nature of your business. It must make clear how you'll manage 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.

3.19 Policies, controls and procedures must be approved by a senior manager, kept in writing and be communicated throughout your organisation to staff, branches, subsidiaries and agents in and outside the UK. It must also be regularly reviewed and updated. You must keep a record of any changes made.

Controls and procedures

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

3.21 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, identity of the 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. Conversely, the measures that you put in place to manage risks associated with lower-risk customers should be less onerous. The risk assessment that you conduct must underpin the nature of your measures for managing money laundering and terrorist financing risks.

3.22 When designing systems to identify and deal with suspicious activity, there are some warning signs of potentially suspicious activity that your systems should be capable of picking up and flagging for attention (see Examples of when you may consider making a SAR). You will always need to consider the circumstances of each case, which you will need to assess in the round.

Minimum requirements

3.23 Your policies, controls, and procedures must also show how you will:

- do customer due diligence checks and conduct ongoing monitoring
- identify when a customer or beneficial owner is a politically exposed person (PEP) or a family member or close associate of a PEP, and do appropriate levels of enhanced due diligence (as described later in this guidance)
- appoint a nominated officer to receive reports of suspicious activity from staff and make suspicious activity reports to the National Crime Agency
- make sure your staff and the staff of your agents 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
- review and update the business's policies, controls and procedures
- maintain accurate, up-to-date record keeping and retention of records

3.24 If you are an MSB principal that uses agents to provide your services, you must also:

- ensure that appropriate measures are taken by the business to assess whether an agent would satisfy the F&P test under reg 58
- assess the extent of the risk that the agent may be used for money laundering and/or terrorist financing
- have processes in place to monitor and manage compliance with and the internal communication of such policies controls and procedures (reg 19 (2) (e))
- have processes in place to identify and monitor transactions which are unusually large or complex, or an unusual pattern of transaction and transactions without apparent economic purpose
- have policies that ensure you adopt appropriate measures to assess and if necessary mitigate the ML risks of new products, business practices or technologies that you adopt

Actions required

3.25 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
- ensure additional controls are in place for approving transactions with PEPs
- ensure low risk situations are assessed and records retained to justify your assessment
- ensure arrangements for monitoring systems and controls are robust, and fully 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
- ensure policies are in place for sharing information with entities within the same corporate structure/group about customers, customer accounts and transactions for the purposes of preventing money laundering and terrorist financing within the group.
- when the business adopts new products, business practices or technology, these must be immediately incorporated into the business' policies, controls and procedures.

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

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

- the appointment of a member of the board of directors (or equivalent body) or senior management 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 auditing the business's compliance with its policies, controls and procedures

Making relevant appointments within your business

3.28 Every business must have a nominated officer, no matter what size it is. The nominated officer is responsible for receiving reports of suspicious activity from staff within the business and deciding whether to report them to the National Crime Agency.

3.29 Whether you have a compliance officer will depend on the size and nature of your business. The compliance officer is responsible for ensuring the business is compliant with the Regulations.

3.30 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.

3.31 A sole practitioner who has no employees and who does not act with another person does not need to appoint a compliance or nominated officer but must carry out the duties of the nominated officer and compliance officer themselves.

Appointing a nominated officer for the business

3.32 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.

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

3.34 You should make sure that your staff and the staff of your agents know the name of the nominated officer and any deputy. You must ensure they receive training on when and how to report their suspicions to the nominated officer (see reporting suspicious activity). HMRC expects the nominated officer to be based in the UK.

Appointing a compliance officer for larger, more complex businesses

3.35 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.

3.36 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.

3.37 For example, businesses with more premises, that use branches or agents, have a high turnover of customers, carry out non-local or cross-border trading or have complex ways to deliver services will need a compliance officer. This is so that the business can ensure that, for example, training, record keeping, and compliance requirements are observed and consistent throughout the organisation.

3.38 You may decide that an existing officer, of the required position and level of authority, may be able to take on the additional role.

3.39 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.

3.40 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 checking adherence to the policies, controls and procedures
    - reviewing how effective these are
    - recommending and implementing improvements following such reviews
- ensure compliance throughout the business (including subsidiaries, branches and agents) with anti-money laundering legislation and internal policies/procedures
- oversight of relevant staff and agent screening.

3.41 For these purposes "relevant staff" are persons involved in the identification of risk, controls and procedures to reduce risk and to ensure your compliance with the Regulations. Screening means an assessment of the skills, knowledge and expertise of these staff to carry out their functions effectively and the conduct and integrity of the individual.

3.42 These functions may be carried out from within the business.

3.43 It is recommended that the compliance officer and nominated officer in larger businesses should not be the same person. This is because the responsibilities between these roles differ: the compliance officer needs to be at a senior management level and needs to review how the business carries out its obligations including the reporting of suspicious activity. However, in some businesses (particularly those that are smaller and/or have a

simple operating model) it may not be practical to have two individuals carrying out these functions and a compliance officer may be suitable to also act as nominated officer.

3.44 Given the importance of this role, larger businesses may need to appoint a deputy compliance officer to take on the responsibilities when the compliance officer is absent for an extended period.

3.45 HMRC expects the compliance officer to be based in the UK.

3.46 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 at a group-wide level.

Personal liability of officers of a business

3.47 You are an 'officer' if you are:

- a director, secretary, chief executive, member of the committee of management, or a person who carries out that role in a business, even if you don't have the title
- a person in control of a business
- any officer of an association or any member of its governing body, or a person carrying out that role
- a partner, any manager, secretary or similar officer of a partnership, or a person carrying out that role.

3.48 An officer who is knowingly concerned in a breach of the Regulations may be subject to a civil penalty.

3.49 They will also be committing a crime if they do not comply with the Regulations. This may result in an unlimited fine and/or a prison term of up to 2 years if:

- The officer agrees to, or is involved in committing a crime
- A crime is committed because of their neglect.

Controls and procedures to put in place

3.50 Once you've identified and assessed the risks of money laundering and terrorist financing associated with your business, you must ensure that you put in place appropriate controls and procedures to reduce and manage them. They'll help to decide the appropriate 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 (who will present a relatively low risk of money laundering and terrorist financing), based on your business's risk assessment.

3.51 Procedures should be easily accessible to staff and agents 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 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 in connection with an individual customer/transaction
- how to keep records, and where and for how long they should be kept
- how and when 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
- policies on training, reliance and risk management .

3.52 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 which alter the risk profile associated with a customer
  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

3.53 This list is not exhaustive and should not be treated as a check-list. You could also have other risk-based controls depending on the circumstances of your business.

3.54 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.

3.55 Your risk assessment of a customer must reflect the risk of that particular customer, your business-wide risk assessment, and take into account risks highlighted by HMRC. Declining a business relationship should be a last resort, when you have concluded that it is not possible to effectively manage the money laundering/terrorist financing risks associated with a particular customer.

Effectiveness of the controls

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

3.57 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.

Managing group subsidiaries and branches

3.58 A parent company who is subject to the Regulations must apply its policies, controls and procedures in all subsidiaries or branches, in or outside the UK, who are also carrying out regulated activities. This will involve:

- putting in place controls for data protection and information sharing to prevent money laundering and terrorist financing, as well as sharing information about customers, customer accounts, and transactions
- sharing information on risk within the corporate group
- ensuring that subsidiaries or branches in EU member states are complying with the money laundering and terrorist financing requirements of that country
- ensuring that subsidiaries or branches in a third country (e.g., a non-EEA state) are applying anti-money laundering/counter-terrorist financing requirements that are equivalent to those required by the UK (as far as permitted under the law of that third country).

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

Managing a branch or agent network

3.60 If you manage a branch or agent network you should consider this (non-exhaustive) list of questions to help inform your risk assessment, and your policies, controls and procedures:

- how will you apply risk management procedures to a network of agents or branches
- how will you manage and maintain records, for example, if the branch closes or you end your relationship with an agent

- if you selected a number of customer files at random, would they all have a risk assessment and adequate customer due diligence records in connection with the customers and beneficial owners, and would ongoing monitoring support your original risk assessment
- if you have applied simplified due diligence, will your records evidence the decision to treat the customer as low risk in line with your risk assessment
- do you have a system that will pick up where individuals, departments, branches or agents are not implementing risk management procedures
- could you demonstrate that all staff, including those in your agents 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 at your branches and your agents know who the nominated officer is, what the firm's policies are and where they can be found

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 undertaking an occasional transaction that requires due diligence
- complete customer due diligence when you suspect money laundering, or have doubts about the documents or information previously collected for customer due diligence
- have adapted 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 persons established in high risk third countries.
- apply customer due diligence when you become aware that the circumstances of an existing customer has changed. This may require you to review the extent of due diligence undertaken, for example applying enhanced due diligence if the customer now represents a higher risk
- not deal with certain persons or entities if you cannot do customer due diligence andconsider making a suspicious activity report
- have a system for keeping copies of customer due diligence and supporting records and keep the information up to date
- understanding the legal and beneficial ownership or control structure of a customer when the customer is one of the following:
    - legal person
    - trust
    - company
    - foundation or
    - similar legal arrangement

Who is the customer?

4.1 The customer is the person or entity with whom the money service business forms a contractual relationship or provides a service to. 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. You must apply customer due diligence to each of them. This is explained further in the sections on beneficial owners, below, and on undertaking transactions with other money service businesses that are not agents.

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 which is 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, either at once, or in a series of linked transactions
- money laundering or terrorist financing is suspected
- you suspect that information obtained for due diligence checks on a customer is not reliable or adequate

4.5 Customer due diligence means:

- identifying all customers and verifying their identity (more details below)
- identifying all beneficial owners, where applicable, and taking reasonable measures to verify their identity to satisfy yourself that you know who they are
- 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

4.6 The customer's identity and where applicable the identity of a beneficial owner, must be verified before entering into a business relationship or undertaking an occasional transaction where customer due diligence is required.

4.7 You can make an exception to when customer due diligence is carried out 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

4.8 However, this exception is very limited and the verification must still be completed as soon as practicable after contact is first established. Even when it is available, it allows for the verification to be completed during the course of setting up the business relationship only and so must be completed by the time that relationship is established and no later than when there are contractual liabilities. This exception does not mean that you can delay customer due diligence because it is hard to verify a customer's or beneficial owner's identity.

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

Non-compliance with customer due diligence

4.10 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

4.11 Money deposited in an account may be repaid to the person who deposited it. However, you must ensure you have consent (in relation to a suspicion) from the National Crime Agency before it is repaid.

4.12 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

4.13 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

4.14 If the customer is a business, the relevant person must collect proof of registration or an excerpt of the register, before a business relationship is established, to show the business:

- is subject to the requirements of Companies Act 2006, Part 21A
- is subject to the requirements of Limited Liability Partnerships (Register of People with Significant Control) Regulations 2016
- is subject to the requirements of the Scottish Partnerships ((Register of People with Significant Control) Regulations 2017 or
- on or after 10 March 2020, is subject to registration under Part 5 of the Regulations.

Ongoing monitoring of a business relationship

4.15 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 the risk assessment. As part of your ongoing monitoring, you may need to contact an existing client to review any information and customer due diligence must be conducted at this point. Examples of requirements to review include:

- the risk assessment for the client
- beneficial ownership of clients who are a corporate structure
- when the relevant business becomes aware that the circumstances of an existing customer, relevant to its risk assessment for that customer has changed.

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

Occasional transaction

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

Beneficial owner

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

4.19 For a corporate body that is not a company whose securities are listed on EEA regulated markets and certain other main markets[1], 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
- holds the right, directly or indirectly, to appoint or remove a majority of the board of directors
- has the right to exercise, or actually exercises, significant influence or control over the corporate body
- exercises ultimate control over the management
- controls the corporate body.

4.20 If shares or rights are held by a nominee the beneficial owner will be the person for whom the nominee is acting. If the nominee is acting for a legal entity, then the beneficial owner will be the person who exercises ultimate control over the legal entity.

4.21 Similarly, if shares and rights are held indirectly, i.e. when a legal entity holds the shares or the rights and someone has a majority stake in that legal entity, the beneficial owner will be the person who has the majority stake and exercises ultimate control over the legal entity.

4.22 A joint interest is where two or more people hold the same shares or voting rights in a company. A joint arrangement is where two or more people arrange to exercise all or substantially all of their rights arising from their shares jointly in a way which is predetermined.

4.23 Where joint interests or joint arrangements are concerned, each person holds the total number of shares or rights held by all of them. So if two or more people hold jointly more than 25% of the shares or voting rights, each of them is a beneficial owner.

[1] Main markets in USA, Japan, Switzerland, and Israel.

4.24 As well as companies incorporated under the Companies Act, 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.

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

- ultimately is entitled to or controls, whether directly or indirectly, more than 25% of the capital or profits of the partnership
- ultimately is entitled to or controls, whether directly or indirectly, more than 25% of the voting rights in the partnership
- satisfies one or more of the conditions in Part 1 of Schedule 1 to the Scottish Partnership (Register of People with Significant Control) Regulation 2017 (guidance at section 2 Scottish qualifying partnerships guidance)
- exercises ultimate control over the management

4.26 For a trust, a beneficial owner includes:

- the settlor
- the trustees
- the beneficiaries
- where the individuals (or some of the individuals) benefiting from the trust have not been determined, the class of persons in whose main interest the trust is set up, or operates
- individuals who exercise control over the trust

4.27 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

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

4.29 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

4.30 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

4.31 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. If the business has exhausted all possible means of identifying the beneficial owner, the business must take reasonable measures to verify the identity of the senior person of the customer responsible for management in a corporate body. The business should keep records in writing of actions taken place to achieve this and any difficulties the business had in achieving this.

4.32 Where the customer is a legal person, trust, company, foundation or similar, you must take reasonable measures to understand their control structure, as well as who is the beneficial owner.

Extent of customer due diligence measures

4.33 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.

4.34 It goes beyond simply carrying out identity checks to understanding who you're dealing with. This is because even people you already know well may become involved in illegal activity at some time; for example if their personal circumstances change or they face some new financial pressure. Your due diligence measures should reduce the risk of this, and the opportunities for staff to be corrupted. This is covered in more detail below, and in the chapters on principal-agent relationships and risk indicators.

4.35 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

4.36 Your business may apply a simplified form of due diligence where the business relationship or transaction is considered low risk in terms of money laundering or terrorist financing. It can apply to any person you assess as low risk with some exceptions.

4.37 You will have to risk assess the customer to establish that they are low risk, taking into account relevant information made available by HMRC.

4.38 If simplified due diligence is applicable, you are still required to identify and verify customers' identities and identify and take reasonable measures to verify beneficial owners' identities. Under simplified due diligence however, you can change when it is done, how much you do, or the type of measures you take to identify and verify a person. For example:

- verifying the customer or take reasonable measures to verify the beneficial owner's identity:
    - during the establishment of a business relationship or
    - within a reasonable time, which HMRC would expect to normally be no more than 14 days from the start of the business relationship or transaction (this does not mean exemption from customer due diligence and any delay to customer due diligence must not be prohibited by any other legal requirement you are subject to)
- if applicable, verify the identity when transactions exceed a reasonably low level, use at least one authoritative identity document to verify identity that:
    - demonstrates the person's name, and (at least) either their address or date of birth
    - contains security features that prevent tampering, counterfeiting and forgery
    - has been issued by a recognised body that has robust identity proofing measures e.g. passport
- use information you already have to determine the nature or purpose of a business relationship without requiring further information, for example, if your customer is a pension scheme you can assume what the purpose is
- adjust the frequency of transaction monitoring such as checks triggered when a reasonable threshold is reached
- adjust the frequency of customer due diligence reviews, for example, to when a change occurs

4.39 If verification is not immediate, your system must be able to pick up on these cases so that verification of identity still takes place.

4.40 To apply simplified due diligence, you need to ensure that:

- it is supported by your customer risk assessment
- you take into account relevant information made available by HMRC

- enhanced due diligence does not apply
- you monitor the business relationship or transactions to ensure that there is nothing unusual or suspicious from the outset
- it is not prevented by information on risk provided by HMRC or any other authority in periodically published risk assessments
- either party to the transaction is established in or operates in a high risk third country identified by the EU, FATF or HMT
- 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
- 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.

4.41 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.

4.42 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 in the UK or equivalent regulation in another country
- an individual resident in a geographical area of lower risk
- a company whose securities are listed on a regulated market
- beneficial owners of pooled accounts held by a notary or independent legal professional, provided information on the identity of the beneficial owners is available upon request
- a European Community institution.

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

- resident or established in another EEA state
- situated outside the EEA in a country:
    - subject to equivalent anti-money laundering measures o with a low level of corruption or terrorism
    - has been assessed by organisations such as FATF, FATF-style Regional Bodies, World Bank, Organisation for Economic Co-operation and Development and the

International Monetary Fund as having in place effective anti-money laundering measures.

4.44 The Joint Money Laundering Steering Group publishes more information about the level of risk in other jurisdictions (Annex 4-1 part 1)

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

4.46 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.

4.47 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.

4.48 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.

4.49 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.

4.50 Your decisions may be tested based on the evidence that your business holds.

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

- suspect money laundering or terrorist financing
- doubt whether documents obtained for identification are genuine
- doubt whether the person is the one demonstrated by the documentation
- suspect that the documents obtained for identification maybe lost, stolen or otherwise fraudulently acquired
- circumstances change and your risk assessment no longer considers the customer, transactions, or location as low risk.

Enhanced due diligence

4.52 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.

4.53 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 established in, or operates in a high risk third country identified by the EU, FATF or HMT
- 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, or unusually large, or with an unusual pattern and have no apparent legal or economic purpose
- a customer is a third country national who is applying for residence rights in or citizenship of an EEA state in exchange for transfers of capital, purchase of a property, government bonds or investment in corporate entities in that EEA state.

4.54 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.

4.55 You should consider several 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.

4.56 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 shares 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

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

- the transaction involves private banking
- the transaction favours anonymity
- 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

4.58 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 under domestic sanctions legislation or "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 Cooperation and Development and the International Monetary Fund as having in place effective anti-money laundering measures.

4.59 When the transaction is related to any of the following, you must consider whether you should carry out enhanced due diligence:

- oil
- arms and weapons
- precious metals and stones
- tobacco products
- cultural artefacts
- ivory and other items related to protected species

Additional measures to take

4.60 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. How this goes beyond standard due diligence must be made clear in your risk assessment and procedures. For example:

- obtain additional information or evidence to establish the identity from independent sources, such as more documentation on identity or address or electronic verification alongside manual checks
- take additional measures to verify the documents supplied such as by checking them against additional independent sources, or require that copies of the customer's documentation are certified by a bank, financial institution, lawyer or notary who are competent at document inspection and impostor detection, or a person from a regulated industry or in a position of trust
- if receiving payment ensure it is made through a bank account in the name of the person you are dealing with
- take more steps to understand the history, ownership, and financial situation of the parties to the transaction
- in the case of a politically exposed person 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.
- measures which must be taken when either party to a business relationship, or relevant transaction is established in a high-risk third country (a business is established in a country if they are incorporated there, is is their principal place of business, or they are regulated there as a financial or credit institution; an individual is established in a country if they are resident there):
    - Obtain additional information on the customer and the customer's beneficial owner
    - Obtain additional information on the intended nature of the business relationship
    - Obtain information on the source of funds of the customer and of the customer's beneficial owner
    - Obtain information on the reasons for the transaction
    - Obtain the approval of senior management for establishing or continuing the business relationship
    - Enhance monitoring of the business relationship by increasing the number and timing of controls applied, and select patterns of transactions which require further examination
- At least one of the following measures must be taken when the transaction relates to a politically exposed person, a family member or known close associate of a politically exposed person:
    - 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 a business relationship.

Certification

4.61 If the original documents are not produced for verification, or cannot be validated with an authoritative source, then you can use a certified document instead.

4.62 You can read more about certification of documents here.

Politically exposed persons (PEPs)

4.63 Politically exposed persons are persons that are entrusted with prominent public functions, whether in the UK or abroad. This is because international standards issued by the Financial Action Taskforce (FATF) recognise that a PEP may be in a position to abuse their public office for private gain and a PEP may use the financial system to launder the proceeds of this abuse of office.

4.64 The definition does not include:

- middle ranking or more junior officials
- persons who were not a politically exposed person under the 2007 regulations where they ceased to hold a prominent public function prior to 26 June 2017, such as former MPs or UK Ambassadors

4.65 In the UK, civil servants below Permanent or Deputy Permanent Secretary-level will not normally be treated as having a prominent public function. When assessing whether a person is a PEP, you should be mindful of whether a person is acting on the instruction of, or on behalf of, a PEP. This is more likely to be the case when the relevant persons hold prominent functions in a third country which presents a relatively higher risk of money laundering.

4.66 Politically exposed persons include:

- heads of state, heads of government, ministers and deputy or assistant ministers
- members of parliament or similar legislative bodies
    - includes regional governments in federalised systems and devolved administrations, including the Scottish Executive and Welsh Assembly, where such bodies have some form of executive decision-making powers. does not

include local government in the UK but it may, where higher risks are assessed, be appropriate to do so in other countries.

- members of the governing bodies of political parties
    - member of a governing body will generally only apply to the national governing bodies where a member has significant executive power (e.g. over the selection of candidates or distribution of significant party funds).
    - political parties who have some representation in a national or supranational Parliament or similar legislative body.
- members of supreme courts, of constitutional courts or of any judicial body the decisions of which are not subject to further appeal except in exceptional circumstances; in the UK this includes judges of the Supreme Court but does not include any other member of the judiciary
- members of courts of auditors or boards of central banks
- ambassadors, and high-ranking officers in the armed forces
    - where persons holding these offices on behalf of the UK government are at Permanent Secretary or Deputy Permanent Secretary level, or hold the equivalent military rank e.g. Vice Admiral, Lieutenant General or Air Marshal
- members of the administrative, management or supervisory bodies of state owned enterprises
    - this only applies to for profit enterprises where the state has ownership of greater than 50% or where information reasonably available points to the state having control over the activities of such enterprises
- directors, deputy directors and members of the board, or equivalent of an international organisation.
    - includes international public organisations such as the UN and NAT does not include international sporting federations.

4.67 The Regulations require that family members of PEPs must also have enhanced due diligence measures applied to them. For these purposes, the definition of "family member" includes:

- spouses/civil partners of PEPs;
- children of PEPs and their spouses/civil partners
- parents of PEPs
- brothers and sisters of PEPs.

4.68 Beyond this definition, firms should take a proportionate and risk-based approach in assessing whether any given individual is a family member of a PEP – it may, for example, be appropriate to treat a wider circle of family members (such as aunts and uncles) as subject to enhanced due diligence measures in cases where a firm has assessed a PEP to present a higher risk.

4.69 Known 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.

Politically exposed person's risk

4.70 You must always apply enhanced due diligence on politically exposed persons, their family members or known close associates. Guidance on how to identify such persons is set out in the section above. You must have appropriate risk management systems and procedures in place to determine whether a customer is a politically exposed person or a family member or known close associate of one. You should take account of:

- your own assessment of the risks faced by your business in relation to politically exposed persons
- a case by case assessment of the risk posed by a relationship with a politically exposed person
- any information provided through the National Risk Assessment or by HMRC

4.71 Information is available in the public domain that will help you to identify politically exposed persons. You can make use of several sources, for example:

- ask the customer
- search the internet
- news agencies and sources
- government and parliament websites
- Electoral Commission: http://search.electoralcommission.org.uk/
- Companies House Persons of Significant Control: https://beta.companieshouse.gov.uk/
- Transparency International: https://www.transparency.org/
- Global Witness: https://www.globalwitness.org/en-gb/campaigns/corruption-andmoney-laundering/

4.72 You are not required to, but you may decide to use a commercial provider to assist in identifying politically exposed persons.

4.73 Whatever source is used you need to understand how any database is populated, for example how often it is updated. You should ensure that those flagged by the system fall within the definition of a politically exposed person, family member or known close associate as set out in the Regulations and this guidance.

4.74 If a 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 a business relationship.

4.75 You must, however, assess in each case the level of risk that the politically exposed person presents and apply an appropriate level of enhanced due diligence. More frequent and thorough measures should be taken if the politically exposed person is higher risk. Similarly, a reduced level of enhanced due diligence measures can be applied to lower-risk politically exposed persons. A politically exposed person who has a prominent public function in the UK should be treated as lower risk unless other factors in your risk assessment indicate a higher risk. The same treatment should be applied to family members or close associates of lower risk UK politically exposed persons.

4.76 You must continue to apply enhanced due diligence when the politically exposed person has left their function or position and for a further period of at least 12 months after they cease to hold such a function. Any extension over 12 months will normally only apply to a politically exposed person you have assessed as higher risk. As set out above, UK PEPs should be treated as lower risk unless specific factors indicate otherwise, and so you should typically cease applying enhanced due diligence measures to such persons 12 months after they cease to hold a prominent public function.

4.77 For family members and known close associates, the obligation to apply enhanced due diligence stops as soon as the politically exposed person no longer holds the office unless there are other reasons for treating them as higher risk.

4.78 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.

4.79 A lower risk politically exposed person may be one who holds office in a country 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.

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

- are subject to rigorous disclosure requirements such as registers of interests or independent oversight of expenses
- do not have decision making responsibility such as a government MP with no ministerial responsibility or an opposition MP.

4.81 A high risk politically exposed person may be from, or connected to, a country viewed as having a higher risk of corruption that may have 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 a small number of people or entities with close links to the state
- lacking a free press and where legal or other measures constrain journalistic investigation
- a criminal justice system vulnerable to 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
- human rights abuses.

4.82 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

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

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

4.84 The family and known 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
- an appointment to a public office that appears inconsistent with personal merit.

4.85 Where you have assessed a politically exposed person as a higher risk it may be appropriate to consider a wider circle of family members, such as aunts or uncles, as part of your risk assessment.

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

- supervision of the business relationship is at a less senior management level
- source of wealth and funds established from information you already have or publicly available information only
- ongoing monitoring is less intensive such as only when necessary to update due diligence information.

4.87 You should identify when a politically exposed person is a beneficial owner of a corporate body and take appropriate measures based on your risk assessment. This does not make the legal entity or other beneficial owners politically exposed persons as well. If the politically exposed person has significant control and can use their own funds through the entity then a higher risk is indicated and enhanced due diligence may be required.

Customer due diligence on transactions below €15,000

4.88 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.

4.89 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

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

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

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

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

4.94 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 may check that you have an adequate system in place and are operating it effectively.

Identifying individuals

4.95 If your customer is an individual, you must identify them as part of your customer due diligence. You should obtain a private individual's given and family name, date of birth and residential address as a minimum.

4.96 Documentation purporting to offer evidence of identity may come from a number of sources. These documents differ in their integrity, reliability and independence. Some are issued after due diligence on an individual's identity has been undertaken; others are issued on request, without any such checks being carried out. There is a broad hierarchy of documents:

- certain documents issued by government departments and agencies, or by a court; then
- certain documents issued by other public sector bodies or local authorities; then
- certain documents issued by regulated firms in the financial services sector; then
- those issued by other firms' subject to the Regulations, or to equivalent legislation; then
- those issued by other organisations.

4.97 You should verify these using identity evidence that has been issued by a recognised body, for example a Government department, that has robust identity proofing measures, and includes security features that prevent tampering, counterfeiting and forgery 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

4.98 When verifying the identity of a customer using the above list of government-issued documents, you must take a copy and keep it in the customer's file. However, it may be appropriate to also record the details of what identity evidence was presented and the information that was on the document, as well as how this evidence was checked and the outcome of the verification process.

4.99 Documents issued by official bodies such as Government departments are independent of the customer, even if provided by the customer.

4.100 Where the customer doesn't have one of the above documents you should ask for the following:

- A valid and genuine identity document from a recognised and authoritative source, such as 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, that can be verified as true by the company that issued it, commonly by confirmation of a reference number, name and address; for example, a utility bill, bank, building society or credit union statement or a most recent mortgage statement

4.101 If you verify the customer's identity by documents, you should see the originals and not accept photocopies, unless certified.

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

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

- spellings
- validity
- photo likeness
- whether addresses match.

4.104 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.

4.105 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.

4.106 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.

Persons without standard documents

4.107 Some persons such as elderly persons or those that cannot manage their own affairs may not be able to produce current standard documents because they have been incapacitated or have not driven or travelled for some time and have allowed licenses and passports to lapse.

4.108 Before accepting non-standard documents, you should exhaust the traditional forms of identification first.

4.109 The types of documents that you could accept should be from a reliable and independent source that has knowledge of the person, for example documents from:

- a medical professional
- a legal professional
- the head of a care home with relevant professional qualifications
- a pension provider stating that the person is in receipt of a pension

4.110 If non-standard documentation is used to confirm the client's identity, measures should be taken to establish whether the documentation is genuine – for example, the use of documents references or organisation

4.111 The JMLSG Guidance for the UK financial sector Part I, at the section "Customers who cannot provide the standard evidence" (from 5.3.108) gives more detail on situations where nonstandard documents may be acceptable.

Electronic verification

4.112 Simply carrying out electronic records checks on limited information, such as the name and address of a person you have not seen, does not mean that you have verified that the person you are dealing with is who they say they are. You must 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 (to protect against impersonation). You should therefore verify key confidential facts that only the customer may know to establish who they say they are. For example, testing the person using robust information that is not known to be, or likely to be, in the public domain. Manual identity documents can be checked alongside electronic verification where greater risk is indicated. 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.

4.113 If you verify an individual's identity electronically, you must:

- use a package which addresses the risks detailed in your risk assessment and understand how it addresses those risks
- use multiple positive information sources, such as addresses or bill payment details
- use negative sources, such as databases identifying identity fraud and deceased persons
- use data from multiple sources collected over a period of time
- incorporate checks that assess the strength of the information supplied
- ensure that the system is set to fail/refer a customer at a level appropriate to the risk posed by the customer you are carrying out customer due diligence on

- retain, or have access to, sufficient records in order to comply with your record keeping requirements, which must take into account events such as an external provider going out of business.

4.114 The extent of the checks should satisfy the level of risk established in your risk assessment. It is not sufficient to maintain, for example, that the electronic outsourcing provider has stated it meets your needs or the requirements of the Regulations, including additional services such as a 'PEP check'.

4.115 Care must be taken if you are using remote identification methods to ensure the risks are understood and are sufficiently addressed; for example, simply viewing a photo document over the internet or a "selfie" of a person holding identification documents using Skype, is not an appropriate form of customer due diligence if there are not also reliable measures to identify counterfeits or forgeries. The use of facial recognition software does not address this issue as an individual seeking to bypass the checks will successfully match a face to a photo of the same face on a false document.

4.116 If using an electronic/digital identity (eID) provider you should ensure that it is reliable, accurate, independent of the customer, is secure from fraud and misuse, and capable of providing an appropriate level of assurance that the person claiming a particular identity is in fact the person with that identity. You should consider the following criteria in your selection:

- it is a notified eID scheme under the eIDAS Regulation[1];
- it is provided by means of a trust service covered by the eIDAS Regulation[2];
- it is accredited, or certified, to offer the identity verification or trust services through a government, industry or trade association process that involves meeting minimum published standards (such as those set out in the government's guidance on identity proofing[3] , GOV.UK Verify or the eIDAS regulation);
- it is registered with the Information Commissioner's Office (or national equivalent for EEA/EU registered organisations) to store personal data
- the standards it works to, or accreditation, require its information to be kept up to date
- its compliance with the standards is assessed
- it uses a range of 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 sources, such as up to date financial sanctions information

[1] https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS
[2] https://webgate.ec.europa.eu/tl-browser/#/
[3] https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual

- it has transparent processes that enable the firm to know the level of certainty as to the identity
- should be able to keep records of the information used to verify identity and make them available to the relevant authorities as required
- If it is not
    - An eIDAS eID or trust service
    - accredited, or certified, to offer eID or trust services through a governmental, industry or trade association process that involves meeting minimum published standards; or
    - regulated, recognised, approved, or accepted by the relevant national authority for the provision of digital identity or trust services; then they should have processes that allows you to capture and store the information they used to verify an identity.

4.117 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.

Individuals not resident in the UK

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

4.119 If you have concerns that an identity document might not be genuine, contact the relevant embassy or consulate or use the link to PRADO below.

4.120 Public Register of Authentic travel and identity Documents Online: http://www.consilium.europa.eu/prado/en/prado-start-page.html

4.121 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 certified translations when inspecting your customer due diligence records.

Identifying organisations as customers

4.122 For customers who are corporate entities, partnerships, trusts, charities, or 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
- ownership and control structure of the entity

4.123 Where you find a discrepancy about the beneficial ownership of your customer, you must report it to Companies House. Further guidance can be found on the Companies House website.

4.124 Where the customer is a trustee acting on behalf of a trust, you must identify and verify the identity of the trustee(s) and assess – and where appropriate obtain information on – the purpose and intended nature of the business relationship or occasional transaction. You should also identify and verify the identity of the settlor and identify/verify the identity of other beneficial owners of the trust on a risk-sensitive basis, and in accordance with your assessment of the risk associated with the customer relationship.

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

- country of incorporation and laws it is subject to (from Articles of Association or an equivalent document)
- names of the members of management body, or if none, its equivalent and the name of the senior person responsible for the company

4.126 You should establish the names of all directors (or equivalent) and must identify the ultimate beneficial owners (the section on beneficial ownership provides information on who they are). You must look through the ownership structure of any companies or trusts to establish the ultimate beneficial owners. If you exhaust all means of identifying the beneficial owner, you must take all reasonable steps to verify the identity of the senior person. You must keep a written record of all the steps you have taken and who you have identified.

4.127 Beneficial owner's identity may be found through, for example:

- enquiries of or requesting the information from the company
- searching for Persons of Significant Control (PSC) at the Companies House register
- company website searches
- public records in the UK and overseas.

4.128 You do not satisfy your obligation to verify the identity of beneficial owners by relying only on information contained in a PSC register.

4.129 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.

4.130 Where an individual claims to act on behalf of a customer, you must also obtain evidence that the individual has the authority to act for them, identify the individual and verify their identity. Evidence that the individual has the authority to act may be through a call to the customer with a confirmation email by return, legal documents, Companies House information showing a connection or third-party confirmation.

Obligation of customers to provide information

4.131 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.

4.132 Guidance on the requirements to maintain PSC registers is available at: https://www.gov.uk/government/publications/guidance-to-the-people-with-significantcontrol-requirements-for-companies-and-limited-liability-partnerships

4.133 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.

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

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

Beneficial owners

4.136 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 take reasonable measures to 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 and look through company structures until you reach individuals who are the ultimate beneficial owners.

4.137 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 the Register of People with Significant Control.

4.138 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 and consider whether they should be treated as a higher risk.

Reliance on third parties

4.139 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.

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

4.141 You must enter into an arrangement with the third party to allow you to:

- obtain immediately 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 on which the transaction occurs or the business relationship with the customer ends.

4.142 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.

4.143 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.

4.144 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. Within outsourcing arrangements, you still remain responsible for any failure to apply due diligence measures appropriately.

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

4.146 See also the section on undertaking business with another money service business that is not your agent.

5. Money transmitters - additional obligations

5.1 Money transmission businesses must comply with Regulation (EU) 2015/847 on complete 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 The European Supervisory Authorities have produced guidance to assist money transmitters on the measures payment service providers should take to detect missing or incomplete information on the payer or the payee, and the procedures they should put in place to manage a transfer of funds lacking the required information.

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

5.4 Complete information refers to information obtained on the payee and payer for the purpose of a relevant transaction on the basis of documents, data or information obtained from a reliable and independent source. Full details can be found in Information accompanying transfer of funds.

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

5.6 The money transmitter for the "payer" must:

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

5.7 **For transfers outside the EU:**

- obtain complete information (as detailed in section 5.7) on the payer and payee for all customers wanting to transmit money; and
- verify the complete information on the payer on the basis of documents data or information from a reliable independent source

5.8 **For transfers inside the EU**, where all payment service providers are established in the EU:

- Obtain payment account numbers of payer and payee or unique transaction reference number.
- On request from payment service provider of the payee, must also provide (within 3 days):
    - For transactions (including several linked transactions) over €1,000 – complete information as set out in section 5.7
    - For transactions under €1,000 - payer and payee names, in addition to the payment account numbers or unique transaction ID.

- 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

5.9 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

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

- ensure the payer and payee information accompanies 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

5.11 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

5.12 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 payee

5.13 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)

5.14 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.

5.15 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.

5.16 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.

5.17 Where a transaction is greater than €1,000 or money laundering or terrorist financing is suspected then customer due diligence must be carried out and copies of the records used to identify and verify the customer must be retained.

Exclusions

5.18 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

5.19 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

Minimum requirements

- Staff, including the staff of your agents 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, or their appointed alternative, 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, following a disclosure to a nominated officer or to the NCA, to do or say anything that might either 'tip off' another person that a disclosure has been made or prejudice an investigation.

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, an employee, an agent, or their 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:

- Queries regarding SAR Online/general enquiries:
  - Option 1 – Telephone 0207 238 8282
  - Option 2 – email – ukfiusars@nca.gov.uk
- Defence Against Money Laundering (DAML) Enquiries. All contact with the UKFIU DAML team is via email: DAML@nca.gov.uk

6.6 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).

6.7 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).

6.8 You must provide regular training for your staff and your agents in what suspicious activity may look like in your business and you should keep records of that training, who has received it and when.

6.9 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.

6.10 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.

6.11 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

6.12 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.

6.13 Employees 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.

6.14 Agents must also be aware of the process of reporting a transaction to your nominated officer.

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

6.16 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.

A defence (consent)

6.17 If you wish to go ahead with the transaction or start a business relationship with the customer who you have made a report about, then you must ask for permission from the NCA to progress the transaction. This permission, (if granted) will constitute a defence to a money laundering or terrorist financing offence. This is also known as a Consent SAR and the consent needs to be given by the NCA. It is only when the consent is given that it provides you with a defence against a charge in relation to money laundering or terrorist financing offences.

6.18 You should tick the “consent requested” box on the SAR form. See the guidance Requesting a defence from the NCA under POCA and TACT

6.19 It is an offence for the nominated officer to allow a transaction to proceed 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.

6.20 A defence relates to the principle offences in Proceeds of Crime Act (s327 to 329) and the Terrorism Act (s15-18) but not to other criminal offences.

6.21 A granted response or no reply from the NCA within the notice period does not imply that the NCA approve of the proposed act(s), persons, corporate entities, or circumstances contained within the disclosure, nor does it oblige or mandate a reporter to undertake the proposed act. You should consider your position carefully. A defence does not provide derogation from, or replace, a reporter's professional duties of conduct or regulatory requirements, such as those under the Regulations concerning, for example, customer due diligence.

6.22 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 at the end of the notice period.

6.23 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. It is an offence to allow the transaction to proceed during the moratorium period if consent has been refused. In terrorist financing cases the moratorium period does not apply, you do not have a defence until a request is granted.

6.24 The moratorium period can be extended, by a court, in cases where further information or evidence is required.

6.25 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 must 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
- if the request is urgent and 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 confirm their decision in writing.

6.26 Requesting a defence can only apply where there is prior notice to the NCA of the transaction or activity. The NCA cannot provide consent after the transaction or activity has occurred. The receipt of a SAR after the transaction or activity has taken place will be dealt with as an ordinary standard SAR, and in the absence of any instruction to the contrary, a business will be able to provide services to the customer until such time as the NCA determines otherwise through its investigation.

Tipping off

6.27 It is a criminal offence for anyone to say or do anything that may prejudice an investigation or 'tip off' another person that a suspicion has been raised, a SAR has been submitted 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.

6.28 Nobody should tell or inform the person involved in 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.

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

Suspicious activity

6.30 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

6.31 These are some of the questions to consider in deciding risk and whether 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

6.32 These are some of the questions to consider when deciding risk and whether 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

6.33 These are some of the questions to consider when deciding risk and whether 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

Minimum requirements

7.1 You must retain:

- copies of the evidence obtained to satisfy customer due diligence obligations and details of customer transactions for at least five years after the end of the business relationship
- details of occasional transactions for at least 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 that the third party's relationship with the customer ends, the agreement should be in writing

7.2 You must also maintain a written record of:

- your risk assessment and any changes made
- your policies, controls, and procedures and any changes made
- what you have done to make staff aware of the money laundering and terrorist financing legislation and related data protection requirements, as well as the training given to staff

Actions required

7.3 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

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

- for at least 5 years after the end of the business relationship
- for at least 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.

7.5 The records should be reviewed periodically to ensure, for example, that a fresh copy of expired documents, such as driving licenses or passports are held. This review need only include ongoing relationships.

7.6 You are not required to keep customer transaction records that are part of a business relationship for more than 10 years, where a business relationship is ongoing.

7.7 After the period above the records must be deleted unless you are required to keep them in relation to legal or court proceedings or any other legislation.

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

7.9 You can keep records in the form of original documents or copies in either hard copy or electronic form. Copies should be clear and legible. The aim is to ensure that the business meets its obligations and, if requested, can show how it has done so.

7.10 This evidence may be used in court proceedings.

7.11 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.

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

8. Employees and agents awareness and training

Minimum requirements

8.1 You must:

- ensure relevant employees, your agents and their employees 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 their responsibilities are, trained in the firm's procedures and in how to recognise and deal with potential money laundering or terrorist financing transactions or activity
- ensure staff, your agents and their employees are trained at regular intervals
- maintain a written record of what you have done to raise awareness and the training given to your employees, agents, and their employees
- ensure that a relevant director or senior manager has overall responsibility for establishing and maintaining effective training arrangements.

8.2 Larger and more complex businesses must:

- screen relevant employees before they take up post to assess that they are effective in carrying out their function and are of good conduct and integrity.

Actions required

8.3 You should ensure that your firm is doing each of the following points, and keep the extent to which these points are satisfied under regular review:

- provide appropriate training to make relevant staff aware of money laundering and terrorist financing issues, including how these crimes operate and how they might take place through the business
- ensure that relevant employees have information on, and understand, the responsibilities and legal obligations of the business - individual members of staff, e.g. the functions of the nominated officer and any changes to these positions
- regularly share risk assessment, policy, control, and procedures information within the business and with branches and subsidiaries
- consider providing relevant staff with case studies and examples related to the firm's business to illustrate where risks of money laundering and terrorist financing are most likely to arise
- train relevant staff in how to operate a risk-based approach to assessing the risks of money laundering and terrorist financing and how to accurately verify identity documents (to standards laid out by Home Office)
- where appropriate for a larger business and/or more complex business set up a system to screen staff before they take up the post and refresh the screening at intervals

- keep records of training given

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

8.5 You must take steps including:

- telling your staff about your anti-money laundering and counter terrorism financing obligations and the risk of IT systems being abused
- making them aware of data protection obligations

8.6 You should also consider the following steps as part of their training:

- making them aware about how to effectively verify the identity of individuals.
- giving them suitable (risk based) training on their legal obligations
- telling them how to identify and deal with the risks

8.7 A money service business acting as a principal should ensure that agents (and the agents' employees) are trained to an equivalent standard to that of their own employees.

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

Training

8.9 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 whether (and if so, how) reception staff, administrative staff and finance staff should be trained, because they'll each have different levels of involvement in compliance, and different training needs.

8.10 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.

8.11 Nominated officers, 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.

8.12 Each member of employee and agent should be ready to deal with the risks posed by their role. Their training should be good enough, and delivered sufficiently frequently, to keep their knowledge and skills up to date.

8.13 It must include, in relation to money laundering and terrorist financing risks, matters including:

- data protection requirements
- 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.

8.14 It should cover, in relation to money laundering and terrorist financing risks, matters including:

- the employee or agent's duties
- the risks posed to the business
- the business' policies, controls and procedures
- how to conduct customer due diligence and check customers' documents
- how to spot and deal with suspicious customers and activity
- document inspection and imposter detection
- how to make internal reports, including disclosures of suspicious activity
- record keeping

8.15 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.

8.16 A policy manual outlining the policies, controls and procedures the business has put in place for the purpose of preventing money laundering and terrorist financing is useful to raise awareness and for reference between training sessions.

8.17 You must train new staff who join the business and you should re-train staff when they move to a new job or when they change roles. You must train agents when they are appointed to provide relevant services. They should also have ongoing training at least every 2 years or when a significant change happens, for example legislation or the business' risk assessment changes.

8.18 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.

8.19 Training records include:

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

9. Principal-agent relationships and other business models

9.1 Money service businesses frequently enter into arrangements with other parties to enable the money service business to provide its services to customers, typically as follows:

Principal–agent business models

9.2 These include:

- appointing an agent or agents to act on behalf of a money service business (the principal) in the provision of their services. For example, this may be to:
    - accept money transmission instructions from customers
    - accept cheques for encashment
    - undertake currency exchange
- appointing 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

9.3 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.

9.4 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 transactions.

9.5 An agent may have agency agreements in order to act on behalf of more than one principal.

9.6 This may, for example, enable the agent to offer remittances to a wider range of destinations.

Meaning of 'principal'

9.7 Acting as a principal in this context 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.

9.8 In a principal-agent relationship, the principal is the person or entity 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 Regulations and the Proceeds of Crime Act.

9.9 Typically, a written contract or 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.

Meaning of Agent

9.10 An agent is a separate person or entity, who are appointed to act on behalf of the principal in the provision of their services. This arrangement may be directly between agent and principal or may be a between an agent of the original principal and a further agent.

9.11 For example, everyone (except the original MSB principal and the customer) described below would come under the definition of agent:

9.12 MSB A enters into a contract with Agent B under which MSB services will be provided via Agent B. Agent B delivers its business through different arrangements (including the MSB's services) with Agent C.

9.13 Agent B directly provides MSB services on behalf of MSB A. Agent C also provides MSB services on behalf of MSB A, even though their arrangement is with Agent B. The employees of Agents B and C who provide the MSB service to customers are also agents.

9.14 When HMRC refers to your agents, it refers to the equivalent personnel in the agent as it does for you as a principal. For example, when HMRC refers to the beneficial owners, officers, and managers, it also means the beneficial owners, officers, and managers of your agents. When HMRC refers to any employees that provide regulated activity, it also means the employees of your agents that provide regulated activity.

Guidance for appointing and managing an agent

9.15 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 of an agent before they begin to provide MSB activity.

9.16 An MSB principal must tell HMRC of the removal of an agent within 30 days.

9.17 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.

9.18 A principal should also have an up-to-date record of any agents that are appointed through their agents.

9.19 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.

9.20 HMRC expects principals to have checked whether the agent and its beneficial owners, officers and managers (BOOMs) are fit and proper persons. You can read more about this in our fit and proper technical guidance, here: https://www.gov.uk/government/publications/money-laundering-supervision-fit-and-proper-test-and-approval

9.21 The principal should establish strong oversight of all agents providing their services 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.

Minimum expectations

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

9.23 An 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 this obligation to check their own employees.

9.24 Guidance can be found at: https://www.gov.uk/government/publications/right-to-work-checks-employers-guide

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

9.26 Principals should ensure that an agent meets minimum expectations, in particular that the agents and its beneficial owners, senior managers, officers and nominated officer of the agency:

- are fit and proper persons for their fiduciary role
- are of good character
- do not have criminal records (see **Appendix 1: Relevant offences under schedule 3 of the Regulations**)
- have not been the subject of any professional conduct or disciplinary action
- must demonstrate professional standards and competence in business conduct
- have the right to work in the UK and documents have been checked
- should be sufficiently well capitalised and have adequate staff for its role
- should meet minimum record keeping, internal controls and consumer protection measures
- should maintain a good compliance record.

9.27 Principals and their agents should know who this responsibility falls to when agents appoint further agents.

Before making an appointment

9.28 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
- develop 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

9.29 Once an agent is appointed, the principal should:

- carry out ongoing monitoring of customers and business transactions, including regular onsite 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 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.

9.30 When an agent is appointed by another agent, or when the agent is part of a large network, HMRC expects the principal to have a process in place to carry out the actions above.

Foreign currencies

9.31 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 and transfer that information if necessary
- require their agents to have physical controls and security measures, which might include counterfeit detection equipment and closed-circuit cameras as a deterrent against crime.

Transactions with other money service businesses that are not agents

9.32 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 a business relationship and 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.

9.33 There are some additional requirements when undertaking money transmission as an intermediary for another money service business, you must do all 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.

9.34 When acting as a settlement agent in order to settle in bulk a series of transactions undertaken by two other money service businesses, 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
- 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.

9.35 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.

9.36 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 2017, or under an equivalent regime under the Payment Services Directive (2015/2366/EC).

Franchising

9.37 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.

9.38 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.

9.39 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.

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 or act as both an agent and a 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
- are located geographically in a high-risk area (e.g. in another cash intensive business, or in a border area)
- remit funds overseas in cash through couriers or parcel companies
- former money service businesses re-registering as different cash businesses

- money service businesses not disclosing money service business activity to their bank
- multiple money service business premises operating in very small area
- money service businesses with bank accounts held in higher risk countries rather than the UK

Money transmitters

10.3 The following are examples of common risks 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.

10.4 The Risk Factors Guidelines produced by the European Supervisory Authorities provides guidance (at chapter 4) on the factors money transmitters should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions.

New customers

10.5 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

10.6 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
- are destined for money service businesses around the borders of countries at high risk of terrorism.

10.7 Where the beneficiary of a money transmission is in a high-risk country you should do enhanced due diligence checks on your customer. To help you decide if you're sending money to a high-risk country, FATF 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

10.8 When you receive a transfer of funds from a foreign money service business, you must treat the foreign money service business as your customer. This occurs when a customer outside the UK wishes to carry out a transfer of funds to a beneficiary in the UK. 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. This information will allow you to monitor that the number and average value of transactions is consistent with the anticipated level of activity when you began your business relationship. It will also give you an indication of risk, particularly where the number of transactions or the average transaction value is significantly above what you expected.

10.9 Where the transfer of funds is included in any sort of 'offset arrangement' (where you pay the beneficiary from your own funds and the debt owed to you by the overseas Money Service Business is satisfied by a payment from them to a third party at your instruction) this is a separate, potentially high risk transaction. You must perform customer due diligence and if appropriate enhanced due diligence checks on the overseas Money Service Business. Based on your assessment of the risk this should include checking some specific transactions where you have instructed the overseas Money Service Business to make a payment to a third party.

10.10 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. The location of the customer does not affect your need to perform customer due diligence. You must apply customer due diligence and where appropriate, ongoing monitoring if an overseas customer deals directly with you in the UK.

Third party payments

10.11 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 is sometimes described as 'third party pooling' or 'cover payments'. This type of remittance and settlement involves 2 separate transactions, each of which requires the appropriate customer due diligence or enhanced due diligence.

10.12 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. Where the payment is to be made against an invoice you should check that the document is genuine. This could include checking if the:

- name and address of the purchasing business are correct
- supplier exists

- description of the goods is credible
- value of the goods is realistic

10.13 You should seek further evidence if you have any level of doubt about the invoice and check that it is genuine by getting supporting documentation such as movement certificates, shipping orders, packing lists and/or bills of loading.

10.14 Third party payments exclude circumstances where payment is made to a beneficiary in the UK or elsewhere on the instructions of an overseas customer which does not involve offset of a payment. In this situation the Money Service Business in the UK needs to do the appropriate level of customer due diligence on the overseas customer

Third party cheque cashing

10.15 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

10.16 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

10.17 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

10.18 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

10.19 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

10.20 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

10.21 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 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
- border transaction

Regular and existing customers

10.22 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

10.23 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. You should regard any request to buy or sell €500 notes as potentially suspicious. You should refuse to sell €500 notes and submit a suspicious activity report. Requests for high denomination notes by a customer should be treated as high-risk and you should do enhanced due diligence checks and submit a suspicious activity report if appropriate.

Dealing with other money service businesses

10.24 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

10.25 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

11. More information

11.1 If after reading this guidance you have any queries, or would like further information you can contact us by:

- Telephone: 0300 200 3700.
- Email: mlrcit@hmrc.gov.uk

11.2 HMRC always aims to give you the best possible service. However, if you're unhappy with our service or the way we have treated you may wish to make a complaint. More information about how to complain can be found in our guidance on complaints and putting things right on the GOV.UK website.